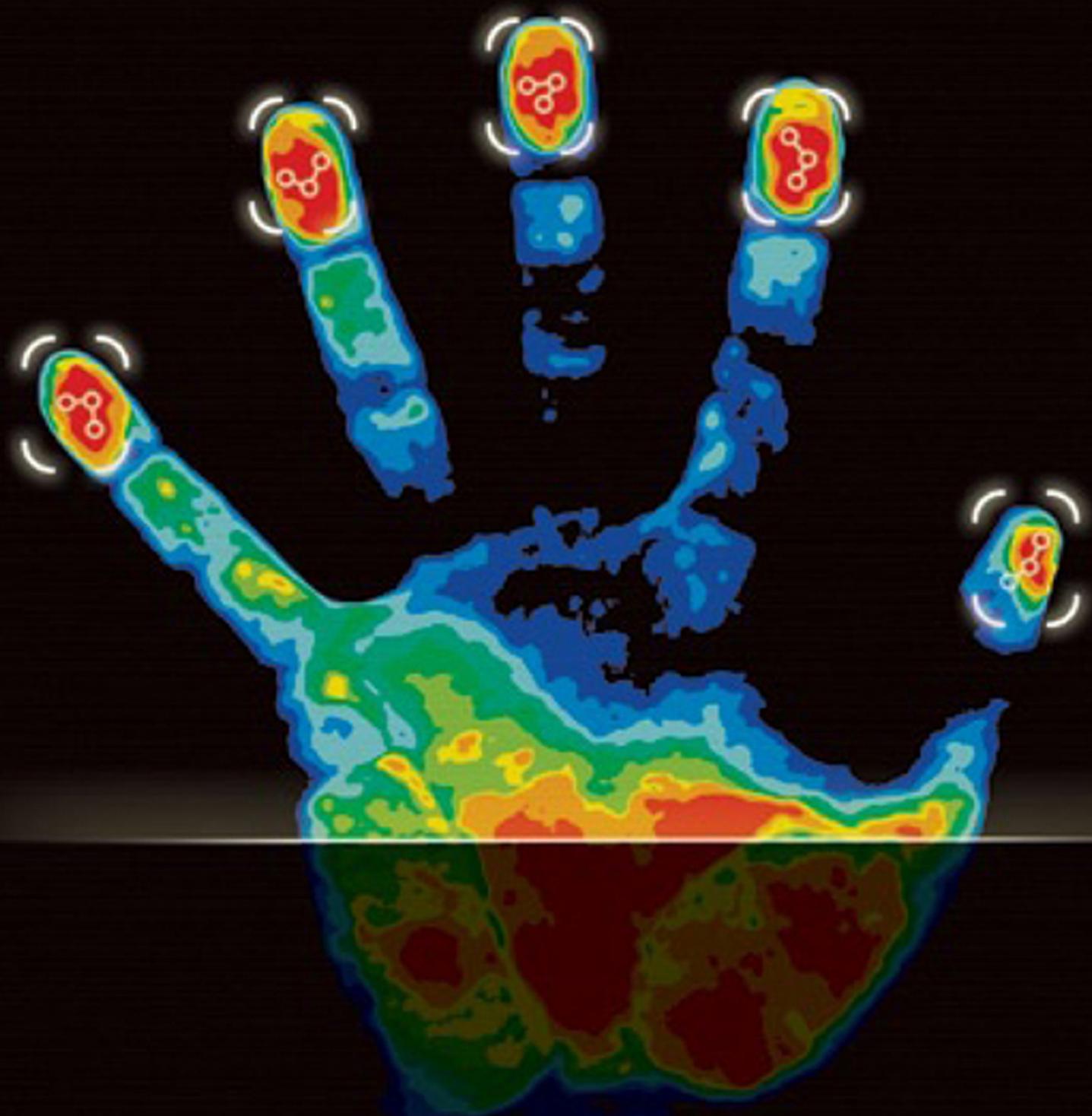




# Global Privacy Protection

The First Generation



Edited by

**James B. Rule** and **Graham Greenleaf**

# Global Privacy Protection

# Global Privacy Protection

The First Generation

---

*Edited by*

James B. Rule

*University of California at Berkeley, USA*

and

Graham Greenleaf

*University of New South Wales, Australia*

**Edward Elgar**

Cheltenham, UK • Northampton, MA, USA

© The Editors and Contributors Severally 2008

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical or photocopying, recording, or otherwise without the prior permission of the publisher.

Published by  
Edward Elgar Publishing Limited  
The Lypiatts  
15 Lansdown Road  
Cheltenham  
Glos GL50 2JA  
UK

Edward Elgar Publishing, Inc.  
William Pratt House  
9 Dewey Court  
Northampton  
Massachusetts 01060  
USA

A catalogue record for this book  
is available from the British Library

Library of Congress Control Number: 2008935926



**PEFC**<sup>™</sup>

PEFC/16-33-111

CATG-PEFC-052

[www.pefc.org](http://www.pefc.org)

ISBN 978 1 84844 063 0 (cased)

Typeset by Cambrian Typesetters, Camberley, Surrey  
Printed and bound in Great Britain by MPG Books Ltd, Bodmin, Cornwall

# Contents

---

<i>List of contributors</i>	vi
Introduction	1
<i>James B. Rule</i>	
1 International agreements to protect personal data	15
<i>Lee A. Bygrave</i>	
2 The United States	50
<i>Priscilla M. Regan</i>	
3 Germany	80
<i>Wolfgang Kilian</i>	
4 France	107
<i>Andre Vitalis</i>	
5 Privacy in Australia	141
<i>Graham Greenleaf</i>	
6 Hungary	174
<i>Ivan Szekely</i>	
7 Republic of Korea	207
<i>Whon-Il Park</i>	
8 Hong Kong	230
<i>Robin McLeish and Graham Greenleaf</i>	
Conclusion	257
<i>James B. Rule</i>	
<i>Bibliography</i>	276
<i>Index</i>	299

# Contributors

---

**Lee A. Bygrave** (<http://folk.uio.no/lee>) is Associate Professor at the Law Faculty of the University of Oslo. He is currently a member of a Privacy Commission established by the Norwegian government to assess the state of privacy protection in Norway and to propose measures for bolstering such protection.

**Graham Greenleaf** is Professor of Law at the University of New South Wales, Sydney, Australia, and Asia-Pacific Editor of *Privacy Laws & Business International*, and from 1994–2004 was the founding editor of *Privacy Law & Policy Reporter*. His current privacy research includes leading an Australian Research Council project ‘Interpreting Privacy Principles’ which investigates whether an Asia-Pacific privacy jurisprudence is emerging.

**Wolfgang Kilian** is Professor of Law at the University of Hanover/Germany and President of the Federation of European Research Institutes for Information Technology and Law ([www.iri.uni-hannover.de/kilian](http://www.iri.uni-hannover.de/kilian)).

**Robin McLeish** practices as a barrister in Hong Kong, and writes on privacy law issues. He was the Deputy Privacy Commissioner in Hong Kong during the formation of that office in the 1990s.

**Whon-Il Park** is Associate Professor of Law at Kyung Hee University, Seoul, Korea. He teaches corporation law, Internet law and international business transactions. Professor Park is currently at work on a study of how to facilitate trans-border data flow and inter-Korean economic cooperation.

**Priscilla M. Regan** is Professor of Government and Politics at George Mason University in Fairfax, VA. She has authored many scholarly publications analyzing privacy and technology policy issues and served as a member of the National Academy of Sciences, Computer Science and Telecommunications Board, Committee on Authentication Technologies and their Privacy Implications.

**James B. Rule** is Distinguished Affiliated Scholar at the Center for the Study of Law and Society, University of California, Berkeley. He is currently working on

a study of new uses of – and demands for – personal information likely to emerge in the next several decades.

**Ivan Szekely** is Counsellor, Open Society Archives, and Associate Professor at the Budapest University of Technology and Economics. His recent publications include *Access to archives* (with Charles Kecskemeti; Council of Europe Publishing, Strasbourg, 2005) and ‘Central and Eastern Europe: Starting from Scratch’, in A. Florini (ed.), *The right to know. Transparency for an open world* (Columbia University Press, 2007).

**Andre Vitalis** is Professor at the Michel de Montaigne University of Bordeaux, where he heads the Media Studies Research Group. His research and writing deal with the social roles of media and technologies, and their regulation.

# Introduction

## James B. Rule

---

Public issues are like living creatures. They have life-cycles – beginnings, middles and (eventually) ends. Issues are typically the offspring of non-issues: things that people once considered trivial, normal or inevitable, but which they redefine as unacceptable, even intolerable, and susceptible to change. Very often these transitions into issue-hood are the work of social movements that publicize and condemn what they hold to be scandalous conditions – as in the public definition of *sexual harassment* as a condition requiring remedial action in law and policy. Other issues ‘just grow’, as people come to agree even without exhortation that certain conditions, perhaps of long standing, are no longer acceptable. Whatever their origins, public issues are defined by their contested nature – their acknowledged status as matters on which people have to take stands for or against change.

This book traces the birth and early history of privacy, and the need for its protection, as a public issue. Privacy is an inexact term, one that gets applied to a variety of related concerns. We focus here on controversies over the fate of personal data held by government and private institutions in conventional or computerized files. Since roughly the 1960s, such privacy concerns have risen to the state of issue-hood in virtually all the world’s democracies. At stake are such questions as what personal information institutions may collect, where and how it can be stored, who can gain access to it, and what actions can be taken on its basis.

Spurring these concerns has been the growing realization that such files have potentially sweeping consequences for the lives of those depicted in them. People’s records direct the attentions of law enforcement authorities; shape consumers’ access to credit and insurance; guide the search for suspected terrorists; help determine our tax liabilities; shape the medical care and social welfare benefits that we receive – and on and on. In a world where one’s records count for more and more, in terms of the treatment one receives from major institutions, questions of what practices should govern creation and use of such records were all but inevitable. It was the growing conviction that these consequential processes require active attention and response in law and policy that transformed privacy into a public issue.

This work seeks to make sense of divergences and parallels across countries

on these matters. It traces the interactions between global forces and national contexts on the privacy issue in seven countries since the 1960s. Separate chapters focus on the United States, Australia, Hong Kong, France, Germany, Hungary and South Korea. One additional chapter covers the evolution of international agreements that have shaped privacy policy throughout the world.

Many people believe that computing was the unique and original cause of the emergence of privacy as a public issue. This is not strictly true. Struggles over what personal information could be committed to records, who could compile such records and what could be done with them were under way well before anyone realized that computing might play a role in these processes. What new information technologies have done is to accelerate the expansion of personal data systems – making them both more extensive and more consequential in the lives of ordinary citizens.

Most obviously, computing makes it vastly more feasible for government and private institutions to create and use enormous databases of personal information that would have been prohibitively costly under conventional technologies. I can recall, from some very early research, a centralized American security clearance agency in Ohio in the 1960s that relied on blue paper index cards for every individual. Today reliance on paper-based records on that scale would be unfeasible at any reasonable cost. By contrast, we take it for granted that the incremental costs of adding to, sharing and manipulating personal data in today's computerized record-systems are all but negligible. The result is that all sorts of personal data that would otherwise simply be 'lost' – passing unrecorded from human notice – are now 'harvested' by institutions that do everything from allocating consumer credit to directing anti-terrorist efforts. Such institutional appetites for personal data generate a never-ending stream of privacy controversies.

Computing thus makes it attractive to capture and use personal data in all sorts of settings and for all sorts of purposes that would once have been inconceivable. One result is to narrow the realm of anonymity – so that fewer interactions, relationships and transactions are possible without identifying one's self. Any American can attest to this phenomenon over the last decade, particularly in the wake of the 11 September attacks. From boarding a domestic air flight to renting a car to entering large buildings, presentation of 'government-issued photo ID' has become a taken-for-granted requirement. Telephone calls widely announce the identity of the caller – regardless of the caller's preferences in the matter. In cities abroad, subway travel often involves the rider identifying himself or herself by name. As one result, London's Metropolitan police have used the resulting travel records to track supposed perpetrators of crime who appear to have stolen victims' transit cards. Similar stories could be told about access to medical care, toll roads and bridges, cable TV service and a host of other everyday conveniences.

New information technologies have not compelled anyone to collect the data at issue in these settings. But they have enabled large institutions to associate specific transactions and events with specific individuals in ways that alarm privacy advocates.

There are countless examples. Consider RFID technology. RFID (radio-frequency identification) chips are tiny transmitting devices, often no bigger than a grain of rice, that can broadcast their whereabouts to sensors, without being noted by the person who might be carrying them. They can be unobtrusively loaded in merchandise, passports, pets or indeed in people themselves (that is, by insertion under one's skin) so as to track the chip's movements. Originally used to monitor inventory and prevent theft from retail establishments, they now promise to provide another source of data on the movements of people and the things they carry with them.

All these changes make personal information available in new forms, to new parties, and for new purposes. Often the personal data in question simply did not exist previously, at least in any enduring form. Who (besides the wearer) could tell, before the use of RFID chips, where one's underwear came from, or where it was going? Who could take stock, before automated toll collections, of the identities of the hordes of travelers on superhighways or bridges? The existence of personal data in recorded form inevitably brings new opportunities – and conflicts. Who can use RFID equipment to track the whereabouts and movements of American passports? When can data on toll road use be accessed? Should these data be more open to government investigators, say, than to parties to divorce proceedings?

Answers to such questions help define what one might call the privacy culture prevailing in any setting – the 'map' of taken-for-granted expectations of what categories of personal information one can expect to keep to one's self, and what will normally be disclosed to one party or another. The one sure generalization about privacy cultures in recent times is that they are everywhere in headlong change. Demands on our privacy from what sociologists like to call 'primary groups' – family, church or community – generally diminish, as the claims of such groups on our loyalties grow weaker. But at the same time, in the spheres of concern to this book, privacy cultures shaped by demands of government and private-sector institutions on personal information are reflecting new constraints. From tax collection agencies to credit reporting companies to anti-terrorist investigators, bureaucratic organizations are seeking and using more and more of 'our' data – and the prerogatives of such access are more and more accepted in prevailing privacy cultures.

Individually, capture of any one new form of personal information is apt to strike anyone simply as an annoyance or indignity. But cumulatively, the broad growth of systems like these – with their long-lasting storage of personal data and easy sharing across systems – points to trends that alarm privacy advocates.

The accumulation of these vast stores of personal information, and their systematic use by public and private organizations, change basic relationships between ordinary people and institutions. These changes signal long-term shifts in the ability of governments and corporations to 'reach out' and shape people's lives. And in so doing they trigger the search for new principles, new institutions, and new legal and policy constraints to address the newly-defined issue of information privacy.

\*

The United States seems to have been the first country to focus on privacy as a public issue. As early as the 1960s, Americans' anxiety over creation and use of files on consumers' credit histories triggered demands for public action. The ultimate result was federal legislation on credit records based on principles that became widely applied in other domains. But credit controversies quickly paled in comparison to those surrounding political abuse of government data files by the Nixon administration in the Watergate period. Coming at a moment of maximum mistrust of public institutions, demands for reform of institutional record-keeping on 'private' citizens thus joined a striking array of other new public issues. One key result was America's Privacy Act of 1974, governing administrative records held by federal agencies. Today this law remains the American privacy legislation of broadest applicability – in contrast to piecemeal legislation covering specific forms of personal data in health care, bank records, video rentals and the like.

In 1973, Sweden passed its Data Act – the first national privacy act in the world. By the end of the 1970s, West Germany, France, Norway, Luxembourg, Denmark and Austria had framed their own national personal data-protection legislation. In the 1980s, Canada, the UK, Australia, the Netherlands, Finland, Iceland, Israel and Japan joined this 'privacy club'. In 1995, the European Union adopted its influential Privacy Directive, for eventual 'transposition' into the legal systems of all member countries. Today the EU membership stands at 27 countries with roughly 450 million inhabitants; all these states are formally committed to the precepts of the 1995 Directive. Other countries adopting privacy codes in recent years include India, South Korea and Argentina.

In all these countries, the status of privacy as a public issue is now taken for granted. Whatever institutions and policies have been adopted in response, one assumption has to be taken for granted: personal data must not be treated as though it were just any form of data. As German privacy spokesman Spiros Simitis commented, regarding a trade dispute between Europe and the United States over the export of personal information, 'This is not bananas we are talking about.' The fact that information refers to people, and accordingly has

direct repercussions on their lives, means that some special principles must govern its use.

But what should those principles be? Indeed, what are the essential ‘goods’ to be defended by privacy protection efforts, or the most notorious ‘bads’ to be avoided? How should misuse or abuse of personal data be understood – and what forms of these things should be considered most dangerous? What sorts of institutions, policies or legal forms provide the most effective measures to these ends? Here countries adopting privacy codes have evolved answers that differ considerably.

Considerably, but not totally. Even a casual look at the unfolding of the privacy issue since its inception reveals striking national parallels. Like many another issue that came into existence in the 1960s, privacy concerns today constitute a global phenomenon. Global, in that many of the forces shaping privacy controversies take much the same form all over the world.

Among these are the technologies and management strategies of privacy invasion. Managers everywhere, in both government and private institutions, pursue very similar visions of doing better by knowing more about the people they are dealing with. Tax authorities in all countries yearn to develop more comprehensive information that might reflect on citizens’ tax liabilities. Security agencies always seek to find ways of using available personal data – and data that might be created – to identify and track potential terrorists. Police and other law-enforcement agencies eye anonymous populations and wish that they had more reliable tools for knowing who is who. Credit grantors and sellers of insurance everywhere seek information that will reveal which consumers will prove to be profitable customers – and which ones to avoid. Direct marketers strive constantly for information on individuals and their living situations that will reveal what consumers are most susceptible to which advertising campaigns. And for all these purposes, the possibilities offered by present-day information technology know no borders. Software systems, servers or data-base management systems available in one country today can be in place on the other side of the world next week – if the proper investments are made.

\*

Even before the rise of computing, privacy concerns elicited global attention – in terms of international declarations on the importance of protecting privacy. As early as 1948, the UN adopted the Universal Declaration of Human Rights, which declares

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

This rather vague statement took no cognizance of changes soon to be triggered by computing. But as the potential for overbearing use of computerized personal data became clear, a number of influential bodies proposed codes of practice to govern systems of personal data – codes that have had far-reaching repercussions in law and policy. Among the most influential of these codes are those promulgated by US Department of Health, Education and Welfare (1973), the Council of Europe (1981), the Organization for Economic Cooperation and Development (1980), the Australian Privacy Charter Council (1992) and the Canadian Standards Association (1996).

These bodies came up with recommendations showing some notable common themes. One can condense their precepts into the following nine points:

1. The keeper of any system of personal records is responsible for the safety, security and integrity of the data so stored. (HEW, OECD, CSA, APC, C of E)
2. The existence, purposes and workings of such systems should be readily accessible to public understanding. (HEW, OECD, CSA, APC, C of E)
3. A single figure (a ‘privacy officer’ or ‘data controller’) should be identified publicly as responsible for safeguarding the privacy interests affected by the working of each such system. (OECD, CSA, APC, C of E)
4. Information held in such systems must be collected legally and fairly. (OECD, CSA, APC, C of E)
5. Individuals must be able to review the content of information held on them in such systems and the uses and disclosures of such information; individuals must be able to obtain redress for inaccurate and inappropriate uses and disclosures of such data. (HEW, OECD, CSA, APC, C of E)
6. Personal data should only be collected in the form and to the extent necessary to fulfill the purposes of the system. (OECD, CSA, APC)
7. Information held in file should be as accurate and up-to-date as necessary to fulfill the purposes of the system. (OECD, CSA, APC, C of E)
8. Information collected for one purpose should not be used or released for other purposes, except under legal requirement or with permission of the individual. (HEW, OECD, CSA, APC)
9. Information held in file should be collected with the knowledge or consent of the person concerned. (OECD, CSA, APC)

(from *Privacy in Peril*, James B. Rule, Oxford University Press, New York, 2007, p. 26)

Most of the five codes propose at least a few precepts not found in the

others. Principle 10 of the Australian Privacy Charter, for example, stipulates that ‘People ought to have the option of not identifying themselves when entering transactions.’ But all things considered, the nine points above can be considered consensus principles of ‘fair information practices’ – practices now widely held to be basic to protecting privacy in institutional treatment of personal data.

It would be hard to overemphasize the global influence of these principles. They have individually and jointly inspired privacy codes all over the world. The recommendations of the Canadian Standards Association, for example, directly shaped that country’s 2000 legislation governing personal data practices in the private sector. The OECD Guidelines had much influence over the European Community’s 1995 Privacy Directive, which in turn now forms the basis for privacy law in all EU member countries. Lee Bygrave devotes his chapter to tracing these direct and indirect lines of influence, and other contributors to this work note their repercussions for policy in each country.

\*

A more diffuse carrier of global ideas has been the growing world-wide community of what I call ‘privacy watchers’ – people who track the issue from within many countries and many different social positions within those countries, yet communicate freely across international boundaries. Privacy watchers include journalists, jurists, government officials, business people, scholars and grass-roots citizens. Some are professional activists working, often on shoe-string budgets, in organizations like Privacy International in London; the Citizens’ Action Network in South Korea; the Center for Democracy and Technology and EPIC in Washington, DC; and Option Consommateurs in Montreal. Among government officials, privacy watchers include staff members of the national and provincial privacy commissions established in most of the world’s prosperous democracies. Though these figures hardly speak with a single voice, they share an informed understanding of the underlying issues that makes them a force in decisions on treatment of personal data all over the globe. They play the indispensable role of monitoring and analyzing the workings of systems whose complexity and scope are bound to overwhelm the attention capacity of most members of the public.

If this mix of human and technological forces were all that mattered, privacy protection would take something close to the same form everywhere – and there would be no need for a book like this. But even in a world where such global influences make themselves felt predictably, national responses are far less predictable. Ultimately, only states can create privacy codes. Even

casual examination reveals that these codes take many forms – in the institutions created to protect privacy, the legal precepts invoked to that end, and in the political cultures through which the issue is contested. Uses of personal data widely accepted in one country – for example, the unauthorized trade in personal financial data for credit and marketing in the United States – are blocked by privacy strictures in France, Australia and elsewhere. Independent national agencies dedicated to privacy protection at the national level are all but universal among the world's prosperous democracies – yet the United States, which gave birth to privacy as a public issue, has consistently refused to create such a body. Citizens and residents of some countries have long been inured to carrying government-mandated ID cards – as in South Korea and Germany – whereas other governments, however attracted to the advantages that such systems would place at their disposal, have failed to impose them.

In short, the evolution-in-progress of privacy as a public issue resembles many other forms of globalization. Each country presents an array of privacy developments recognizable to virtually any informed outside observer – along with practices, attitudes and institutions that appear utterly peculiar to the countries in which they occur. And often these parallels and divergences are deceptive. Apparently similar laws and institutions in fact work in different fashions in different countries – whereas what seem to be quite different arrangements may conduce to rather similar results.

Thus policy-makers in every country adopting privacy codes have had to confront some predictable and consequential choices. Many countries, including EU members, have enacted generic privacy legislation that establishes rights applying to *all* personal data held in file – for example, rights of access to one's own file. Such rights are typically qualified by exceptions, for example excluding from privacy codes investigative activities by law enforcement or state security agencies. But notwithstanding such exceptions, a system of generic privacy rights creates a different environment from the piecemeal approach prevailing, say, in the private sector in the United States. There one's rights over information on choices of video rentals are different from those regarding health-care data – and those in turn different from rights over consumer credit files. And many forms of private-sector data in the US are not governed by any subjects' rights.

Then there are questions of what authority should be empowered to act on behalf of citizens' privacy interests. In the United States, individuals normally must act on their own behalf to enforce privacy rights, where they exist. In nearly every other democracy, a privacy commission or commissioner has authority to act on behalf of privacy interests – including interests of aggrieved individuals who have no other recourse. But the powers accorded to commissions and commissioners differ from country to country. Some privacy

commissioners have the right to initiate investigations of data systems suspected of violating data rights; others do not. Some privacy commissioners can introduce, on their own initiative, national legislation; most do not have this power. Some privacy commissioners can condemn personal data uses as violations of privacy law at their own instance; others act only in response to complaints from the public. Some commissioners and commissions have as a major element of their responsibilities adjudication and conciliation between individuals and institutional users of their data; others do little or no such mediation. All these distinctions turn out to have far-reaching repercussions in terms of what privacy interests receive enforcement, when, how and on whose behalf. Each chapter of this book considers the distinctive directions taken in these respects in one country.

Then, too, there are significant differences in interpretation of crucial ideas of privacy-protection practice, even when the underlying principles are shared. Many privacy codes specify that an individual's consent is necessary, before specific forms of personal information can be collected and used. But how is 'consent' manifested – when does it exist by implication, for example? And what circumstances should be held to render consent meaningless? On subscribing to a magazine, most of us no doubt feel we are granting implicit consent to the publisher to retain our address data for the duration of the subscription; without these data, the publication could not be sent. But do we also grant consent, in these circumstances, to the publisher to use our data for other purposes – for example, to exchange with other publications, so that they may direct advertising appeals our way? And what about the 'consent' of the sort that used to be sought from Americans seeking medical care – authorizing the care-giver to share information with virtually any parties that might be necessary for purposes ranging from medical determinations to billing? At what point do incentives against withholding one's consent render such consent meaningless?

Related issues arise in tensions between 'opt-in' and 'opt-out' interpretations of privacy measures. Is my consent to dissemination of my bank account data assumed, if I fail to indicate wishes to the contrary (the 'opt-out' interpretation)? Or is the absence of any statement to be interpreted as no consent ('opt-in')? This dilemma arises in countless settings – from banking and finance; to the capture of data for direct advertising; to uses of data from telephone books and local tax records. Opt-in requirements are obviously more protective of privacy; data-keeping institutions generally favor opt-out. Here, too, different countries have navigated the resulting policy pressures in quite different ways.

National approaches to privacy protection in matters like these of course differ across countries, but also across time. Many privacy-watchers would hold that privacy protection is weaker in the United States – with its scarcity

of broad rights and lack of any national office dedicated to privacy protection – than in other prosperous democracies. But most observers would probably also agree that world-wide levels of privacy protection have declined in recent years, especially in response to the ‘war on terror’. The influence of the United States, both in commercial and government data practices, has played a key role in this global trend – as America has pressured other countries to compile and share personal data, such as that on air travelers, that would otherwise be protected by national privacy guarantees. Then, too, American corporations have been extending their reach into many other consumer societies – causing scandal recently in Canada, for example, by selling the personal telephone records of Canada’s Privacy Commissioner to Canadian journalists. The erosion of privacy guarantees over time, and the role of the US government and private interests in that erosion, are themes for the chapters that follow.

\*

The idea for this book arose in dinner conversations between Graham Greenleaf and James Rule in 2003. We reflected that a number of valuable sources provide basic comparative information on the state of privacy law and institutions in different countries (for example, *Privacy and Human Rights 2005*, published by the Electronic Privacy Information Center). But we could think of no comparative analyses of what one might call the *social and political chemistry* underlying the state of current practice in various countries. Our interest lay not mainly in documenting what forms of data collection were and were not legal in each country. Instead, we wanted to sponsor analyses from experts within a series of countries of how privacy sensitivities had arisen and asserted themselves in each place.

We wanted to consider who had first brought the issue to the fore; what forms of privacy protection were readily accepted in each country, and which were contested; what different government agencies did and did not define roles for themselves in protecting people’s interests in treatment of ‘their’ data; and what parties and what groups in each country might reasonably be considered winners, and losers, as a result of the unfolding of the privacy issue. In short, we wanted the chapters to portray the unfolding fate of privacy in each country as a distinctive manifestation of the political and cultural life of that country.

We knew that coverage of all countries with working privacy codes was impossible. By the new millennium, that would have yielded a volume with scores of chapters. Instead, we resolved to commission accounts of parallel developments in a representative variety of countries. It would make no sense, we concluded, to commission chapters on countries where privacy issues had barely surfaced. But among countries with some history of privacy-protection

measures, we could ensure a measure of variability in coverage. Thus some countries covered here have relatively long-standing privacy codes; others are relatively new members of the global 'privacy club'. The United States and France were among the first countries to adopt privacy codes, in the 1970s; Hong Kong, South Korea and Hungary have done so just since the 1990s.

As context for the national studies, we needed a look at international agreements whose precepts have inspired national privacy codes around the world. Lee Bygrave's chapter does this. It shows how a core of consequential ideas have emerged, beginning with the Council of Europe initiatives in the 1970s, that have come to define the meaning of adequate privacy protection around the globe.

Many of the countries covered here have strong and long-standing national-level agencies dedicated to privacy protection; the United States, by contrast, has no such body, and no sign of creating one. Nor does the United States have a strong tradition of establishing what privacy watchers call *omnibus* privacy rights – rights over all or nearly all categories of personal data files. Instead, more than other countries, the United States has generated specific protections for treatment of data in narrowly-defined settings – health care, for example, or consumer credit. Priscilla Regan explores the implications of this form of American exceptionalism in her chapter on the United States.

We also wanted this work to cover as many different continents, legal traditions, levels of prosperity and other dimensions of social, political and economic difference as possible. Some of the countries included here have long-standing liberal traditions that have lent themselves readily to establishment of privacy rights. The United States, Australia, France and Germany, for example, all have long histories of efforts – unevenly successful, to be sure – to defend individual rights and autonomy. But the differences across these countries are revealing. France, as Andre Vitalis points out, has a strong and long-standing national privacy commission that bans much private-sector reporting on consumers' personal finances – whose parallels in the United States are the stuff of everyday commerce.

Australia has a more populist public ethos that has supported widespread resistance to identity cards and American-style credit reporting. But as Graham Greenleaf shows in his chapter, Australians accept many of the same forms of state surveillance orchestrated by the French and American governments. In this latter connection, Wolfgang Kilian's chapter on Germany suggests that privacy sentiments have generated more substantial resistance to state monitoring there than in many other countries.

Hungary and South Korea strike a contrast here. These countries have recently emerged as liberal democracies, after years of authoritarian rule. As Ivan Szekely and Whon-II Park demonstrate, recent memories of abuse of personal information by the authorities have generated added public support

for privacy protection – at least in the immediate aftermath of the repressive eras.

Finally, Hong Kong presents the most interesting case of all – not a country, but a polity occupying a precarious space between an overtly authoritarian regime and the world of liberal market societies. As Robin McLeish and Graham Greenleaf show, institutions and legal precepts of privacy protection have flourished under Hong Kong's semi-autonomous status – without much active support or awareness as yet from the populace.

\*

Every contributor to this volume is a highly-qualified privacy watcher, steeped in the history and lore of the issue in her or her own country. Quite possibly, each contributor knows more than any other single person about the twists and vicissitudes of the issue in that country, while also maintaining a firm grip on the global culture of privacy that has impinged on national affairs.

We have sought to produce a work that is more than the sum of its parts. In preparing these chapters, the authors (and editors) have exerted themselves to keep attending to each other's work. Each chapter author has been asked to address – not slavishly, but thematically – a common agenda of concerns. An early meeting at the Rockefeller Foundation's Bellagio conference center provided the setting for an extended seminar where the first draft of each chapter received a full and thoughtful airing. A major focus of those discussions was our effort to ensure that the individual chapters really do raise parallel questions and shed light on similar processes.

Thus all chapters begin with a capsule national history of privacy protection, forswearing any attempt at exhaustiveness, but noting key events and turning points in the evolution of the issue. All chapters comment on the role of public opinion – thus revealing some striking differences. Some countries, for example – the United States, Australia and South Korea, notably – have seen privacy propelled into national consciousness by explosions of public outrage over official misuse of personal data. Elsewhere, privacy measures emerged far more quietly, as part of elite policy agendas, often introduced into national legislation in response to events in other countries or international privacy agreements. All chapters comment on the role of distinctive national values and traditions in shaping privacy measures. Is it true, as is sometimes alleged, that special 'Asian' (or Anglo-Saxon, or Continental) values and traditions make for privacy demands distinctive to any one country? Or, as one often suspects, are citizens of all countries susceptible to a taste for privacy, if only the political process provides appropriate openings?

Each chapter also seeks judgments on what groups and what interests have gained, and which have lost, through the emergence of privacy as an issue.

Have privacy codes significantly reduced government freedom of action? Have they blocked significant profit-making but privacy-invading forms of business? Or have privacy measures (as commentators in some countries allege) served more to legitimize inherently privacy-invading practices – such that the country has ended up with more privacy laws, but less privacy? Finally, each author seeks to read the tea leaves of future developments in his or her country – asking what privacy advocates can reasonably hope for in the years to come, and what they have to fear.

\*

In the lifetime either of a human being or of a public issue, 40 years provides ample vantage to assess long-term directions and possibilities. Obviously the evolution of privacy continues, absorbing new influences from both global and local contexts. But some straws in the wind ought to be apparent. Which of the early aspirations of privacy protection have met with success – and which have notably failed? What kinds of institutions and measures seem really to have accorded people a measure of control over their own data – and which now appear misconceived, futile, or hopelessly outweighed by opposing forces? Where, if anywhere, have agencies and commissions dedicated to protecting privacy managed to retain their independence from government and corporate influence? Does public opinion provide a reliable source of support to privacy protection efforts, for example? Or (as some observers fear) has growing familiarity with personal data systems, and computing in general, fostered acquiescence or even fatalism concerning resistance to invasion of privacy?

These are just a few of the questions to be addressed in the pages to follow. Though our work can hardly yield definitive answers, we hope that the chapters to follow provide indispensable ingredients for continuing conversations on all these questions.

\*

Publication of this volume has depended from the beginning on generous and indispensable support from a variety of institutions and individuals. At the very beginning, John Grace of Canada, Peter Hustinx of the Netherlands, and the Hon Justice Michael Kirby of Australia – elder statesmen on privacy matters from Canada, the Netherlands and Australia, respectively – were good enough to vouch for the idea for the work as it was presented to various funding agencies. Among those agencies, the US National Science Foundation, Program on Ethics and Values of Science, Engineering and Technology, played the most crucial support of all, by providing funding for the project

(Award Number SES 0421919). The NSF funds were later supplemented by a generous grant from the Rockefeller Foundation, making it possible for the editors and chapter authors to meet in an extended seminar at that foundation's conference center in Bellagio, Italy.

Each of the authors is indebted to his or her home institution for supporting the work appearing here. James Rule is particularly grateful to the Center for Advanced Study in the Behavioral Sciences at Stanford University for providing a most agreeable and productive setting for the early phases of planning and editing.

\*

The volume begins with Lee Bygrave's context-forming chapter on international agreements that have shaped global privacy protection from its earliest years. Each of the following seven chapters focuses on a single country, beginning with the first to adopt national privacy legislation – the United States – continuing with progressively later adopters and ending with the most recent member of the 'privacy club' treated here, Hong Kong.

# 1. International agreements to protect personal data

**Lee A. Bygrave**

---

## CLEAVAGE, CO-OPERATION AND THE INCREASING WEIGHT OF THE WORLD

‘This is not bananas we are talking about.’ Thus spoke Spiros Simitis when describing the European view of privacy in an interview with the *New York Times* in May 1999.<sup>1</sup> Simitis, Europe’s de facto privacy doyen,<sup>2</sup> made his remark at a time when the European Union (EU) was locked in a dispute with the United States of America (USA) over what constitutes adequate protection of personal data. The primary catalyst for the dispute was the adoption by the EU of a Directive on data protection in 1995.<sup>3</sup> The Directive places a qualified restriction on flow of personal data from the EU to any non-EU member state failing to offer ‘adequate’ protection of personal data. For many non-Europeans, this seemed to be a case of the EU legislating for the rest of the world and, indeed, legislating to the detriment of legitimate business interests. Concern about such detriment was especially strident in the USA. There, federal government officials had estimated that the restriction threatened up to USD120 billion in trade – an amount far greater than had supposedly been at stake in previous trans-Atlantic trade conflicts.<sup>4</sup>

In May 1999, the dispute between the EU and USA had entered a particularly tense stage. After months of negotiations, talks were stalling, each side claiming that the other was trying to impose unacceptable terms.<sup>5</sup> It was a time of brinkmanship in the setting of trans-Atlantic privacy policy.

---

<sup>1</sup> Andrews 1999.

<sup>2</sup> Simitis was the world’s first ‘data protection’ commissioner in name and one of the pioneers of European regulatory policy in the field.

<sup>3</sup> Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (O.J. L 281, 23 November 1995, pp. 31–50); adopted 24 October 1995; hereinafter also termed ‘EU Directive’.

<sup>4</sup> Heisenberg 2005, pp. 2, 84.

<sup>5</sup> Andrews 1999; more generally, see Heisenberg 2005.

To begin this chapter with an episode highlighting tension may seem strange. International initiatives to protect privacy and personal data have involved considerable co-operation between countries. Initiatives of this kind have yielded agreements binding (legally and/or politically) on many nation states. Much of this chapter is about such agreements. Indeed, the trans-Atlantic dispute in the wake of adoption of the EU Directive ended up being patched over, at least temporarily, in the form of the ‘Safe Harbor’ scheme.<sup>6</sup> Yet the last 40 years of international work on privacy issues are as much a story about tensions and cleavage as about co-operation. There have been collisions between views about the value of privacy, the most appropriate means of safeguarding it, and, concomitantly, about who should foot the bill for its protection.

All of these types of collision figured in the dispute leading up to the Safe Harbor scheme. Simitis’ remark about bananas underlined that Europeans tend to view privacy not as a commodity but as a fundamental right deserving of rigorous and comprehensive legislative safeguards. In much of Europe, protection of privacy tends to be intimately tied to protection of dignity and honour. It is also often perceived as valuable not just for individual persons but society generally, particularly for maintaining civility, pluralism and democracy. Americans, however, tend to see privacy as important primarily in ensuring freedom from government intrusion.<sup>7</sup> They tend also to view privacy as an interest that is mainly, if not exclusively, valuable for individual persons *qua* individuals, and therefore often in tension with the needs of wider society.<sup>8</sup> Legislative safeguards for privacy in the USA have been less stringent than in Europe, especially regarding the private sector.<sup>9</sup> The relative laxity of US legislative safeguards is not just a symptom of cultural differences in the way privacy is valued; it reflects numerous factors, not least a paucity of first-hand domestic experience of totalitarian oppression in the USA – at least for the bulk of ‘white society’. In contrast, European legislative policy reflects the traumas from first-hand experience of such oppression. These traumas impart to that policy an anxiety and gravity – some would claim paranoia – largely missing in US policy.

Differences occur even at the terminological level. American discourse on the fears raised by the (mis)use of computer technology has tended to revolve around the term ‘privacy’. By contrast, European discourse has tended to employ the more colourless appellation ‘data protection’.

---

<sup>6</sup> See further p. 41 in this chapter.

<sup>7</sup> See generally Whitman 2004. See also, e.g., Eberle 2002 (elaborating on these differences in the context of German and US constitutional law).

<sup>8</sup> See generally Regan 1995, chapters 2 & 8 and references cited therein.

<sup>9</sup> See, e.g., Schwartz & Reidenberg 1996.

It is important to spell out these tensions and differences at the start, because they have shaped most of the international initiatives described here. This is not to say that similar tensions have been absent between other constellations of countries, but the tensions inherent in the USA–Europe relationship have generated most noise and had the greatest practical impact in shaping privacy policy at the international level. They are long-standing tensions unlikely to dissipate in the near future.<sup>10</sup>

One might have expected that tensions between Western liberal democracies on the one hand, and, on the other, states operating with quite different regimes for protecting human rights would dog the work on drafting international privacy and data protection agreements. However, the bulk of that work has largely been undertaken by Western liberal democracies alone. These states seem rarely to have engaged seriously with other countries on privacy issues specifically.

The dispute leading to the Safe Harbor scheme highlights too the tension between the legal-political power of international organisations and the ability of individual nation states to develop privacy policy on their own. Taken together, the international agreements described here have exercised great influence on regulatory regimes at the national (and sub-national) level. This influence has gradually strengthened. Not only has the number of such agreements grown but their provisions have become increasingly elaborate. At the same time, courts and committees have teased out ever more detailed data protection requirements from the relatively terse texts of treaties dealing with fundamental human rights. The overall result of this growth in regulatory density is clear: over the last 40 years, individual nation states have been increasingly unable to adopt privacy regimes as they alone see fit.

This increasing weight of the world is far from unique to the privacy field; international regulatory instruments generally are cutting ever greater swaths through areas once largely the preserve of national policy. Yet the exercise of influence in the privacy field has not been unidirectional, flowing only from the international to the national plane. National regulatory regimes have also inspired and shaped many international initiatives.

A profusion of actors have contributed to development of international privacy policy. In any brief history of this development, the natural tendency is to focus on the norms drafted by large organisations. However, policy has also been shaped by a small group of individual persons, who, on their own and together, have combined special expertise in the field with strong persuasive powers.<sup>11</sup> Prominent instances of such ‘policy entrepreneurs’ are Michael

---

<sup>10</sup> Further on these tensions, see, e.g., Charlesworth 2000; Reidenberg 2000; Swire & Litan 1998; Heisenberg 2005; Whitman 2004.

<sup>11</sup> See further Bennett 1992, pp. 127–129.

Kirby, Jan Freese, Alan Westin, Hans-Peter Gassmann, Spiros Simitis, Ulf Brühmann and Stefano Rodotà. While many of these people have exercised their influence when formally attached to an organisation, they have been able to make their mark over and above that connection. This was particularly possible in the 1970s and 1980s. In more recent years, relatively faceless organisations seem increasingly to drive policy development in the field.

There are many such organisations. The Council of Europe (CoE), the Organisation for Economic Cooperation and Development (OECD), the United Nations (UN) and the EU have for a long time played the main roles, though not always uniformly or at the same time. Other bodies, such as the International Labour Organisation (ILO), have made relatively marginal, though not insignificant, policy contributions.<sup>12</sup> In very recent years, the Asia-Pacific Economic Cooperation (APEC) has asserted itself as a potentially influential policy-broker in the field.

Beyond these organisations lies a vast array of bodies and interest groups which have pushed – and continue to push – particular privacy policies in an international context. Some are groups advocating relatively strong regimes for protection of personal data. Foremost of such bodies in the public sector are the regional groupings of national data protection authorities (Privacy Commissioners, Data Protection Commissioners and the like). These consist primarily of the Data Protection Working Party set up under Article 29 of the EU Directive,<sup>13</sup> the International Working Group on Data Protection and Telecommunications,<sup>14</sup> and the Asia-Pacific Privacy Authorities (APPA).<sup>15</sup> Of these, the Article 29 Working Party has been the most influential in shaping policy with transnational impact.<sup>16</sup>

Flanking these are civil society groups with strong pro-privacy agendas but relatively marginal impact on the formulation of major international agreements. Prominent examples of such bodies are the Electronic Privacy Information Center and Privacy International. Ranged usually against them are industry groups, such as the International Chamber of Commerce and the European Direct Marketing Association, determined to ensure that privacy safeguards do not unduly dent business interests. These groups were

---

<sup>12</sup> See the code of practice issued by the ILO on data privacy in the workplace: *Protection of Workers' Personal Data* (Geneva: ILO, 1997).

<sup>13</sup> See <[http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm)> (last accessed 15 February 2008).

<sup>14</sup> See <<http://www.datenschutz-berlin.de/doc/int/iwgdp/>> (last accessed 15 February 2008).

<sup>15</sup> See <<http://www.privacy.gov.au/international/appa/>> (last accessed 15 February 2008).

<sup>16</sup> See further p. 37 in this chapter.

particularly active lobbyists during the drafting of the EU Directive on data protection.<sup>17</sup>

In the course of the last 40 years, it has become clear that the major international declarations and treaties on fundamental human rights constitute the central formal normative basis for data protection norms.<sup>18</sup> Important in this regard are the Universal Declaration of Human Rights (UDHR),<sup>19</sup> the International Covenant on Civil and Political Rights (ICCPR)<sup>20</sup> along with certain regional human rights treaties, such as the European Convention on Human Rights and Fundamental Freedoms (ECHR).<sup>21</sup> However, of greater *practical* importance for the shaping of national regimes on privacy and data protection over the last four decades are certain agreements emanating from the Council of Europe, the OECD and the EU. The most influential of these agreements are the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,<sup>22</sup> the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,<sup>23</sup> and the EU Directive on data protection.

This chapter accordingly focuses on these latter agreements.

## COUNCIL OF EUROPE INITIATIVES

The Council of Europe<sup>24</sup> was one of the first international bodies to begin developing prescriptions for practice in response to the privacy threats posed by computer technology. It is also the first and only international body to have drafted a multilateral treaty dealing directly with protection of personal data.

---

<sup>17</sup> See generally Regan 1999.

<sup>18</sup> See further pp. 45–46 in this chapter.

<sup>19</sup> United Nations (UN) General Assembly resolution 217 A (III) of 10 December 1948.

<sup>20</sup> UN General Assembly resolution 2200A (XXI) of 16 December 1966; in force 23 March 1976.

<sup>21</sup> European Treaty Series (ETS) No. 5; opened for signature 4 November 1950; in force 3 September 1953.

<sup>22</sup> ETS No. 108; opened for signature 28 January 1981; in force 1 October 1985; hereinafter also termed 'CoE Convention'.

<sup>23</sup> OECD Doc. C(80)58/FINAL; adopted 23 September 1980; hereinafter also termed 'OECD Guidelines'.

<sup>24</sup> The Council of Europe is an intergovernmental organisation established in 1949, with headquarters in Strasbourg. It currently encompasses 47 states from the Greater European region. Amongst its chief aims are the achievement of greater unity amongst its members, and promotion of human rights, democracy and rule of law. In furtherance of those aims, it has adopted some 200 various treaties and an even greater number of recommendations and declarations.

This is the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. As of 15 February 2008, the Convention had been signed by 43 of the 47 CoE member countries and ratified by 38 of them.<sup>25</sup> Although a European product, it is envisaged to be potentially more than an agreement between European states. Accordingly, it may be ratified by states not belonging to the Council of Europe (see Article 23). However, this possibility has yet to be exploited. At the same time, the EU – or, more accurately, European Communities (EC) – has long signalled a wish to become a party to the Convention. Amendments to the Convention were adopted in June 1999 in order to permit accession by the EC but are not yet in force.<sup>26</sup>

The Convention is based partly on resolutions and recommendations emanating from the Council in the late 1960s and early 1970s. Most noteworthy of these are two resolutions adopted by the CoE Committee of Ministers: Resolution (73)22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector (adopted 26 September 1973), and Resolution (74)29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector (adopted 24 September 1974). The annexes to each resolution contain broadly similar sets of data protection principles, drawing inspiration from German, Swedish, Belgian and US legislative initiatives.

Work on the resolutions and the subsequent Convention arose out of a view that the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms did not provide sufficient protection for individuals in the face of computerised processing of personal data, particularly in the private sector.<sup>27</sup> Also important was the absence in many CoE member states of adequate laws to provide such protection. It was hoped that the resolutions

---

<sup>25</sup> Ratifying states are Albania, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Macedonia, Malta, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland and the United Kingdom (UK). Five member countries have signed the Convention but not yet ratified it: Andorra, Moldova, Russia, Turkey and Ukraine. Four member countries have not yet signed the Convention: Armenia, Azerbaijan, Monaco and San Marino.

<sup>26</sup> See Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) allowing the European Communities to accede. The amendments will enter into force on the thirtieth day after approval by all of the Convention Parties (Article 21(6) of the Convention). As of 15 February 2008, not all Parties had registered their approval.

<sup>27</sup> See, e.g., Hondius 1975, pp. 65–66 and references cited therein.

and the Convention would stimulate the creation of such laws.<sup>28</sup> A related object was to prevent legal divergence, thereby promoting the Council's general goal of achieving greater unity between its members.<sup>29</sup>

For the purposes of the Convention, this harmonisation was – and remains – not only to strengthen data protection and thereby the right 'to respect for private life' pursuant to ECHR Article 8, but, somewhat paradoxically, to ensure also the free flow of personal data across national borders and thereby safeguard the right in ECHR Article 10 'to receive and impart information and ideas without interference by public authority and regardless of frontiers'.<sup>30</sup> The need to harmonise national laws in order to maintain free flow of data across borders arose in the latter half of the 1970s in the wake of a growing number of European countries passing data protection legislation that expressly restricted data flow to countries without similar laws. The primary aim of such restrictions has been to hinder data controllers from avoiding the requirements of the legislation by shifting data-processing operations to countries with more lenient standards.<sup>31</sup>

While this aim is entirely legitimate, its practical realisation could seriously impede the realisation of other, at least equally legitimate, interests. Moreover, 'outsiders' could perceive such restrictions as serving a less legitimate agenda: economic protectionism.<sup>32</sup> Not surprisingly, then, work on the Convention has been informed by a desire to minimise the potential risks that such restrictions represent but without unduly compromising privacy interests. This desire has also informed work on most of the other main international agreements in the field.

---

<sup>28</sup> Thus, Article 1 of the Convention stipulates as a basic object 'to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")'.

<sup>29</sup> In this respect, note the Convention's Preamble ('Considering that the aim of the Council of Europe is to achieve greater unity between its members . . .'). See too *Explanatory Report on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Strasbourg: CoE, 1981 – hereinafter 'Explanatory Report'), para. 21.

<sup>30</sup> See the Preamble, which states that the goal of extending data protection is to be balanced with a 'commitment to freedom of information regardless of frontiers', and recognises 'that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples'. See further Article 12 of the Convention dealt with below.

<sup>31</sup> See generally Ellger 1990, pp. 87ff and references cited therein.

<sup>32</sup> See, e.g., the allegations directed at early European privacy legislation in Eger 1978; McGuire 1979–80; and Pinegar 1984.

The Convention is intended primarily to cover computerised ('automated') processing of data on physical persons in both the private and public sectors (including police and national security agencies). Nevertheless, contracting states are expressly permitted to apply the Convention's principles to information on corporate and/or collective entities (Article 3(2)(b))<sup>33</sup> and to data processed manually (Article 3(2)(c)). Moreover, a party to the Convention is free 'to grant data subjects a wider measure of protection than that stipulated in this convention' (Article 11).

While the Convention requires contracting states to incorporate its principles into their domestic legislation (Article 4(1)), it does not provide, of itself, a set of rights directly enforceable in courts.<sup>34</sup> The CoE wanted the Convention to be a catalyst and guide for national legislative initiatives; it did not want to short-circuit these initiatives by providing a finished package of directly applicable rules.<sup>35</sup>

The heart of the Convention lies in Chapter II which sets out, in broad-brush fashion, basic principles for processing personal data. As intimated above, these principles were hardly ground-breaking at the time of the Convention's adoption. They embody a common minimum of the standards already promulgated in the CoE resolutions and in an increasingly large number of laws passed by member states. Nonetheless, when set down in the Convention, they established a key reference point for subsequent elaborations of principles in both international and national codes. The principles may be summed up in the following terms:

- Fair and lawful processing – personal data 'shall be obtained and processed fairly and lawfully' (Article 5(a));
- Purpose specification – personal data shall be stored for 'specified and legitimate purposes and not used in a way incompatible with those purposes' (Article 5(b));
- Minimality – the amount of personal data collected and stored shall be limited to what is necessary for achieving the purpose for collection/storage (Article 5(c) and (e));
- Adequate information quality – personal data shall be 'adequate', 'accurate' and 'relevant' in relation to the purposes for which they are processed (Article 5(c) and (d));

---

<sup>33</sup> A possibility currently exploited by Albania, Austria, Italy, Liechtenstein and Switzerland. Denmark, Norway and Iceland exploited this possibility in their first data protection laws but have largely dispensed with express protection of data on collective entities under their current legislation, except in relation to credit reporting. See generally Bygrave 2002, part III.

<sup>34</sup> Explanatory Report, para. 38; see also para. 60.

<sup>35</sup> Simitis 1990, pp. 9–10; Henke 1986, pp. 57–60; Hondius 1983, p. 116.

- Sensitivity – certain kinds of personal data (notably those concerning a person’s ‘health or sexual life’, their ‘racial origin, political opinions, religious or other beliefs’, or their ‘criminal convictions’) ought to be subject to more stringent protection on account of their sensitivity (Article 6);
- Security – ‘appropriate security measures’ shall be taken to protect personal data ‘against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination’ (Article 7);
- Transparency – any person shall be able to
  - (i) ascertain ‘the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file’ (Article 8(a)); and
  - (ii) ‘to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data files as well as communication to him of such data in an intelligible form’ (Article 8(b)).
- Rectification – any person shall be able to have data about them rectified or erased if the data have been processed in breach of rules implementing Articles 5 and 6 of the Convention (Article 8(c)).

The principles are not absolute. Article 9(2) permits departure from them when this

is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

- a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
- b. protecting the data subject or the rights and freedoms of others.

Rules on transborder data flow constitute another crucial element of the Convention. These are contained in Chapter III and govern the flow of personal data between states that are parties to the Convention. The basic rule is that a state party shall not restrict flows of personal data to the territory of another state party unless the latter fails to provide ‘equivalent protection’ for the data (Article 12(2) and (3)(a)).

A major gap in Chapter III is the absence of rules for the flow of personal data from a party to non-party state. Initially of small significance, this gap became increasingly anachronistic, particularly after 1995 when the EU adopted its Directive on data protection laying down extensive rules on flow of personal data from EU member states to other countries. In 2001, the CoE remedied the anomaly by adopting an Additional Protocol to the Convention

with provisions on data flow from party to non-party states.<sup>36</sup> These provisions (set out in Article 2) follow the broad thrust of the equivalent provisions of the EU Directive.<sup>37</sup>

The same Protocol fills other gaps too. Although the Convention contains fairly detailed provisions envisaging both establishment of authorities to help oversee implementation of the Convention and a high level of co-operation between these authorities (see Articles 13–17), it falls short of mandating that each contracting state establish a special control body in the form of a data protection authority or the like.<sup>38</sup> It also fails to specify minimum requirements regarding the competence and independence of such an authority. Again, these gaps became increasingly anomalous, particularly after adoption of the EU Directive, which requires each EU member state to establish one or more data protection authorities and prescribes in detail their independence, competence and various functions.<sup>39</sup> Article 1 of the Protocol stipulates broadly similar requirements.

Although the Protocol plugs some gaps, others remain. For instance, the Convention does not specifically deal with the issue of choice/collision of laws – that is, which state’s law shall apply to a given data-processing operation. Neither does the Convention set up a body specifically charged with overseeing and enforcing its implementation. This omission is mitigated somewhat by the provision in Chapter V for establishing a Consultative Committee (consisting primarily of state party representatives) which is charged with developing proposals to improve application of the Convention.<sup>40</sup>

---

<sup>36</sup> Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows (ETS No. 181); open for signature 8 November 2001; in force 1 July 2004. As of 15 February 2008, 18 CoE member countries have ratified the Protocol. They are: Albania, Bosnia and Herzegovina, Croatia, Cyprus, the Czech Republic, France, Germany, Hungary, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania, the Slovak Republic, Sweden and Switzerland. The Protocol is, or will soon be, in force in all of these countries. Fifteen countries have signed the Protocol but not yet ratified it. They are: Andorra, Austria, Belgium, Denmark, Finland, Greece, Iceland, Ireland, Italy, Macedonia, Norway, Russia, Turkey, Ukraine and the UK. Fourteen member countries have not yet signed the Protocol: Armenia, Azerbaijan, Bulgaria, Estonia, Georgia, Liechtenstein, Malta, Moldova, Monaco, Montenegro, San Marino, Serbia, Slovenia and Spain.

<sup>37</sup> The latter provisions are described on pp. 31–39 of this chapter.

<sup>38</sup> See also the Convention’s Explanatory Report, para. 73.

<sup>39</sup> See further pp. 31–39 in this chapter.

<sup>40</sup> The Committee was responsible for drafting, *inter alia*, the 1999 Amendments allowing EC accession and the 2001 Additional Protocol.

Still other problems afflict implementation of the Convention. The Chapter II principles are formulated in a general, abstract way and many key words are left undefined – also by the Convention's Explanatory Report. While this has certain advantages, the diffuseness of the principles detracts from their ability to harmonise the laws of the contracting states. This weakness is exacerbated by the Convention otherwise permitting discretionary derogation on numerous significant points (see, for example, Articles 3, 6 and 9). This, in turn, has undermined the ability of the Convention to guarantee the free flow of personal data across national borders.<sup>41</sup> At the same time, the abstract nature of the principles undercuts their ability to function as practical 'rules for the road' in concrete situations.

Addressing this latter problem are a long series of CoE recommendations dealing specifically with data processing in particular sectors, such as telecommunications,<sup>42</sup> medical research<sup>43</sup> and insurance.<sup>44</sup> These recommendations usefully supplement the general principles of the Convention. Though not legally binding, the recommendations have strong persuasive force, especially as they are drafted with participation from all member states. Their authority is reflected in the fact that when they are adopted, individual member states frequently issue reservations on points of contention. The recommendations are also highly influential on the policies and practices of national data protection authorities.

Furthermore, the CoE has adopted a range of other instruments which, whilst directly concerning issues other than privacy, indirectly promote privacy-related interests. An important example is the 1997 Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine,<sup>45</sup> which contains several provisions (in Article 10) on data protection with respect to health information.

Hence, while the 1981 Convention is, in many respects, the Council of Europe's crowning achievement in the field of privacy and data protection, the Council has gone on to generate a large number of other instruments relevant

---

<sup>41</sup> See further, e.g., the case study in Nugter 1990, chapter VIII (showing that, as of 1990, the Convention had failed to establish more than a minimal, formal equivalence between the national data protection laws of the Federal Republic of Germany, France, the UK and the Netherlands).

<sup>42</sup> See Recommendation No. R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (adopted 7 February 1995).

<sup>43</sup> See, e.g., Recommendation No. R(97) 5 on the protection of medical data (adopted 13 February 1997).

<sup>44</sup> See Recommendation No. R(2002) 9 on the protection of personal data collected and processed for insurance purposes (adopted 18 September 2002).

<sup>45</sup> ETS No. 164; adopted 4 April 1997; in force 1 December 1999.

to the field. Many of these have considerably more practical bite in their respective areas of application than does the Convention. Nonetheless, the Convention is far from *passé*. It continues to be a key reference point for shaping regulatory policy – also outside the CoE framework. This is evidenced, for example, in recent use of the Convention as a benchmark in development of EU data protection rules for policing and judicial co-operation.<sup>46</sup>

## OECD INITIATIVES

The Organisation for Economic Cooperation and Development<sup>47</sup> began taking an interest in privacy and data protection issues not long after the Council of Europe. In the early 1970s, the OECD commissioned several reports on these issues as part of a series of ‘Informatics Studies’.<sup>48</sup> Later in that decade it began work – in close liaison with the CoE – on drafting its own regulatory code. These efforts bore fruit in the form of guidelines published in 1980 bearing the title *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. The core of the Guidelines are a set of eight data privacy principles intended to apply to manual and electronic processing of personal data in both the private and public sectors (including police and national security agencies).

The Guidelines are not legally binding on OECD member states. Their publication was simply accompanied by an OECD Council Recommendation stating that account be taken of them when member countries develop domestic legislation on privacy protection. Significantly, the recommendation also

---

<sup>46</sup> See, e.g., Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (O.J. L 63, 6 March 2002, pp. 1–13), Article 14(2) and recital 9. Eurojust is an EU body set up in 2002 to co-ordinate efforts by EU member states’ judicial authorities in countering serious crime.

<sup>47</sup> The OECD is an intergovernmental organisation established in 1961 with headquarters in Paris. It grew out of the Organisation for European Economic Cooperation set up in 1948 to administer the Marshall Plan. The OECD currently encompasses 30 member states from around the globe, the bulk of which are advanced industrial nations: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the UK and USA. As its name suggests, the organisation’s primary aim is to foster economic growth and co-operation, including expansion of free trade, though its mandate also involves facilitating development of international policy on a broad range of social, technological and environmental issues.

<sup>48</sup> See, e.g., Niblett 1971.

stressed that member countries should 'endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder data flows of personal data'.

According to Justice Michael Kirby, who headed the expert group responsible for drafting the Guidelines, the work of the OECD in the field was motivated primarily by economic concerns:

It was the fear that local regulation, ostensibly for privacy protection, would, in truth, be enacted for purposes of economic protectionism, that led to the initiative of the OECD to establish the expert group which developed its Privacy Guidelines. The spectre was presented that the economically beneficial flow of data across national boundaries might be impeded unnecessarily and regulated inefficiently producing a cacophony of laws which did little to advance human rights but much to interfere in the free flow of information and ideas.<sup>49</sup>

Nevertheless, the Guidelines urge member states to take legal measures for 'the protection of privacy and individual liberties' (see especially paras 2 and 6). Despite the difference in the traditional focus of the OECD from that of the CoE, the chief privacy codes of both organisations expound broadly similar principles. The similarities are due partly to the extensive co-operation that took place between the bodies charged with drafting the two codes.<sup>50</sup> In terms of content as opposed to status, the most conspicuous difference between the codes is their respective provisions on implementation and international co-operation. These provisions are much more developed in the CoE Convention than in the Guidelines. The Convention's core data protection principles go further than the Guidelines in numerous respects. For instance, unlike the Convention, the Guidelines do not contain specific requirements on the destruction or anonymisation of personal data after a certain period. Neither do they specifically mention the need for special safeguards for certain kinds of sensitive data.

Nonetheless, the Guidelines are themselves described as 'minimum standards . . . capable of being supplemented by additional measures for the protection of privacy and individual liberties' (para. 6; see too para. 3). Indeed, the Guidelines are broader than the Convention on some points. For example, the Guidelines cover, as a point of departure, manual data processing in addition to computerised processing. Further, they embody an 'Openness Principle' (para. 12) more broadly formulated than Article 8 of the Convention.

---

<sup>49</sup> Kirby 1991, pp. 5–6.

<sup>50</sup> See para. 14 of the Convention's Explanatory Report and para. 20 of the Guidelines' Explanatory Memorandum. See also Hondius 1983, p. 112; Seip 1995.

Part 3 of the Guidelines contains principles dealing with data flows between member states. The principles are essentially the same as the equivalent provisions in Article 12 of the Convention. However, paragraph 18 of the Guidelines is of more general application and serves to underline the pronounced concern of the OECD with facilitating commerce:

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

Like the CoE Convention (as originally adopted), the Guidelines neither recommend nor require that countries establish data protection authorities.<sup>51</sup> Neither do they contain provisions dealing directly with choice/conflict of laws – again like the Convention. Yet the Guidelines go a step further than the Convention by urging member states to ‘encourage and support self-regulation, whether in the form of codes of conduct or otherwise’ (para. 19(b)).

Although not legally binding, the Guidelines have been highly influential on the enactment and content of data protection legislation in countries outside Europe, particularly Japan, Australia, New Zealand, Canada and Hong Kong.<sup>52</sup> Moreover, the APEC Privacy Framework of 2004/2005 touts the Guidelines as a significant source of inspiration.<sup>53</sup>

Since 1980, the OECD has adopted a range of other guidelines on privacy-related matters. These deal with information security,<sup>54</sup> cryptography policy,<sup>55</sup> and consumer protection in electronic commerce.<sup>56</sup> The OECD has also issued a declaration on privacy protection on global networks,<sup>57</sup> along with a recommendation on international co-operation in enforcement of privacy laws.<sup>58</sup>

---

<sup>51</sup> See further para. 70 of the Guidelines’ Explanatory Memorandum.

<sup>52</sup> See further the chapters in this volume dealing with Australia and Hong Kong.

<sup>53</sup> See further pp. 43–44 in this chapter.

<sup>54</sup> Guidelines for the Security of Information Systems (C(92)188/FINAL; adopted 26 November 1992); since replaced by Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (adopted 25 July 2002).

<sup>55</sup> Guidelines for Cryptography Policy (C(97)62/FINAL; adopted 27 March 1997).

<sup>56</sup> Guidelines for Consumer Protection in the Context of Electronic Commerce (adopted 9 December 1999).

<sup>57</sup> Declaration on the Protection of Privacy on Global Networks (C(98)177, Annex 1; issued 8–9 October 1998).

<sup>58</sup> Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (adopted 12 June 2007).

While the bulk of these initiatives develop OECD information policy along new avenues, each of them pays deference to the 1980 Guidelines and reaffirms their vision.

## UN INITIATIVES

The UN General Assembly adopted a set of Guidelines on privacy and data protection in resolution 45/95 of 14 December 1990.<sup>59</sup> Work on the Guidelines was rooted primarily in human rights concerns; commercial anxieties about restrictions on transborder data flows apparently took a back seat.<sup>60</sup>

The first UN initiative dealing directly with privacy and data protection was a 1968 General Assembly Resolution inviting the UN Secretary-General to examine the impact of technological developments on human rights, including consideration of individuals' right to privacy 'in the light of advances in recording and other techniques'.<sup>61</sup> The resulting study by the Secretary-General led to the publication of a report in 1976 urging states to adopt privacy legislation covering computerised personal data systems in the public and private sectors, and listing minimum standards for such legislation.<sup>62</sup> The 1990 Guidelines essentially repeat and strengthen this call. Their adoption underlines that privacy and data protection have ceased to be exclusively a 'First World', Western concern.

The Guidelines are two-pronged: one prong lays down 'minimum guarantees' for inclusion in national laws (Part A). These guarantees apply to 'all public and private computerized files', though states are also given the express option to extend application to manual files and to data on legal persons (para. 10).

The other prong aims at encouraging international organisations – both governmental and non-governmental – to process personal data in a privacy-friendly manner (Part B). This is a particularly progressive element of the Guidelines not specifically found in the CoE Convention, OECD Guidelines or EU Directive. Other progressive elements are present, too. The 'principle of

---

<sup>59</sup> Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72, 20 February 1990) – hereinafter also termed 'UN Guidelines'.

<sup>60</sup> On the background to the Guidelines, see generally Michael 1994, pp. 21–26.

<sup>61</sup> UN General Assembly Resolution 2450 of 19 December 1968 (Doc E/CN.4/1025).

<sup>62</sup> See *Points for Possible Inclusion in Draft International Standards for the Protection of the Rights of the Individual against Threats Arising from the Use of Computerized Personal Data Systems* (Doc E/CN.4/1233). Cf. Doc E/CN.4/1116 dealing more generally with surveillance technology.

accuracy' in the UN Guidelines emphasises the duty of data controllers to carry out *regular* checks of the quality of personal data (para. 2), whereas the equivalent provisions in the OECD Guidelines, CoE Convention and EU Directive make no mention of this obligation. Arguably, though, such a duty may be read into the provisions of the Directive. To take another example, the UN Guidelines uphold the need for national data protection authorities to be impartial, independent and technically competent (para. 8). This is a point upon which the OECD Guidelines and CoE Convention (minus Additional Protocol) are silent, though not the EU Directive (*viz.* Article 28).

The UN Guidelines seek to regulate data flows between a broader range of countries than do the equivalent provisions of the CoE Convention and OECD Guidelines. At the same time, they employ slightly different formulations of the criteria for restricting such flows (para. 9):

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only insofar as the protection of privacy demands.

Both 'comparable' and 'reciprocal' are more diffuse and confusing than the criterion of 'equivalent' protection used in the CoE Convention and OECD Guidelines. It is probable, though, that paragraph 9 seeks to apply essentially the same standards as the latter. Despite their progressive character, the UN Guidelines appear to have had a lower public profile and practical impact than the majority of the other main international codes on point.<sup>63</sup> At least part of the problem arises from the absence in the Guidelines of definitions of key terms. Even central concepts such as 'personal data' and 'personal data file' remain undefined. Such omissions diminish considerably the Guidelines' practical utility.

## EU INITIATIVES

The European Union and its older related bodies (primarily the European Economic Community and European Community (EC)) were slower off the mark than the Council of Europe, OECD and UN to develop privacy codes. However, the instruments eventually adopted within the EU/EC framework have been the most ambitious, comprehensive and complex in the field. The key text is Directive 95/46/EC. Since its adoption in 1995, it has constituted

---

<sup>63</sup> See further, e.g., Bygrave 2002, p. 33 and references cited therein.

the most important point of departure for national privacy and data protection initiatives within the EU – and often outside Europe as well.

The Directive gave EU member states until 24 October 1998 to bring their respective legal systems into conformity with its provisions (Article 32(1)). National implementation of the Directive was also a prerequisite for the subsequent accession to the EU of 12, largely East European states in respectively 2004 and 2007.<sup>64</sup> Moreover, the Directive has been incorporated into the 1992 Agreement on the European Economic Area (EEA) such that states which are not EU members but are party to the EEA Agreement (that is, Norway, Iceland and Liechtenstein) are legally bound to bring their respective laws into conformity with the Directive. The Directive has also exercised considerable influence over other countries outside the EU not least because it prohibits (with some qualifications) the transfer of personal data to these countries unless they provide 'adequate' levels of data protection.

The adoption of the Directive is the culmination of a series of proposals, strung over two decades. The main impetus initially came from the European Parliament (EP) which made repeated calls for drawing up a data protection Directive and for EU member states to sign and ratify the CoE Convention.<sup>65</sup> The European Commission, along with the Council of Ministers, initially acted much more slowly, with their energies directed primarily to fostering development of the internal market and a European computer industry.<sup>66</sup>

The Commission issued its first proposal for a data protection Directive in 1990,<sup>67</sup> but it took another five years of intensive bargaining before the Directive was finally adopted.<sup>68</sup> The extensive tugs-of-war between various member states, organisations and interest groups during the drafting process

---

<sup>64</sup> The Slovak Republic, Czech Republic, Malta, Poland, Hungary, Lithuania, Latvia, Estonia, Slovenia, and Cyprus joined the EU in 2004; Bulgaria and Romania joined in 2007. The other EU member states comprise Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden and the United Kingdom.

<sup>65</sup> See, e.g., EP Resolution of 21 February 1975 on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing (O.J. C 60, 13 March 1975, p. 48); EP Resolution of 8 May 1979 on the protection of the rights of the individual in the face of technical developments in data processing (O.J. C 140, 5 June 1979, pp. 34–38); EP Resolution of 9 March 1982 on the protection of the rights of the individual in the face of technical developments in data processing (O.J. C 87, 5 April 1982, pp. 39–41).

<sup>66</sup> See generally Kirsch 1982, pp. 34–37; Geiger 1989; Ellger 1991a, pp. 59–61.

<sup>67</sup> See Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (COM(90) 314 final – SYN 287; O.J. C 277, 5 November 1990, p. 3).

<sup>68</sup> For overviews of some of the political manoeuvring that occurred in the lead-up to the Directive's adoption, see Platten 1996, pp. 23–32; Simitis 1995.

resulted in a text that is nebulous, dense and somewhat ambivalent in its general policy thrust.

On the one hand, the Preamble to the Directive expresses concern to promote realisation of the internal market of the EU, in which goods, persons, services, capital and, concomitantly, personal data are able to flow freely between member states.<sup>69</sup> To further this concern, the Directive seeks to harmonise member states' respective privacy laws. On the other hand, the Directive also emphasises the importance of protecting privacy in the face of technological and economic developments.<sup>70</sup> Indeed, it was the first EU Directive to expressly accord protection of human rights a prominent place. As such, it reflects and reinforces the gradual incorporation of law and doctrine on human rights into the EU legal system.<sup>71</sup>

The ambivalence in aims is not unique. It is manifest in many of the other agreements on privacy and data protection presented in this chapter. However, the Directive is unique in that it proscribes restrictions on the flow of personal data between EU member states on the grounds of protection of privacy and other basic human rights (Article 1(2)). This absolute prohibition could be construed as evidence that the Directive is ultimately concerned with realising the effective functioning of the EU's internal market, and only secondarily with human rights. Nevertheless, the Directive strives to bring about a 'high' level of data protection across the EU (recital 10), and it seeks not just to 'give substance to' but 'amplify' the CoE Convention (recital 11). Thus, the Directive does more than establish a 'lowest common denominator' of rules found in member states' existing laws.

The European Court of Justice (ECJ) has confirmed that the Directive is rooted in more than simply concern to promote the internal market and has as one of its main goals the protection of fundamental human rights.<sup>72</sup> The Court has further held (in the same judgments) that interpretation of the Directive must turn partly on relevant case law from the European Court of Human Rights pursuant to the ECHR.

---

<sup>69</sup> See especially recitals 3, 5, 7. The need to ensure free flow of personal data throughout the EU is not rooted entirely in commercial considerations; the pan-EU ambit of government administration also plays a role (see, e.g., recital 5).

<sup>70</sup> See, e.g., recitals 2, 3, 10, 11.

<sup>71</sup> See especially Title I, Articles 6(1) and 6(2) of the 1992 Treaty on European Union (as amended); the Charter of Fundamental Human Rights of the European Union, adopted 7 December 2000 (O.J. C 364, 18 December 2001, pp. 1–22); and Articles 1–2, I–9 and Part II of the Treaty establishing a Constitution for Europe, adopted 29 October 2004 but not yet in force (O.J. C 310, 16 December 2004, pp. 1–474).

<sup>72</sup> Judgment of 20 May 2003 in Joined Cases C-465/00, C-138/01, and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989; judgment of 6 November 2003 in Case C-101/01 *Bodil Lindqvist* [2003] ECR I-129711.

Also noteworthy is the growing recognition in the EU that data protection is in itself (that is, distinct from a broader right to privacy) a basic human right. This is evidenced in the EU's Charter of Fundamental Human Rights and its proposed Constitution, both of which contain separate provisions on data protection and privacy protection respectively.<sup>73</sup>

The Directive embodies a profoundly European vision of what protection of privacy and personal data should involve. It lays down a relatively broad and rigorous set of rules to safeguard what it sees as fundamentally important rights. Part of this rigour lies in its detailed specification of a baseline for data protection from which EU member states cannot depart. The Directive introduces, for instance, not just a simple requirement that member states establish independent authorities to monitor and enforce their data protection laws; it specifies a large number of attributes for such authorities.

Nevertheless, in its baseline specifications, the Directive also affords member states a 'margin for manoeuvre' (recital 9). This is manifest in Article 5 which provides that 'Member States shall, within the limits of the provisions of [Chapter II] determine more precisely the circumstances in which the processing of personal data is lawful'. This margin for manoeuvre is a natural consequence of the Directive's basic nature *qua* Directive (as opposed to Regulation).<sup>74</sup> It reflects also the principle of subsidiarity that generally informs EU regulatory policy.<sup>75</sup> And it reflects the extensive controversy accompanying the Directive's gestation.

In 1995, Spiros Simitis made some telling observations of EU member states' attitudes during the lengthy gestation of the Directive:

Experience has shown that the primary interest of the Member States is not to achieve new, union-wide principles, but rather to preserve their own, familiar rules. A harmonization of the regulatory regimes is, therefore, perfectly tolerable to a Member State as long as it amounts to a reproduction of the State's specific national approach.<sup>76</sup>

---

<sup>73</sup> See Charter of Fundamental Rights of the European Union, *supra* n. 72, Article 8 (providing for a right to protection of personal data); cf. Article 7 (providing for the right to respect for private and family life). See also the right to protection of personal data in Articles I-51 and II-68 of the Treaty establishing a Constitution for Europe, *supra* n. 71.

<sup>74</sup> Basically, a Directive requires achievement of a specified result, leaving member states some discretion as to how to achieve the result. A Regulation, however, does not provide any such discretion. Further on the differences between Directives and Regulations, see, e.g., Craig & de Búrca 2008, pp. 83–85.

<sup>75</sup> See Treaty on establishing the European Community (hereinafter 'EC Treaty'), Article 5. The principle of subsidiarity essentially means that the EU and its institutions shall only take action when the objectives of such action cannot be more effectively achieved by member states alone.

<sup>76</sup> Simitis 1995, p. 449.

Over a decade later, his observations are just as pertinent. Evidence abounds of considerable divergence between member states' respective laws.<sup>77</sup> Particularly problematic from an international perspective is that national implementation of the provisions in the Directive regulating flow of data to countries outside the EU (see Articles 25–26, dealt with further below) has varied broadly. Indeed, it has sometimes been inconsistent with the Directive.<sup>78</sup>

The Directive applies to personal data processing in both the private and public sectors. Processing of data on collective entities (private corporations etc.) falls outside its scope, though the Directive does not prohibit member states' privacy laws applying to such data. While most member states' laws are limited to safeguarding data on natural persons, several (for example, the laws of Austria and Italy) safeguard data on collective entities as well.<sup>79</sup> Moreover, in a subsequent Directive from 2002 dealing with privacy and electronic communications, the EU expressly permits some safeguards of corporate privacy interests in the electronic communications context.<sup>80</sup>

The Directive does not apply to data processing carried out as part of activities falling beyond the ambit of EC law as such.<sup>81</sup> This includes activities relating to 'public security, defence, State security (including the economic well-being of the State where such processing relates to State security matters) and the activities of the State in areas of criminal law' (Article 3(2)). Also exempt is the processing of data 'by a natural person in the course of a purely personal or household activity' (Article 3(2)).<sup>82</sup> Member states are additionally required to lay down exemptions from the central provisions of the Directive with respect to data processing 'carried out solely for journalistic purposes or the purpose of artistic or literary expression', insofar as is 'necessary to reconcile the right to privacy with the rules governing freedom of expression' (Article 9).

<sup>77</sup> European Commission 2003; Korff 2002; Charlesworth 2003.

<sup>78</sup> European Commission 2003.

<sup>79</sup> See generally Bygrave 2002, part III.

<sup>80</sup> See further Directive 2002/58/EC dealt with further below.

<sup>81</sup> There is, strictly speaking, a distinction between EC law and EU law. The former covers primarily matters pertaining to the internal market; it does not extend to police and judicial co-operation in criminal matters or to common foreign and security policy. The latter range of matters falls, however, under two other 'pillars' of the EU system. See further Treaty on European Union, signed 7 February 1992; in force 1 November 1993.

<sup>82</sup> The ECJ has recently ruled that the latter exemption does not apply to processing of personal data 'consisting in publication on the internet so that those data are made accessible to an indefinite number of people': *Lindqvist* decision, *supra* n. 72, para. 47.

The Directive is the first and only international privacy code to tackle directly the vexed issue of which national law is applicable to a given case of data processing. Article 4(1) specifies the applicable law as that of the member state in which the data controller<sup>83</sup> is established. More controversially, the Directive also provides for the law of an EU state to apply outside the EU in certain circumstances – most notably where a data controller, based outside the EU, utilises ‘equipment’ located in the state to process personal data for purposes other than merely transmitting the data through that state (Article 4(1)(c)).<sup>84</sup>

The basic principles in the Directive parallel those laid down in the other international codes, especially the CoE Convention. Yet many of the principles in the Directive go considerably further than those in the other codes. For instance, Articles 10 and 11 require data controllers to directly provide data subjects with basic information about the scope of data-processing operations, independently of the data subjects’ use of access rights. None of the other main international data privacy instruments stipulate such requirements directly. Article 12 provides data subjects with access and rectification rights similar to, but more extensive than, the equivalents found in the other international codes. Especially innovative is the right of a person to obtain ‘knowledge of the logic involved in any automated processing of data concerning him . . .’ (Article 12(a)).<sup>85</sup>

Also innovative is Article 15(1), which grants a person the right

not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.<sup>86</sup>

Arguably, this right adds to the catalogue of core data protection principles a new principle – namely that fully automated assessments of a person’s character should not form the sole basis of decisions that impinge upon the person’s interests. The right is not absolute; a person may be subjected to such decisions if they are, in summary, taken pursuant to a contract with the data

---

<sup>83</sup> That is, the person or organisation who/which determines the purposes and means of processing personal data (Article 2(d)).

<sup>84</sup> See further, e.g., Kuner 2007, chapter 3; Charlesworth 2003, pp. 948–951.

<sup>85</sup> A right inspired by roughly similar provisions in French legislation (*viz.*, Act no. 78-17 on Data Processing, Data Files and Individual Liberties (as amended), Article 39(I)(5)).

<sup>86</sup> A right also inspired by roughly similar provisions in the French legislation, *op cit.*, Article 10. For further analysis of Article 15 in the Directive, see Bygrave 2002, pp. 319–328.

subject or authorised by law, and provision is made for 'suitable measures' to safeguard the person's 'legitimate interests' (Article 15(2)).

At the same time, the Directive empowers member states to restrict the scope of many of the general rights and obligations it sets down, when the restriction is 'necessary' to safeguard, *inter alia*, national security, public security, law enforcement and/or 'important' economic or financial interests of the member states (Article 13(1)). These exemptions grant member states extensive freedom to legitimise surveillance at the expense of individuals' privacy interests. They also lay the way open for significant disparities between the privacy laws of the various member states.

Other special aspect of the Directive are its relatively elaborate provisions on monitoring and supervisory regimes. Article 28 requires each member state to establish one or more 'supervisory authorities' to monitor and help enforce the national law on point. These authorities are to 'act with complete independence in exercising the functions entrusted to them' (Article 28(1)). In order to enhance the authorities' control and monitoring capability, the Directive requires, with some exceptions, that data controllers or their representatives notify the authority concerned of 'any wholly or partly automatic processing operation' they intend to undertake (Article 18(1)). The Directive also allows for a system of 'prior checking' by data protection authorities of processing operations that 'are likely to present specific risks to the rights and freedoms of data subjects' (Article 20(1)). The Directive fails to clarify what such a system practically entails though does state that such a system is to apply only to a minor proportion of data-processing operations (recital 54). The Directive does not directly specify that supervisory authorities may, pursuant to such a system, stop a planned operation, but seems to envisage such an ability. Article 28(3) provides that data protection authorities generally are to have 'effective powers of intervention', including the ability to impose 'a temporary or definitive ban on processing'. Several EU/EEA member states operate with licensing schemes whereby the national data protection authority must formally approve certain types of data processing before the processing can proceed.<sup>87</sup>

Article 27 requires member states and the Commission to 'encourage' the drafting of sectoral codes of conduct, at national and/or Community level, in pursuance of implementing the measures contemplated by the Directive. Nothing is provided in Article 27 on the exact legal status of such codes.

The Directive envisages high levels of co-operation between the national data protection authorities in Europe. Member states' respective authorities

---

<sup>87</sup> See, e.g., Norway's Personal Data Act of 2000 section 33 which subjects, as a point of departure, planned processing of certain categories of sensitive information (such as information on racial origin, religion or criminal records) to licensing.

may, for example, exercise their powers in relation to a particular instance of data processing even when the national law applicable to the processing is that of another member state, and they are to 'cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information' (Article 28(6)). In this way, the Directive stimulates some internationalisation, at least within the EU/EEA, of supervisory regimes.

More important for this internationalisation process, however, is Article 29. This establishes a 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data'. The Article 29 Working Party is composed largely of representatives from each member state's data protection authority. Its chief task is to provide independent advice to the European Commission on a range of issues, including uniformity in the application of national measures adopted pursuant to the Directive, and privacy protection afforded by non-member states (Article 30).

Such a body is unique in the EU regulatory system and has proved to be a valuable asset. Despite having purely advisory competence, the Working Party has played an influential role in setting the Commission's agenda in privacy matters. This is due not least to the sheer industry of the body. Since beginning operations in January 1996, the Working Party has generated a wealth of reports, recommendations and opinions generally showing both insight and foresight.<sup>88</sup> It has been fairly quick to grapple with cutting-edge matters, such as biometrics and radio-frequency identification (RFID).<sup>89</sup> Yet as elaborated on below, its influence has been most felt internationally in the application of the Directive's provisions on data flow to countries outside the EU.

Also assisting the Commission on privacy matters is a Committee composed of representatives from the member states (Article 31). This 'Article 31 Committee' has legal power over the Commission. If it disagrees with a Commission proposal, the Council is to be given an opportunity to determine the proposal's fate (Article 31(2)).

The Directive specifies relatively strong controls on the transfer of personal data to countries outside the EU (so-called 'third countries'). The basic rule is that transfer is permitted 'only if . . . the third country in question ensures an adequate level of protection' (Article 25(1)). No other international code goes so far as to proscribe flow of personal data to states not offering a particular level of data protection.

---

<sup>88</sup> See further <[http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2007\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm)> (last accessed 15 February 2008).

<sup>89</sup> See, e.g., Working Document on data protection issues related to RFID technology (January 2005, WP 105); Working Document on biometrics (August 2003; WP 80).

Article 25(2) stipulates that the adequacy criterion cannot be fleshed out in the abstract but ‘. . . in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations . . .’. The Directive does not otherwise specifically define what is meant by ‘adequate’, though the criterion is generally understood as a less stringent standard than the criterion ‘equivalent’ in the CoE Convention and OECD Guidelines.<sup>90</sup> This softens the potentially negative impact of the rule in Article 25(1) on data flows to third countries.

Its impact is softened further by Article 26, which permits transfer of personal data to a third country lacking adequate protection if, in summary, the proposed transfer:

1. occurs with the consent of the data subject; or
2. is necessary for performing a contract between the data subject and the controller, or a contract concluded in the data subject’s interest between the controller and a third party; or
3. is required on important public interest grounds, or for defending ‘legal claims’; or
4. is necessary for protecting the data subject’s ‘vital interests’; or
5. is made from a register of publicly available information (Article 26(1)).

The proposed transfer may alternatively be allowed if accompanied by ‘adequate safeguards’, such as ‘appropriate contractual clauses’, instigated by the controller for protecting the fundamental rights of the data subject (Article 26(2)). The Commission may make binding determinations of what constitute adequate safeguards in this context (Article 26(4)). It has exercised this power by stipulating standard contractual clauses to govern data transfers.<sup>91</sup>

In very recent years, business groups have been pushing for recognition of ‘Binding Corporate Rules’ (BCRs) as a form of ‘adequate safeguard’. The essential idea is that a group of companies draft their own set of data protection rules which are enforceable against each entity in the group regardless of location. Once approved by an appropriate data protection authority, the BCRs

---

<sup>90</sup> See, e.g., Schwartz 1995, pp. 473 & 487; Greenleaf 1995, p. 106; Ellger 1991b, p. 131.

<sup>91</sup> See Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (O.J. L 181, 4 July 2001, pp. 19–31); Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (O.J. L 6, 10 January 2002, pp. 52–62); Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (O.J. L 385, 29 December 2004, pp. 74–84).

permit cross-border data transfers within the company group.<sup>92</sup> While ostensibly attractive, the practicalities of this co-regulatory strategy are still being thrashed out. A major problem has been the dearth of a single, pan-European approval system for BCRs. The Commission has yet to set up such a system. However, the Article 29 Working Party has lessened, though not eliminated, the problem by developing a co-ordinated fast-track procedure for BCR approval by all of the relevant national data protection authorities.<sup>93</sup>

The Commission can make general determinations of adequacy under Article 25 which are binding on EU/EEA member states (Article 25(6)). The Commission does not make such decisions alone but with input from the Article 29 Working Party, the Article 31 Committee, and European Parliament.<sup>94</sup> Basic criteria for adequacy assessments have been developed by the Article 29 Working Party and form an important point of departure for Commission decisions.<sup>95</sup>

So far, positive determinations of adequacy have been made for a small number of jurisdictions and schemes, including Switzerland,<sup>96</sup> Canada,<sup>97</sup> Argentina,<sup>98</sup> the United States' (US) Safe Harbor scheme<sup>99</sup> and the transfer of Air Passenger Name Records (PNR data) to US border-control agencies.<sup>100</sup>

---

<sup>92</sup> Further on BCRs, see, e.g., Kuner 2007, pp. 218–232.

<sup>93</sup> Article 29 Working Party 2005.

<sup>94</sup> The procedure follows the ground rules contained in Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (O.J. L 184, 17 July 1999, pp. 23–26).

<sup>95</sup> Article 29 Working Party 1998.

<sup>96</sup> Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (O.J. L 215, 25 August 2000, pp. 1–3).

<sup>97</sup> Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (O.J. L 2, 4 January 2002, pp. 13–16).

<sup>98</sup> Commission Decision C(2003) 1731 of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (O.J. L 168, 5 July 2003, pp. 19–22).

<sup>99</sup> Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (O.J. L 215, 25 August 2000, pp. 7–47).

<sup>100</sup> See initially Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (notified under document number C(2004) 1914) (O.J. L 235, 6 July 2004, pp. 11–22) (subsequently annulled – see below); approved in Council Decision

In May 2006, the European Court of Justice nullified the first decision of the Commission regarding transfer of PNR data to the USA, together with the Council decision approving that decision.<sup>101</sup> Both decisions were held to be unlawful, not for privacy-related reasons, but because they apply to matters currently falling outside the scope of EC law – namely, public security and prevention of crime. A new agreement on the same subject, albeit with new legal legs, was hurriedly adopted in October 2006,<sup>102</sup> though not without considerable tussle between the USA and EU over its terms.<sup>103</sup> That agreement expired in July 2007 and was replaced by yet another.<sup>104</sup> Again, negotiations over the terms of the replacement agreement were tough.<sup>105</sup> The end-result has been strongly criticised by the Article 29 Working Party for further weakening protection of PNR data.<sup>106</sup>

Articles 25–26 have otherwise caused considerable consternation in some ‘third countries’, especially the USA which has been concerned about the provisions’ potentially detrimental effect on US business interests.<sup>107</sup> Some of the US discussion has focused on the legality of the provisions under international trade law, most notably the 1994 General Agreement on Trade in Services (GATS) which restricts signatory states from limiting transborder data flow in ways that involve arbitrary or unjustified discrimination against other such states.<sup>108</sup> At the same time, GATS allows restrictions on trans-

---

2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (O.J. L 183, 20 May 2004, p. 83)(subsequently annulled – see below).

<sup>101</sup> Judgment of 30 May 2006 in Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*.

<sup>102</sup> Council Decision 2006/729/CFSP/JHA of 16 October 2006 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (O.J. L 298, 27 October 2006, pp. 27–28).

<sup>103</sup> See Phillips & Bilefsky 2006.

<sup>104</sup> Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) (O.J. L 204, 4 August 2007, pp. 16–17).

<sup>105</sup> See, e.g., Meller 2007.

<sup>106</sup> See Article 29 Working Party 2007.

<sup>107</sup> See generally Swire & Litan 1998.

<sup>108</sup> See Agreement Establishing the World Trade Organization, adopted 15 April 1994, Annex 1B, especially Articles II(1), VI(1), XIV(c)(ii) and XVII. Prominent instances of the US discussion are Swire & Litan 1998 and Shaffer 2000, pp. 46–55.

border data flow when necessary to secure compliance with rules relating to 'protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts' (Article XIV(c)(ii)). While such restrictions must also conform to the Agreement's basic prohibition against arbitrary or unjustified discrimination between countries and against disguised restrictions on trade in services, little if any solid evidence indicates that Articles 25 and 26 of the Directive have been or are being applied in breach of that prohibition.<sup>109</sup>

The initial tension between the USA and EU in the wake of the Directive's adoption cooled considerably after they agreed to adopt the 'Safe Harbor' scheme (hereinafter 'SH'). The agreement permits US organisations to qualify as offering adequate protection for personal data flowing from the EU/EEA, by voluntarily adhering to a set of basic data protection principles.<sup>110</sup> The principles are loosely modelled upon, though fall short of, the core standards set in the Directive.<sup>111</sup>

Despite slow corporate take-up in its early days, the SH scheme had well over 1000 corporations (including major businesses) formally certifying adherence to it as of 15 February 2008. However, doubts attach to the efficacy and viability of the scheme in terms of privacy protection. For instance, in a detailed analysis of the negotiations behind the scheme, Heisenberg observes that the scheme's chief goal has been to maintain trans-Atlantic data flow, with preservation of privacy very much a secondary concern.<sup>112</sup> Further, a study carried out for the Commission in 2004 found considerable deficiencies in the transparency, comprehensibility and comprehensiveness of a random selection of corporate privacy policies that sought (at the time) to reflect the SH principles.<sup>113</sup> The study also found little evidence to indicate that US authorities (primarily the Federal Trade Commission) or, indeed, national regulators in Europe, were taking any real interest in monitoring or enforcing compliance with the scheme.<sup>114</sup>

Beyond Directive 95/46/EC, the EU has adopted three other Directives concerned directly with privacy issues. The first, dealing specifically with telecommunications, was adopted in December 1997.<sup>115</sup> It has since been

---

<sup>109</sup> See also Shaffer 2000, pp. 49–52.

<sup>110</sup> Commission Decision 2000/520/EC, *supra* n. 98.

<sup>111</sup> See further, e.g., Greenleaf 2000.

<sup>112</sup> Heisenberg 2005, especially p. 160.

<sup>113</sup> Dhont *et al.* 2004.

<sup>114</sup> More generally, see Heisenberg 2005, chap. 6.

<sup>115</sup> Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (O.J. L 24, 30 January 1998, pp. 1–8).

repealed and replaced by Directive 2002/58/EC, which concerns electronic communications (including communications on the internet) more generally.<sup>116</sup> The latter contains provisions on, *inter alia*, security and confidentiality of communications (Articles 4–5), storage and use of communications traffic data (Articles 6, 15), processing of location data other than traffic data (Article 9), calling and connected line identification (Article 8), content of subscriber directories (Article 12), and unsolicited communications for direct marketing purposes (Article 13).

In 2006, the EU adopted a Directive on retention of communications traffic data.<sup>117</sup> This Directive owes most of its life to the terrorist attacks in Madrid and London in 2004 and 2005 respectively and the concomitant interests of law enforcement agencies in gaining access to communications traffic data as part of their ‘war’ on terror and serious crime. It requires member states to ensure that providers of public communications networks store such data for a minimum of six months and maximum of two years. However, the future of the Directive is uncertain. Ireland is seeking annulment of the Directive by the European Court of Justice on the same grounds that felled the first agreements on transfer of PNR data to the USA,<sup>118</sup> while a large number of other member states have postponed implementing certain provisions of the Directive due to textual ambiguity.

The EU has also established the office of European Data Protection Supervisor (EDPS).<sup>119</sup> The EDPS has supervisory and control functions with respect to EU institutions only. It can issue legally binding orders, which may be appealed to the European Court of Justice.<sup>120</sup>

At the time of this writing, the EU is drafting a Framework Decision on privacy protection rules for the police sector. The Commission has issued a proposal for such a decision,<sup>121</sup> which is now being negotiated with input from

---

<sup>116</sup> Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (O.J. L 201, 31 July 2002, pp. 37–47).

<sup>117</sup> Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (O.J. L 105, 13 April 2006, pp. 54–63).

<sup>118</sup> See European Court of Justice, Case C-301/06, *Ireland v Council and Parliament* (O.J. C 237, 30 September 2006, p. 5).

<sup>119</sup> Established pursuant to Regulation (EC) 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data (O.J. L 8, 12 January 2001, pp. 1–22). Article 286(2) of the EC Treaty mandates establishment of the EDPS.

<sup>120</sup> See further Hijmans 2006.

<sup>121</sup> Proposal for a Council Framework Decision on the protection of personal data

the European Parliament, the EDPS, the Article 29 Working Party and the Council.

Finally, some privacy safeguards are provided under other EU codes that do not deal primarily with privacy or data protection. The main example here is the Schengen Convention of 1990,<sup>122</sup> primarily concerned with enhancing border control and security but also containing data protection rules in provisions regulating use of the Schengen Information System (SIS).<sup>123</sup> The rules of procedure for Eurojust operations are another example on point.<sup>124</sup>

## APEC PRIVACY FRAMEWORK

The most recent privacy code of global significance is an agreement between the 21 member states of the Asia-Pacific Economic Cooperation on a set of common principles to guide their respective approaches to regulation.<sup>125</sup> This agreement takes the form of a 'Privacy Framework', the complete version of which was adopted in 2005.

Work on the Framework signals a readiness by the APEC states to forge their own approach to privacy regulation largely independent of European norms.<sup>126</sup> It appears to foster privacy regimes less because of concern to protect basic human rights than concern to engender consumer confidence in business.<sup>127</sup>

The Framework is clearly inspired by, and modelled upon, the OECD Guidelines rather than EU and CoE instruments. Indeed, in its Preamble, it goes out of its way to laud the continuing importance of the Guidelines.

While concern for privacy is far from absent in the formal rationale for the Framework,<sup>128</sup> economic concerns are clearly predominant. One familiar concern is to prevent commercially harmful restrictions on transborder data

---

processed in the framework of police and judicial co-operation in criminal matters (COM(2005) 475 final, Brussels, 4 October 2005).

<sup>122</sup> While the Schengen *acquis* has non-EU origins, it was incorporated into the EU legal system by the Treaty of Amsterdam in 1997.

<sup>123</sup> Further on these rules, see Karanja 2008.

<sup>124</sup> Rules of procedure on the processing and protection of personal data at Eurojust (O.J. C 68, 19 March 2005, pp. 1–10).

<sup>125</sup> The APEC states are Australia, Brunei, Canada, Chile, China, Hong Kong, China, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, the Russian Federation, Singapore, Taiwan, Thailand, the USA and Vietnam.

<sup>126</sup> However, not all APEC states have formally endorsed the Framework. China is a significant example on point.

<sup>127</sup> See also Greenleaf 2005.

<sup>128</sup> The Preamble states, e.g., that the Framework 'reaffirms the value of privacy to individuals and to the information society' (para. 5).

flow. Another is to bolster consumer confidence and thereby ensure growth of commerce, particularly in the electronic context. The Framework seems implicitly to treat privacy safeguards not as valuable in themselves but as principally valuable for their ability to facilitate the realisation of the 'potential' of electronic commerce. The Framework scarcely, if at all, alludes to privacy safeguards as fundamental rights.

The heart of the Framework is a set of 'Information Privacy Principles' (IPPs). These are essentially rather diluted reformulations of the core principles of the OECD Guidelines.<sup>129</sup> Though consistent with the broad thrust of the OECD Guidelines, the IPP standards are lower than those of the European instruments. For instance, the Framework does not embrace the sensitivity principle, and it applies the criteria of 'fair' and 'lawful' only to the *collection* of personal information (para. 18) as opposed to further stages of information processing.

The Framework does not prescribe that it be implemented in a particular way – for example, through legislation or establishment of data protection authorities. Instead it avers that a variety of implementation methods may be appropriate. Suspensions of the principles are permitted according to criteria more lax than those specified under the EU and CoE codes. They are to be 'limited and proportional to meeting the objectives' to which they relate, and they are either to be 'made known to the public' or 'in accordance with law' (para. 13).

Regarding transborder data flow, the Framework does not expressly permit or mandate restrictions when the recipient jurisdiction lacks equivalent or adequate protection for the data (see generally Part IV(B)). Nor does it require data exports to be allowed to countries with APEC-compliant laws (or equivalent protections). Nonetheless, Principle IX (para. 26) states that a data controller 'should be accountable for complying with measures that give effect to the Principles', which could be read as imposing some liability on a data controller that exports data to other countries. But the threshold for satisfying this 'accountability' is far from high:

[w]hen personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles (para. 26).

The Framework has been aptly described as 'OECD Lite' and criticised

---

<sup>129</sup> See further Greenleaf 2005.

accordingly.<sup>130</sup> Nevertheless, it is possible to view the Framework more positively as a significant first step in arriving at policy consensus for a region characterised by great cultural, ethical and legal diversity.

## HUMAN RIGHTS INSTRUMENTS

Forty years ago, it was common to regard the principal catalogues of fundamental human rights as having little direct relevance for tackling the privacy issues thrown up by the computer age. Today the situation is greatly changed. The Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), along with the main regional human rights treaties,<sup>131</sup> are now firmly considered to provide the central formal normative roots for laws on privacy and data protection. They are also increasingly seen and used as data protection instruments in themselves.

Jurisprudence developed pursuant to ICCPR Article 17 and ECHR Article 8 provides the backbone for this development. Both provisions have been authoritatively construed as requiring national implementation of the basic principles of data protection. Moreover, the jurisprudence is increasingly regarded as providing an important touchstone for interpreting ordinary codes on privacy and data protection.<sup>132</sup>

Article 17 of the ICCPR provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

Whereas the above provisions are framed essentially in terms of a prohibition on ‘interference with privacy’, the equivalent provisions of ECHR Article 8 are framed in terms of a right to ‘respect for private life’:

---

<sup>130</sup> Greenleaf 2003; Greenleaf 2005. See too Lawson 2007.

<sup>131</sup> With the possible exception of the African Charter on Human and People’s Rights (OAU Doc. CAB/LEG/67/3 rev. 5; adopted 27 June 1981; in force 21 October 1986) which does not include privacy in its catalogue of rights. The omission of privacy in the African Charter is not repeated in all human rights catalogues from outside the Western, liberal-democratic sphere. For example, Article 18 of the Cairo Declaration on Human Rights in Islam (UN Doc. A/45/421/5/21797, p. 199), adopted 5 August 1990, expressly recognises a right to privacy for individuals.

<sup>132</sup> See, e.g., the ECJ decision of 20 May 2003 in *Joined Cases C-465/00, C-138/01, and C-139/01 Österreichischer Rundfunk and Others* [2003] ECR I-4989.

1. Everyone has the right to respect for his private and family life, his home and correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Human Rights Committee set up to monitor implementation of the ICCPR has held that Article 17 requires processing of personal data in both the public and private sectors to be legally regulated in accordance with basic data protection principles.<sup>133</sup> This is particularly significant as the ICCPR has the greatest reach of treaties on human rights, having been ratified by over two-thirds of the world's nation states.

As for ECHR Article 8, the European Court of Human Rights has over a long series of cases gradually reached a standpoint similar to the broad thrust of General Comment 16. The bulk of these cases have concerned surveillance and control activities by police or state intelligence services.<sup>134</sup> Up until recently, uncertainty attached to the extent to which Article 8 could regulate data-processing activities of private sector bodies. In a famous decision in 2004 in the case of *Von Hannover v Germany*, the Court finally made clear that although Article 8 (and the ECHR generally) aims primarily to protect individuals from the actions of state authorities, it also requires CoE states to place limits on private actors' processing of personal information, even when the information concerns celebrities. Concomitantly, the Court held, celebrities have a right to respect for their private life and cannot be 'free game' for the mass media. The Court went on to hold that, in the main, publication of personal information is only justified (under the Convention) when the information contributes to a debate of general societal interest (as opposed to publication purely to satisfy curiosity).

---

<sup>133</sup> General Comment 16 of 23 March 1988 (U.N. Doc. A/43/40, pp. 180–183), paras. 7 & 10.

<sup>134</sup> See, e.g., *Klass v Germany* (1978) Series A of the Publications of the European Court of Human Rights ('A'), 28; *Malone v United Kingdom* (1984) A 82; *Leander v Sweden* (1987) A 116; *Gaskin v United Kingdom* (1989) A 160; *Kruslin v France* (1990) A 176-A; *Niemietz v Germany* (1992) A 251-B; *Amann v Switzerland* (2000) Reports of Judgments and Decisions of the European Court of Human Rights 2000-I. See further Bygrave 1998.

## POWER PLAY AND THE DECREASING SIZE OF THE WORLD

Of all of the codes reviewed in this chapter, the EU Directive is the most prominent trendsetter for data protection norms around the world. While its influence is naturally greatest in Europe, numerous non-European countries have enacted legislation or are on the way to doing so, in order, at least partly, to meet the adequacy criterion in Article 25. Australia, Hong Kong and Korea are all examples on point.<sup>135</sup> Further, Argentina has enacted legislation in 2000<sup>136</sup> modelled on the EU Directive and equivalent Spanish legislation. Dubai passed legislation in 2007 also modelled on the Directive – the first Arab state to do so.<sup>137</sup> The South African Law Commission has prepared a privacy Bill which is clearly influenced by the Directive and partly aimed at enabling the country to be deemed as providing adequate protection for the purposes of Article 25.<sup>138</sup> Turkey appears to be following suit.<sup>139</sup>

Nevertheless, the ability of the EU to bring the privacy regimes of non-European states in line with its preferred model, is clearly vulnerable. This is partly because of sovereignty factors, and partly because of the emergence of APEC as a potential competitor in the role of international privacy policy-broker. Yet it is also because of ‘problems at home’. Not only has national transposition of the Directive often been slow, there appear to be – even after transposition – low levels of harmonisation, enforcement, compliance and awareness with respect to the national European regimes.<sup>140</sup> Especially problematic for the Directive’s global credibility is the weak implementation of its regime for transborder data flow to third countries. That regime is caught between ‘a rock and a hard place’: if properly implemented, the regime is likely to collapse from the weight of its cumbersome, bureaucratic procedures. Alternatively, it could well collapse because of large-scale avoidance of its proper implementation due precisely to fears of such procedures. Use of contractual and co-regulatory strategies, such as BCRs, may alleviate this situation somewhat but will probably not resolve it.

---

<sup>135</sup> See further the chapters in this volume dealing with each of these jurisdictions.

<sup>136</sup> Law for the Protection of Personal Data of 2000.

<sup>137</sup> Dubai International Financial Centre (DIFC) Law No. 1 of 2007, described in Michael 2007.

<sup>138</sup> South African Law Commission 2005.

<sup>139</sup> See draft Law on the Protection of Personal Data of 2003; available (though only in Turkish) at <<http://www.kgm.adalet.gov.tr/kisiselveriler.htm>> (last accessed 15 February 2008).

<sup>140</sup> See generally European Commission 2003.

The chances of achieving, in the short term, greater harmonisation of privacy regimes across the globe are slim. This is due not simply to the strength of ingrained ideological and cultural differences around the world, but also to the lack of a sufficiently strong, dynamic and representative international body to bridge those differences. The World Trade Organisation (WTO) is occasionally touted as such a body. Yet its ability to negotiate a broadly acceptable agreement on privacy issues may be hampered by its commercial bias.

Calls are occasionally made to draft a truly international convention on privacy and data protection, within the framework of the UN.<sup>141</sup> And UNESCO has recently emerged as a new forum for discourse on international privacy policy.<sup>142</sup> Nevertheless, any UN-sponsored process with a view to a future global treaty will be a very long (and long-winded) affair, and the chances are slight of an eventual treaty having real bite. As for harmonisation at the regional level, this remains incomplete in the EU – home to the hitherto most ambitious harmonisation efforts. As for APEC, its track record is yet to be fully established. APEC represents huge economic muscle, but whether it will develop into a consequential force in privacy matters is too early to say. Its Privacy Framework, though, is unlikely to bring harmonisation much further in the Asia-Pacific. This has not stopped some corporate players, such as Google, touting the Framework as the appropriate baseline for global privacy standards.<sup>143</sup>

Forty years ago the ideological landscape in which international privacy instruments were drafted was more open than now. Back then, discussion about privacy revolved largely about doctrines on human rights and rule of law; economic and trade-related considerations received relatively marginal attention. Today, however, the same sort of discussion cannot be separated from trade issues. Nor can it be separated from attention to a range of other cross-cutting issues, such as the ‘war on terror’, national security and law enforcement generally. Globalisation processes in terms of economy, crime, law enforcement, information and communication networks, etc. are rapidly decreasing the size of the world. The horizons for regulatory policy are increasingly cluttered; various norm sets are more prone to colliding with each other. Concomitantly, future international policy making on privacy issues will

---

<sup>141</sup> See, e.g., the Declaration made at the 27th International Conference of Data Protection and Privacy Commissioners at Montreux in September 2005: ‘Montreux Declaration on protection of personal data and privacy in a globalised world: a universal right respecting diversities’, <[http://www.privacyconference2005.org/fileadmin/PDF/montreux\\_declaration\\_e.pdf](http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf)> (last assessed 15 February 2008).

<sup>142</sup> See, e.g., Greenleaf 2006.

<sup>143</sup> See Privacy Laws & Business 2007.

be increasingly complicated and, arguably, increasingly destined to fail in terms of offering clear and relatively stringent norms.

One of the most intriguing aspects of the policy debates in international forums over the last 40 years is that they have largely occurred within the Western, liberal, democratic 'camp'. There has been little serious engagement with the rest of the world specifically on privacy issues. Where is China? Pakistan? Why have they not yet been the focus of EU adequacy assessments? This situation will and must change. In the coming 40 years, the policy debates will move out of the relatively cozy Western sphere. We see the beginnings of this development in the APEC Privacy Framework. The form and content of that instrument support the argument made out above that international policy in the field will increasingly fall short of prescribing clear and relatively stringent privacy norms. That argument can only gain strength if other players with a distinctly trade-friendly focus, such as the WTO, join APEC in brokering international privacy policy.

## 2. The United States

### **Priscilla M. Regan**

---

In 1989, a young California actress, Rebecca Shaeffer, was stalked and shot to death by an obsessed fan who obtained her home address from the California Department of Motor Vehicles (DMV). The death of this celebrity drew media attention to the problem of stalking and to the myriad databases of personal information that could be used to find someone. In this case, the focus of attention turned to drivers' license records, maintained by the 50 states and considered in most states to be a public record database that could be accessed for a fee. In 1994 Congress passed the Driver's Privacy Protection Act (DPPA) to restrict access to such information including name, address, telephone number, photograph, and medical or disability information. The DPPA was introduced in the Senate by Barbara Boxer (D-CA) and in the House by Jim Moran (D-VA) both of whom had constituents who had been victims of releases of information from state DMVs. Direct marketers, private investigators and the media all lobbied against the DPPA.

As soon as the law became effective in September 1997, the state of South Carolina sued claiming that the law violated the Tenth Amendment which states that powers not delegated to Congress are reserved to the states. A federal district court in South Carolina agreed and enjoined enforcement of the DPPA in South Carolina stating that 'the states have been, and remain, the sovereigns responsible for maintaining motor-vehicle records, and these records constitute property of the states'. The Court held that individuals did not have a 'reasonable expectation of confidentiality' in their DMV information and that the medical information contained in those records could be discerned from observing the individual and therefore was not private (Hammit, 1997).

On appeal, the Supreme Court upheld the constitutionality of the DPPA holding that Congress had the power under its authority to regulate interstate commerce because 'personal, identifying information that the DPPA regulates is a thing in interstate commerce' (*Reno v Condon*). The Court did not specifically address First Amendment claims although some argue that this ruling represents 'a radical break with existing First Amendment principles' and was not justified as the First Amendment arguably protects a right to gather information (Froomkin 2000, 1508).

Questions about driver's licenses reappeared on the policy agenda following 11 September when several of the terrorists used fake driver's licenses to board the planes that they flew to destruction. Several states tightened requirements for getting licenses and the American Association of Motor Vehicle Administrators (AAMVA) began to advocate standardization of state driver's license requirements, standards, and formats. This proposal became part of a larger public discussion about possible introduction of a national identification card and system (NRC 2002). In May 2005, as part of a military appropriations bill, Congress passed the Real ID Act which requires that state driver's licenses and other identification documents meet federal ID standards. These include a digital photograph, anti-counterfeiting features, and machine-readable technology such as a magnetic stripe or RFID tag. The Department of Homeland Security is charged with developing the detailed regulations which are to go into effect in 2008.

This vignette illustrates a number of features of information privacy policymaking and policy in the US. Generally it takes an incident to focus attention on the issue of information privacy – and such incidents tend to focus on one type of record system at a time. This human interest element helps to define the policy problem, galvanize media and public attention, and give members of Congress concrete examples of privacy invasion to justify their votes. There is always vocal and well-financed opposition to privacy protections, generally from business and government bureaucrats who do not want to restrict access to personal information. Their opposition is usually quite successful in weakening the proposed privacy protections and in further narrowing the scope of such protections. And after passage opponents are likely to challenge legislation in the courts, often on the basis of First Amendment grounds that any information, including that about individuals, should flow freely and without government restriction.

State driver's license databases are just one of the countless personal data systems that shape Americans' lives. These systems cover all aspects of daily life. At various points, scholars and commentators have tried to capture the breadth and depth of record-keeping activity in the United States; all conclude that the scope is extensive and expanding (Long 1967, Miller 1971, Westin and Baker 1972, Rule 1973, Burnham 1983, Laudon 1986, Linowes 1989, Garfinkel 2000, Rosen 2004).

States maintain not only databases of driver's licenses but also tax records, property records, registration records for items such as cars and guns, arrest records, criminal and civil court records, school records, library records, life event records (birth, marriage and death), public health records, and records for emergency management.

The federal government also maintains tax records, Social Security records, Selective Service records, government loans, federal criminal records, federal

employment records, military personnel records, and records maintained for national security and homeland security purposes.

Private-sector organizations maintain even more databases on individuals spanning every aspect of an individual's existence: newspaper and magazine subscriptions, communications activities (including detailed records of phone, email and internet usage), credit and debit card purchases, consumer purchases (including detailed records of purchases at grocery, book, and drug stores when one uses a frequent shopper card), video rentals, medical history, banking and investment decisions, and utility usage.

Almost all analyses of privacy protection in the United States conclude that privacy protection is weak, proceeds on a sector-by-sector basis, and consists of a patchwork of protections.

## LEGAL AND CONSTITUTIONAL FRAMEWORK

American legal and philosophical thinking about privacy begins with Samuel Warren and Louis Brandeis's 1890 *Harvard Law Review* article in which they argued that the common law protected a 'right to privacy' and that 'the right to life has come to mean the right to enjoy life – the right to be let alone' (1890, 193). They anchored the right to privacy in the common law protection for intellectual and artistic property – arguing that this protection was not based on private property but instead on the concept of an 'inviolable personality' (1890, 205). Privacy, or 'the right of the individual to be let alone', was similarly protected as part of the inviolable personality. The next major step in legal thinking on privacy is William Prosser's 1960 *California Law Review* article on privacy in which he concluded that a right to privacy, 'in one form or another', was recognized in four different tort protections – intrusion, disclosure, false light, and appropriation. He viewed privacy as a common term for a number of different ways in which the 'right to be let alone' might be invaded. Most legal scholars agreed that traditional privacy protections in common law would not easily or effectively be extended to cover the more general privacy concerns, especially those regarding information privacy, that began to develop in the late 1960s (Fried 1968, Kalven 1966, Miller 1971, Westin 1967).

From a constitutional perspective, it is important to point out that 'privacy' or a 'right to privacy' is not mentioned in the Constitution. However, over time the Supreme Court has recognized a number of privacy rights deriving them from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments. These constitutional protections only apply to government action; they do not restrict private sector or individual actors or provide any protections against privacy invasions in those contexts. Under the First Amendment and due process

clause of the Fifth and Fourteenth, the Court has upheld a number of privacy interests – including ‘associational privacy’ (*NAACP v Watkins* 1958), ‘political privacy’ (*Watkins v US* 1957 and *Sweezy v New Hampshire* 1957), and the ‘right to anonymity in public expression’ (*Talley v California* 1960).

The Fourth Amendment’s protection of ‘the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures’ has been an important basis for privacy protection. The most important Fourth Amendment case is *Katz v United States* (1967), a wiretapping case in which the Court ruled that the Fourth Amendment protected people, not places, and did not require physical trespass or seizure of tangible material. In the concurring opinion, Justice John Marshall Harlan developed a two-part formulation to determine whether an individual had a ‘reasonable expectation of privacy’: ‘first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable’” (*Katz*, 361). In subsequent decisions the Court has constructed a continuum of circumstances under which it agrees that society would regard an individual as having a reasonable expectation of privacy. The continuum ranges from public places (for example, open fields, in plain view, or public highways), in which there is no objective expectation of privacy except in unusual circumstances, to the inside of one’s home with the windows and curtains closed, in which there is an objective expectation of privacy. Through Title III of the Omnibus Crime Control and Safe Streets Act and the Electronic Communications Privacy Act, Congress has given more concrete meaning to the Fourth Amendment protection against unreasonable searches and seizures. requirements.

The Fifth Amendment protection against self-incrimination also provides a basis for a type of privacy protection. Courts have interpreted it to prohibit compelling anyone to disclose incriminating personal information in criminal cases or other governmental proceedings. Its narrow application rests in part of the Court’s distinction between testimonial evidence, involving communication by the individual and hence protected, and physical evidence, which is not protected. With respect to personal information, the Court has limited its protection to information that is in the possession of the individual, not a third party (*Couch v United States*, 1973), and has waived protection for information that is part of a ‘required record’ (*Grosso v United States*, 1968).

The broadest privacy rights have been those adopted to protect reproductive privacy, which is conceptually different from information privacy as it involves control over a personal domain. In *Griswold v Connecticut* (1965), *Eisenstadt v Baird* (1972), and *Roe v Wade* (1973), the Court ultimately recognized a ‘right to privacy’ in ‘the Fourteenth Amendment’s concept of personal liberty and restrictions upon state action’. These protections, however, have not been extended beyond the sphere of reproductive privacy. For example, in

1976 in *Paul v Davis*, the Court refused to expand the areas of personal privacy considered 'fundamental' to include erroneous information in a flyer listing shoplifters. A year later, the Court recognized for the first time two kinds of information privacy interests: 'one is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions' (*Whalen v Roe*, 1977, 599–600). But in this instance, the Court upheld a New York law that required the state to maintain computerized records of prescriptions for certain drugs because the state had taken precautions to protect computer security and had placed restrictions on disclosures from the records, thus minimizing the potential for personal information to be disclosed inappropriately.

From the onset of public debates about personal information in the 1960s, it was clear that privacy was an important and multi-faceted value for which some legal and constitutional protection existed. Additionally it was recognized that privacy was not an absolute value – no one has an unlimited right to be 'let alone' – but one that was often balanced against other competing social and legal values. Finally, it was clear that existing legal and constitutional protections were not easily accommodated to new collections and uses of personal information – and that the courts were reluctant to be at the forefront of such changes. Thus new statutory protections would be needed.

## KEY DEVELOPMENTS IN PRIVACY PROTECTION

The primary catalyst leading to policy discussions about information privacy protection in the United States has been technological change. From computerization of large data sets in the 1960s to computerized processing of all records in the 1970s to computerized searching of record systems in the 1980s to the online linkages and searching capabilities of the 1990s, information and communications technologies have provided the focusing events for concerns about privacy protection. This is not to say that other factors – most notably political events, interest groups, policy ideas, political climate, constitutional issues, and transnational activities – have not played important roles in the development of American privacy protection. But the initial trigger placing information privacy on the policy agenda has been, and is likely to continue to be, technological change. Once on the agenda, privacy issues generally occupy a relatively low position until other political forces or events help to elevate public and congressional interest.

### **First Period – Computerization of Records**

Almost all analyses of the development of information privacy in the United

States identify the first step as the 1965 proposal of the Social Science Research Council (SSRC) to establish a Federal Data Center to provide access to and coordinate the use of government statistical information (Bennett 1992, Flaherty 1989, Regan 1995). This proposal precipitated a number of congressional hearings and some public debate (US House Committee 1966 and US Senate Committee 1966). The following statement by Representative Cornelius Gallagher (D-NJ), chair of the House Special Subcommittee on Invasion of Privacy, captures the public and congressional concern: 'It is our contention that if safeguards are not built into such a facility, it could lead to the creation of what I call "The Computerized Man" . . . [who] would be stripped of his individuality and privacy. Through the standardization ushered in by technological advance, his status in society would be measured by the computer and he would lose his personal identity. His life, his talent, and his earning capacity would be reduced to a tape with very few alternatives available' (US House Committee 1966, 2).

Although proposals to establish a Federal Data Center were rejected, the public and Congress recognized that privacy, computers and government information practices had introduced a policy problem that needed to be addressed. In a somewhat peculiar American fashion, three forums – a congressional committee, an executive agency, and a private foundation – simultaneously began to study the issue and recommend policy options. Beginning in 1970, the Senate Judiciary Committee's Subcommittee on Constitutional Rights, chaired by Senator Sam Ervin (D-NC), played a critical role in collecting information about government data banks and in building congressional support for legislation (US Senate 1971). In 1969 the Russell Sage Foundation and the National Academy of Sciences cosponsored a project to gather empirical information on how computer applications were being used by public and private organizations. The report, *Data Banks in a Free Society*, recommended a number of policy options to apply to both computerized and manual records including: a 'Citizen's Guide to Files; rules for confidentiality and data sharing; technological safeguards; restrictions on the use of the social security number; and information trust agencies to manage sensitive data' (Westin and Baker 1972). Finally the Department of Health, Education and Welfare (HEW) established an Advisory Committee on Automated Personal Data Systems to analyze and make recommendations regarding computerized information systems. Its report, *Records, Computers, and the Rights of Citizens*, was released in 1973 and emphasized the need for legislation and enactment of a Code of Fair Information Practices (HEW 1973).

The HEW Code mirrored the definition of the policy problem as one of privacy, confidentiality and due process – and defined the core of a policy solution in terms of fairness.

## HEW CODE OF FAIR INFORMATION PRACTICES

There must be no personal record-keeping system whose very existence is secret.

There must be a way for an individual to find out what information about him or her is in a record and how it is used.

There must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent.

There must be a way for an individual to correct or amend a record of identifiable information about him or her.

All organizations creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Source: US Department of Health Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens* (Washington, DC: Government Printing Office, 1973).

The various privacy bills introduced in the House and Senate were similar in including the key elements of the Code of Fair Information Practices but differed in their enforcement approaches, especially regarding the establishment of a regulatory Privacy Board, and in their scope of applicability, that is whether the public and private sector would be similarly treated. The primary Senate bill (S 3418) was comprehensive in scope, covering both automated and manual personal information systems in federal, state and local governments, as well as in the private sector. It provided for a Federal Privacy Board with authority to enter premises where information was held and by subpoena compel the production of documents, to hold hearings regarding violations, and to issue cease and desist orders if organizations were engaged in unauthorized information practices. It also established rights for individuals to see and amend their files and be informed of releases of information, similar to the HEW Code. The primary House bill (HR 16373) was weaker and less inclusive; it covered only federal agencies, did not provide for an independent privacy board, and permitted more exemptions.

As congressional deliberations proceeded, there was general agreement that state government personal information practices should not be regulated through an omnibus federal statute. The two most contentious issues in congressional hearings involved the omnibus scope of the legislation and the

establishment of a Federal Privacy Board. Private sector organizations argued vociferously that there was no real concrete evidence of abuses, that they were already overburdened with government regulations, and that companies could and would enact voluntary policies to protect privacy of personal information. They also maintained that the First Amendment limited the restrictions that government could place on the free flow of information, including private commercial information flows. At times the Supreme Court and lower courts had lent support to that view, but courts had also recognized that individuals had the ability to assert their own interests in exerting control over the flow of communication between themselves and another private party (*Lamont v Postmaster General* 1965).

Although the proposal to establish an independent oversight mechanism to protect privacy was viewed as essential by several privacy advocates, both the HEW Committee and the Westin and Baker study recommended against this type of regulation. The HEW Committee concluded that the need did not exist, there was not public support, it would be complicated and costly, and it might impede useful computer applications (HEW 1973, 43). In addition, federal agencies and private sector firms were united in opposition to this proposal. President Ford also spoke in opposition to the establishment of a privacy board.

In both chambers, the images of 1984 and the information abuses associated with Watergate were repeatedly mentioned as support for legislation. References to 'big brother' supervision of individuals, lack of credibility in government, and recent abuses related to personal information were included in virtually all statements on the floors of the House and Senate (Regan 1995, 81). Although many members, perhaps most vocally Senator Sam Ervin (D-NC), believed that the House and Senate committee reports documented long-standing issues of personal information misuse, most commentators agree that legislation would not have been debated and adopted by Congress in 1974 if there had not been the revelations of abuses associated with Watergate (Regan 1995, Bennett 1992, and Gellman).

The bill that passed the Senate included the creation of an independent privacy protection agency while the House bill did not provide for a separate agency. The Privacy Act, passed by Congress at the close of 1974, reflected the minimum protection that was advocated at the time. It incorporated the Code of Fair Information Practices but limited its applicability to federal agencies, placed enforcement responsibilities primarily on the individuals bringing grievances, and gave the Office of Management and Budget implementation authority. The Privacy Act of 1974 established the Privacy Protection Study Commission (PPSC) to investigate the need for an independent agency and private sector legislation. Many privacy advocates adopted the view of Senator Ervin that the Privacy Act was 'an important first step' (US Senate and House Committees 1974, 775) and that the next step would be taken by the PPSC.

The mandate of the PPSC was framed in terms of protecting 'the privacy of individuals while meeting the legitimate needs of government and society for information'. The PPSC held over 60 days of hearings and heard from over 300 witnesses from the private sector, including the insurance, credit, banking, and medical sectors. It also sent questionnaires to 500 companies to determine the extent and nature of information handling as well as perceived problems and costs in complying with proposed legislation (PPSC 1977). The PPSC retained the framework of the Code of Fair Information Practices but restated it as three goals: to minimize intrusiveness; to maximize fairness; and to create legitimate, enforceable expectations of confidentiality.

The PPSC had an opportunity to recommend omnibus legislation for the private sector as a whole. But private sector advocates that a sector-by-sector approach with minimal actual government involvement was the most appropriate given the diversity of information practices. The PPSC report is a fairly exhaustive survey and analysis of how records mediate relationships between individuals and organizations. The concept of 'relationships' provides the fundamental organizing concept: there are chapters discussing different relationships including consumer credit, depository, insurance, employment, medical care, and education. The report focused on the unique features and differences rather than commonalities, and laid the foundation for the sector-by-sector approach to private sector information policies that exists rather uniquely in the US (Bennett 1992, Flaherty 1989).

In 1977, the PPSC concluded that a voluntary approach should be the initial way of implementing privacy protection in the private sector. The PPSC recommended that existing regulatory agencies, such as the Federal Trade Commission, assume some responsibility for ensuring privacy protection in their sectors. With respect to the public sector, the PPSC recommended that a more advisory privacy body be established to monitor and evaluate implementation of the Privacy Act of 1974. Civil liberty groups and privacy advocates were critical of the report of the PPSC seeing it as a missed opportunity for serious policy formulation, as a concession to private sector opposition, and as a result of the strength of private sector influence on the commission itself (Hayden 1978).

The PPSC also issued numerous suggestions for sector-by-sector legislation – all of which were referred to numerous congressional committees. None resulted in legislation. Again in congressional committees and subcommittees, private sector representatives seized a forum for arguing that self-regulation would be sufficient. Indeed several private sector organizations did adopt voluntary policies and began to advertise that they had done so. Aetna Life Insurance Company, whose executive vice-president had been a member of the PPSC, adopted the slogan that 'your privacy is our concern' (Regan 1995, 85). Needless to say, there was no way of ensuring that such sentiments were

being followed internally. One bill containing most of the recommendations of the PPSC, the Omnibus Right to Privacy Act (HR 10076) was introduced in the House. This detailed, 161-page bill was referred to seven different committees, none of which recommended passage.

Despite intensive information gathering, 61 days of hearings, a good staff and an interested public, no legislation resulted directly from the recommendations of the PPSC. Its work was indirectly important in the passage of several federal statutes. But each of these took some event to precipitate renewed congressional and public interest (see below for a list of several of these statutes). For example, in *US v Miller* (1976) the Supreme Court ruled that 'checks are not confidential communications but negotiable instruments to be used in commercial transactions' and that the individual has no property interest or Fourth Amendment expectation of privacy in those records. As a result of this decision and with background and recommendations from the PPSC report, Congress passed the Right to Financial Privacy Act in 1978.

## SELECTED INFORMATION ON PRIVACY LEGISLATION

*Fair Credit Reporting Act of 1970* (PL 91-508) requires credit investigations and credit reporting agencies to make their records available to the subjects of the records, provides procedures for correcting information, and permits disclosure only to authorized customers.

*Family Educational Rights and Privacy Act of 1974* (PL 93-380) requires educational institutions to grant students or parents access to student records, establishes procedures to challenge and correct information, and limits disclosure to third parties.

*Privacy Act of 1974* (PL 93-579) gives individuals rights of access to and correction of information held by federal agencies and places restrictions on federal agencies' collections, use, and disclosure of personally identifiable information.

*Right to Financial Privacy Act of 1978* (PL 95-630) provides bank customers some privacy regarding their records held by banks and other financial institutions and stipulates procedures by which federal agencies can gain access to such records.

*Cable Communications Policy Act of 1984* (PL 98-549) requires cable services to inform subscribers of the nature of personally identifiable information collected, the nature of the uses and disclosures of such information, the time period for which the

information is kept, and the times during which subscribers can access the information. It also places restrictions on the cable services' collection and disclosure of such information.

*Computer Matching and Privacy Protection Act of 1988* (PL 100-503) requires agencies to formulate procedural agreements before exchanging computerized record systems for purposes of searching or comparing those records and establishes Data Integrity Boards within each agency.

*Video Privacy Protection Act of 1988* (PL 100-618) prohibits video stores from disclosing their customers' names and addresses and the specific videotapes rented or bought by customers except in certain circumstances.

*Driver's Privacy Protection Act of 1994* restricts access to information maintained by state Departments of Motor Vehicles including name, address, telephone number, photograph, and medical or disability information.

*Health Insurance Portability and Accountability Act of 1996* provides for standards protecting privacy of individually identifiable health information and establishes an offense of 'wrongful disclosure' with respect to health information.

*Financial Modernization Act of 1999*, commonly referred to as Gramm-Leach-Bliley (GLB) for its primary cosponsors, requires financial institutions to send notices of their information practices to all customers.

*Children's Online Privacy Protection Act of 1998* provides restrictions on the collection of personally identifiable information from children and empowers the FTC to oversee such practices.

## **Second Period – Matching of Record Systems and Surveillance**

Almost as soon as the Privacy Act of 1974 became law, technological applications challenged its effectiveness. In the late 1970s, federal agencies began to compare the computerized files of different programs to identify those who should not be in the programs. The first of these was Project Match in which the records of federal employees was compared to those of recipients of Aid to Families with Dependent Children (AFDC) to determine which federal employees had given false information on the AFDC application. In response to congressional, presidential and interest group concerns about the privacy implications of Project Match, the Office of Management and Budget (OMB) issued guidelines allowing computer matches to occur as a 'routine use'

exemption to the Privacy Act if there was a 'demonstrable financial benefit' (Langan 1979, Kirchner 1981, Weiss 1983).

As the use of computer matching and other automated record searches increased, the definition of the policy problem shifted from a focus on individual privacy to a focus on the surveillance potential of these systems. Rather than concentrating on questions about collection of personal information, individual access to personal information systems, and ability to correct and amend information, commentators began to see the enormous potential of integrating separate record systems and compiling the separate bits of information and records into larger systems with surveillance potential. As Gary Marx and Nancy Reichman pointed out computer systems could serve as 'informants' (1984). Oscar Gandy refers to this ability of organizations, facilitated largely by the use of new computer and information technologies to engage in a 'panoptic sort' – 'a kind of high-tech cybernetic triage through which individuals and groups of people are being sorted according to their presumed economic or political value' (1993). Similarly, Roger Clarke coined the term 'dataveillance' (1998). This represented a qualitative shift in the definition and scope of the problem and consequently in the type of policy response that was appropriate. If the problem was the surveillance potential of systems and not individual abuses of records, then giving individual rights was not likely to be an adequate response. Restrictions on those systems were more appropriate.

With the arrival of the year 1984, the surveillance theme received attention. Several congressional committees held hearings on technology and privacy, and several associations including the American Bar Association, the American Civil Liberties Union and the Public Interest Computer Association organized conferences around the surveillance and 1984 theme (Shattuck 1984a, 1984b). Congress also asked the Office of Technology Assessment (OTA) to investigate federal computerized information practices. The OTA concluded that these practices were rapidly leading to the creation of a *de facto* national database containing personal information on most Americans and that the social security number was becoming a *de facto* national identifier (OTA 1986).

In response to potential abuses resulting from computer matching and other sophisticated information applications, legislation was proposed and Congress held hearings. After two years of off-and-on deliberations, Congress passed the Computer Matching and Privacy Protections Act in the fall of 1988. The CMPPA established some procedural limitations on agency uses of records and established agency-wide oversight by creating Data Integrity Boards in each federal agency.

Concerns about record linkages and privacy implications were not unique to the United States. The same technological forces and organizational needs were driving larger and more integrated data systems in other advanced industrialized countries. In the late 1970s and mid-1980s, many other countries had

adopted national legislation to protect privacy and data. But with computerized searches and exchanges of record systems, countries became aware of the limitations of national laws and recognized the need for some international standards. In 1980 the Organization of Economic Cooperation and Development issued its principles. (See Table 2.1 for the key principles contained in various codes of information that have been developed in the US or that have influenced the development of such codes.)

Table 2.1 Codes of fair information practices

<b>Organization Endorsing Principles</b>	<b>Fair Information Principles Included</b>
US Department of Health Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, <i>Records, Computers, and the Rights of Citizens</i> (Washington, DC: Government Printing Office, 1973)	No secret record systems. Availability of information regarding collection, storage and uses of personal information. Consent to uses of information for purposes other than that for which it was collected (secondary uses). Ability to correct or amend a record. Organizations ensure the reliability of information and prevent misuse.
Privacy Protection Study Commission (1977)	<p>To <i>minimize intrusiveness</i> (to create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return).</p> <p>To <i>maximize fairness</i> (to open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about her made on the basis of it).</p> <p>To <i>create legitimate, enforceable expectations of confidentiality</i> (to create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual).</p>

---

<b>Organization Endorsing Principles</b>	<b>Fair Information Principles Included</b>
Organization of Economic Cooperation and Development (1980)	Collection Limitation Data Quality Purpose Specification Use Limitation Security Safeguards Openness Individual Participation Accountability
The Information Policy Committee of the White House's Information Infrastructure Task Force (IITF) (1995)	Privacy Integrity Quality
National Telecommunications and Information Administration and Office of Management and Budget, 'Elements of Effective Self Regulation for Protection of Privacy' (1998)	Notice Choice Data Security Data Integrity Access Correction and Amendment Accountability
National Information Infrastructure Advisory Council (NIIAC) (1995)	13 principles
Federal Trade Commission (1998)	Notice/Awareness Choice/Consent Access/Participation Integrity/Security Enforcement/Redress
Federal Trade Commission (2000)	Notice Choice Access Security

---

### **Third Period – Electronic Exchanges of Private and Public Records**

In the mid to late 1980s policy interest in the information practices of the private sector and state agencies was rekindled as the press publicized incidents of privacy invasions. *Business Week*, for example, had a 1989 cover story exposing how easy it was to gain access to credit files, including those of the vice-president (Rothfeder 1989). The *City Paper* in Washington DC was informed about the video rental files of a Supreme Court nominee – revealing the fact that there were no restrictions on release of that information. The stalking and murder of actress Rebecca Schaeffer in California exposed the potential abuses with public sector records. And policy interest in health care reform drew attention to the number of organizations that had ready access to health care information and the resulting potential for privacy abuses. In each instance the congressional response was hearings and introduction of new legislation. In the case of video rentals and DMV information, legislation did pass although not with the level of protection and regulation that privacy advocates preferred. In the case of credit information and medical information, legislation did not garner sufficient support during the 1980s but did see action in the 1990s.

The case of medical privacy is particularly interesting. In August 1996 Congress passed the Health Insurance Portability and Accountability Act (HIPAA). This Act addressed several concerns especially the rising cost of health care, the fear many had that they would lose health insurance if they changed jobs, and the paperwork and administrative burdens of the existing system. Recognizing that administrative simplification, consolidation and uniformity of records would also raise concerns about privacy and confidentiality, in HIPAA Congress directed the Department of Health and Human Services to recommend standards to Congress protecting privacy of individually identifiable health information and establishing an offense of ‘wrongful disclosure’ with respect to health information. Under HIPAA Congress was required to establish privacy standards by 1999; if Congress failed to do so by then, HIPAA required Health and Human Services (HHS) to do so by February 2000.

Although Congress held numerous hearings on medical privacy, members were not able to agree on legislation, and HHS then released proposed standards for public comment. These regulations, known as the Privacy Rule, became final in December 2000 after receipt of over 52,000 public comments. The complexity of the Privacy Rule generated confusion and HHS ended up re-opening comment about issues such as the requirement for patient consent, the cost of implementation, and inadvertent disclosures.

In March 2002, HHS issued modifications of the Privacy Rule, which permitted incidental disclosures and made pre-treatment consent optional. These became final in August 2002 after HHS received more than 11,000 comments over a 30-day comment period. Many of these comments, and

members of Congress, were critical of changes that seemed to favor the health care industry over individuals (Pollio 2004, Alpert 2003).

A second area for which there were countless policy discussions is that of financial privacy. Concern about financial privacy had heightened in late 1998 as banks began 'know your customer' programs that expanded the amount of information they held on customers to thwart money laundering. Privacy advocates and public opinion then put pressure on Congress to respond with regulations controlling such programs. Somewhat similar to health privacy, the financial privacy protections that passed Congress in 1999 were part of a larger policy effort, in this case modernization of the financial services sector.

The financial privacy protections are found in Title V of the Financial Modernization Act of 1999, commonly referred to as Gramm-Leach-Bliley (GLB) for its primary cosponsors. From a consumer standpoint the major 'protection' afforded by GLB is the requirement for financial institutions to send notices of their information practices to all customers. These notices have been roundly criticized for being too legalistic, long, and incomprehensible. Additionally the 'opt-out' provisions in the law are regarded by most privacy advocates as being too weak (Swire 2002).

By contrast, consider the European Data Protection Directive of 1995, which harmonized data protection or privacy policies throughout the European Union (EU). This directive provided for more comprehensive and stronger protection for privacy than any US legislation. It provoked much discussion about the discrepancies in the level and scope of privacy protection between the US and EU (Schwartz and Reidenberg 1996, Swire and Litan 1998, Regan 1993, 1999). There was much discussion in both the US and EU about whether the US privacy regime could be considered 'equivalent' or 'adequate' to the EU's requirements. The business community was most concerned about this for fear that there would be serious restrictions on the exchange of personally identifiable data between the US and EU countries. This is not the place to review the policy debates on this topic (see Regan 2002) but it is important to note that debates about privacy issues in the US, particularly financial privacy, were affected by concerns about the EU directive.

#### **Fourth Period – Online Collection and Exchanges**

As the internet began to take off in the early 1990s, concerns about the privacy in that medium received attention from Congress, executive agencies, advocacy groups and business interests. The focus was on business collection and exchanges of personal information rather than governmental activities and the issue was defined primarily as one of protecting consumers. Protection of privacy was seen as essential in achieving a climate more conducive for e-commerce. To this end, the Department of

Commerce and the Federal Trade Commission took the lead in policy formulation concerning online privacy.

The National Information Infrastructure Advisory Council was established by the Secretary of Commerce to advise him on the development of a National Information Infrastructure (NII). It included as members the emerging leaders of online commerce from the telecommunications, broadcast, computer, and cellular fields. Privacy was one of several issues seen as important to the development of the NII. At the same time, the Clinton administration also formed an interdepartmental Information Infrastructure Task Force (IITF) which had a Privacy Working Group tasked with developing privacy principles. The Clinton administration supported privacy as a principle but was reluctant to adopt any policy that might alienate private sector interests. Ira Magaziner, who served as the White House consultant on e-commerce, and advisors to Vice President Gore opposed creation of any privacy agency or statutory enforcement for privacy principles. Instead the administration championed 'self-regulation'.

As policy discussions began, it became clear that more information was needed about the online privacy practices and the feasibility of self-regulation in the online environment. The Federal Trade Commission (FTC) took the lead role in holding workshops on privacy, beginning in 1995 and continuing at least once a year through 2000, and in 1998 first surveyed a sample of 1400 commercial websites. This survey revealed that more than 85 per cent collected information from consumers, 14 per cent provided some notice of their personal information practices, and 2 per cent provided a comprehensive privacy policy notice.

Recognizing that these results revealed that online privacy was not being protected and that self-regulation was not working, several large private sector companies formed the Online Privacy Alliance, drafted privacy guidelines, and encouraged online posting of such policies. The following year, a privately funded Web survey, conducted through the Georgetown Business School, found that 92 per cent of the sites surveyed collected personal information – with 66 per cent posing a privacy notice or information practice statement and over 43 per cent posting a privacy policy notice. The FTC concluded that this was a sufficient increase in the number, if not necessarily the quality, of website notices to indicate that self-regulation was working and that legislation was not needed. In 2000 a new Web survey was conducted showed that, although there was an improvement in the number of websites posting some information about their privacy practices, few websites were not complying with all the fair information practices. They were not disclosing third-party cookies, nor were they independently verifying enforcement of their policies. In May 2000, by a 3–2 vote, the FTC concluded that industry self-regulation was not effective and that legislation to protect online privacy was necessary.

The FTC, acting under its authority to counter 'unfair trade practices', also brought several actions against deceptive online information practices. There were two key cases, one in 1998 against GeoCities and one in 1999 against Liberty Financial Companies.

Both involved websites' misrepresenting the purposes for which they were collecting personal information and their practices in using such information. The FTC brought actions against several online endeavors that resulted in settlements. These included suits against ReverseAuction.com for harvesting personal information from eBay and sending deceptive emails to eBay customers and another against a number of online pharmacies for collecting medical and financial data under false privacy assurances. The FTC also settled with Toysmart.com over its planned sale of its customer lists in violation of its stated online privacy policy.

In response to the administrative and FTC activities and to perceived public concern, a number of bills to protect online privacy have been introduced in Congress since 1996. The only online privacy issue to receive quick action was congressional passage of the Children's Online Privacy Protection Act of 1998 (COPPA). Bipartisan sponsorship, overwhelming public support and favorable media attention, coupled with weak arguments from the industry, ensured COPPA's enactment. In June 1998, the FTC issued a report finding that 89 per cent of children's websites collected personal information from children and fewer than 10 per cent provided any parental control over that collection (FTC 1998). Within the privacy and consumer communities, these findings were widely seen as 'irrefutable evidence' that self-regulation was not working and that 'swift government action' was necessary (CME 1998). Congress did act swiftly, passing COPPA in October 1998. COPPA tasked the FTC with writing implementing rules; proposed rules were issued in April 1999; public hearings held in July 1999; and the final rules issued in November 1999, going into effect in April 2000.

### **Fifth Period – Post 9/11**

Following 9/11, discussions about information privacy in the United States have taken on a different character. Security worries trumped privacy concerns. The USA PATRIOT Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) provides the widest array of new information sharing programs. But there are additional statutes, executive orders, and agency activities that similarly expand information collection and sharing. Almost all of these programs were enacted in haste and fear, without public debate and deliberation, and with the support of private sector firms which marketed sophisticated information sharing and data mining programs. The 342-page USA PATRIOT Act passed Congress 45

days after the terrorist attacks on the World Trade Center and the Pentagon, and while the Hart Senate Office Building was closed due to anthrax. The Senate vote was 98–1 and the House vote 357–66.

The USA PATRIOT Act facilitates access to personal information, increases personal data collection, and reduces due process and privacy protections for record subjects. It amends virtually every information privacy statute including the Family Educational Rights and Privacy Act, the Fair Credit Reporting Act, the Financial Right to Privacy Act, the Electronic Communications Privacy Act, the Cable Communications Policy Act, and GLB (Lee 2003, Lilly 2003, Martin 2003, Regan 2004). Specifically,

- Section 507 amends the Family Education Rights and Privacy Act to require educational institutions to disclose student records when law enforcement authorities certify that they may be relevant to a terrorism investigation;
- Section 505 amends the Fair Credit Reporting Act, the Financial Right to Privacy Act, and the Electronic Communications Privacy Act to permit government access to personal information when an FBI agent certifies that the records are relevant to a terrorist investigation.
- the USA PATRIOT Act amends the Foreign Intelligence Surveillance Act (FISA) to authorize CIA collection and use of domestic intelligence information;
- Section 358 amends the Right to Financial Privacy Act of 1978 to permit banks to disclose banking records to law enforcement authorities for analysis of intelligence activities;
- Section 215 amends the Electronic Communications Privacy Act of 1986 to expand the types of ISP subscriber records that law enforcement can access with an administrative subpoena;
- Section 211 reduces the privacy protections of the Cable Communications Policy Act regarding release of the customer records of cable companies;
- Section 203 amends Rule 6 of the Federal Rules of Criminal Procedure to allow the disclosure of grand jury information containing foreign intelligence information to federal authorities;
- Section 314 notes that the new requirements for sharing of information do not constitute a violation of the privacy protections of the Gramm-Leach-Bliley Act; and
- Section 405 requires the Justice Department to examine the feasibility of ‘biometric identification systems’ at Customs.

Among the most controversial of the provisions from a public opinion perspective are those affecting libraries. Patron library records, which were

formerly accessible only with a subpoena issued if there were probable cause and stating the specific object of the search, may now be accessed with a search warrant issued without requiring specificity or probable cause if foreign intelligence or terrorism is a 'significant purpose' of the search (Martin 2003). Additionally librarians are prohibited from disclosing to the public or the patron that such a search has occurred. Librarians do not have discretion in the decision to disclose records. But they do have discretion in their creation and maintenance of records and some libraries have reportedly stopped keeping certain records to avoid law enforcement inquiries (Pike 2002).

It is unclear how often libraries have been asked to disclose information. In a response to questions from the House Judiciary Committee, the Justice Department responded: 'The number of times the Government has requested or the Court has approved requests under this section [Section 215] since passage of the PATRIOT Act is classified and will be provided in an appropriate channel' (Doyle 2003). The American Library Association in its *Guidelines for Librarians on the USA PATRIOT Act* suggests that libraries review policies regarding retention and access to data, logs, and records with respect to when to discard or save (ALA 2002). The library community also supports a number of legislative proposals to amend the PATRIOT Act.

When Congress passed the PATRIOT Act, it provided that several of the more controversial data gathering and surveillance provisions would sunset, or expire, on 31 December 2005. Included among these was Section 215. Congressional debates to reauthorize the PATRIOT Act were spirited and raised a great deal of public interest. Indeed it had to be extended for two five-week periods while congressional negotiators worked out a compromise. In the end, the president signed the USA PATRIOT Improvement and Reauthorization Act of 2005 (PL 107-56) on 9 March 2006, with relatively modest but important civil liberties provisions. The revised Act provided for a four-year, rather than seven-year, extension of the revised Section 215. The new provisions include greater congressional oversight, procedural protections such as minimization on data collection and dissemination, a more detailed application for a 215 order, limitations on the non disclosure requirements, and a process for judicial review. The Reauthorization Act also provides more procedural protections on national security letters, which are a form of administrative subpoena not needing judicial approval issued by the FBI in cases where the FBI believes a subject to be a foreign spy, and specifies that they are not applicable to libraries unless they have established themselves as an internet service provider (Yeh and Doyle 2006).

Another continuing area of controversy involves airline passenger data. Due to the fact that the 9/11 terrorists used airplanes as their weapons, much subsequent attention has focused on identifying and apprehending potential terrorists before they get on an airplane. To that end the Department of

Transportation and the Department of Homeland Security, especially through the Transportation Security Administration (TSA), have initiated several passenger screening systems. The proposed TSA-operated CAPPS II (Computer-Assisted Passenger Prescreening System) would replace the existing system that operates on airlines' reservation systems. The new system would access more diverse data and perform more sophisticated analyses (GAO 2004). To support the development of CAPPS II, TSA in January 2003 issued a Privacy Act notice proposing a new system of records, 'Passenger and Aviation Security Screening Records'.

In response, TSA received over 200 comments overwhelmingly critical of the proposed system for being too broad and overly invasive of passengers' privacy. TSA modified these plans and announced its intention to begin limited developmental testing in July 2003 (USDHS TSA 2003). But such testing was delayed due to public and airline concerns about privacy and opposition to the system from other countries, especially those of the European Union (USDHS PO 2004). In February 2004 the General Accounting Office (GAO) issued a report criticizing TSA and CAPPS II for not addressing key implementation issues including accuracy of the data, unauthorized access prevention, and privacy concerns (GAO 2004).

The record disclosures and search provisions provided for in the USA PATRIOT Act essentially alter the maze of private sector and government record keeping. Formerly both law and practice created distinct sets of records, a 'stovepipe' approach to record management in which separate record systems were maintained in independent silos. This fragmentation provided its own benefits in terms of privacy protection and made it difficult though by no means impossible, to create dossiers linking all aspects of a person's life. The changes wrought by the PATRIOT Act represent a fundamental shift by overtly designing, and providing operating guidelines for, a surveillance system, which enables connections among and searching capabilities for separate systems, rather than a record management system, which is concerned with the internal efficiency of a single record system.

This emphasis on integrated systems designed to track people's movements and activities is echoed in proposals for new systems. Among the many examples is the US-VISIT (United States Visitor and Immigrant Status Indicator Technology) which will be 'a dynamic interoperable system involving numerous stakeholders across the government', which derives 'its capability from the integration and modification of existing systems' and 'will collect and retain biographic, travel, and biometric (i.e., photograph and fingerprints) pertaining to visitors' (USDHS 2003). Another example is MATRIX (Multistate Anti-Terrorism Information Exchange) program, funded largely by the Department of Homeland Security, created by Seisint Inc. of Florida and managed by a small consortium of states. This data mining system is fed

personal information from a range of public and private databases in the attempt to identify potential terrorists (ACLU 2004).

Concomitant of this surveillance approach is a likely information overload. The PATRIOT Act gives both law enforcement and intelligence arms of the government authority to collect more information – and collect it they will. But as Dempsey points out, ‘investigative and intelligence agencies were already choking on more information than they could digest’ and ‘the expanded surveillance powers are likely to make counterterrorism efforts more inefficient’ (Dempsey 2002). This sentiment is echoed by those who are confronted with implementing the new requirements. Berlau notes that with surveillance programs like FinCEN ‘experience suggests that piling up more data could make it harder to zero in on terrorists’ and that prior to 11 September ‘analysts were trying to find a needle in a very large haystack of data created by laws’ like the Bank Security Act (Berlau 2003).

## PUBLIC OPINION

Over the last 40 years, Americans registered consistently high levels of concern over privacy. But the concern has largely been latent rather than aggressive. Privacy appears to be one of those low level concerns that do not mobilize people to anger or action.

In discussing public opinion surveys, four cautions are in order. First, many of these public opinion polls have been sponsored by private sector companies and, although conducted by reputable polling firms, the question wording and order may have been affected by the sponsors (Gandy 2003). Second, those who are most concerned about privacy may not be willing to respond to public opinion polls, viewing them as yet another intrusion on their privacy (Gandy 1993, Katz and Tassone 1990). Third, surveys that ask only about privacy may exaggerate respondents’ concern about privacy and in some ways may be tapping a ‘non-attitude’ for which respondents do not have genuine views (Regan 1995). Finally, the meaning of privacy that people are thinking about when they respond is not obvious and respondents may be considering different aspects of privacy in their responses (Cantril and Cantril 1994).

From the 1970s to 1993, general concerns about threats to personal privacy increased. In several Harris surveys, the following question was posed: How concerned are you about threats to your personal privacy in America today? The percentage of those who viewed themselves as very or somewhat concerned about privacy increased from 64 per cent in 1978, to 77 per cent in 1983, and to 79 per cent in 1990. Over 70 per cent of respondents from 1990–93 agreed that ‘consumers have lost all control over how personal information about them is circulated and used by companies’. Part of this sense of

Table 2.2 *Seriousness of online privacy invasions*

<b>Internet Privacy Issues</b>	<b>Per cent Regarding as 'Very Serious'</b>
Collecting personal information about children without parental consent	85%
Tracking what websites people visit and using that information improperly	72%
Putting personally-identifiable public record information about individuals on the internet	72%
Reading email that is not addressed to them	71%
Collecting email addresses of website visitors without their knowledge or consent to compile email marketing lists	70%
Receiving unsolicited email (spam)	48%

*Source:* Louis Harris and Associate, Inc. and Alan F. Westin, *E-Commerce and Privacy: What Net Users Want* (Sponsored by *Privacy and American Business* and Price Waterhouse, Inc., June 1998)

loss of control comes from the perception that information is being used and exchanged in ways that individuals do not know. In 1978, 76 per cent agreed that 'Americans begin surrendering their personal privacy the day they open their first charge account, take out a loan, buy something on an installment plan, or apply for a credit card'. Over time increasing numbers of Americans say they believe that personal information about them is being kept in 'some files, somewhere for purposes not known' to them, with 44 per cent believing this in 1974 and 67 per cent in 1983.

More recently, public opinion surveys continue to indicate that over 80 per cent of respondents are concerned about threats to their privacy online. Although only 6 per cent of internet users reported that they were victims of an online privacy invasion, a 1998 *Privacy and American Business* survey revealed that almost three-quarters of internet users regard fairly typical online privacy issues as very serious (see Table 2.2). Industry-sponsored research confirms these findings. At the same time that large numbers of people express concern about online privacy invasions, people do reveal information online and are most comfortable doing so when they are told about the uses of that information. Surveys also reveal that people differentiate among the kinds of information that websites request. An AT&T survey, conducted in November 1998, asked internet users about how comfortable they generally feel providing specific types of information to websites: 82 per cent were comfortable

revealing their favorite TV show; 76 per cent were comfortable revealing their email addresses; 54 per cent were comfortable revealing their name; 44 per cent their postal address; 17 per cent their income; 11 per cent their phone number; and 3 per cent their credit card number (Cranor et al 1999, 9). Information about how personal data will be used is also important to people in making revelations in exchange for survey 'freebies' – such as free email, discounts, sweepstakes, and notices of how the information will be used. A 1999 *Privacy and American Business* survey found that, depending on the circumstances, about 75 per cent of respondents believed that it was fair to require disclosure of personal information in exchange for a benefit if a website offered a 'valuable benefit' and 'fully' informed individuals about what would be done with personal information (Opinion Research Corporation 1999).

However nebulous this public opinion may be, the latent concern for privacy can be inflamed by media reports about privacy invasions or by policy entrepreneurs who champion privacy issues, as has been demonstrated at numerous points. Images of 1984 and concerns about the 'computerized man' were critically important in getting the issue of privacy onto the public agenda in the 1960s. Popular writers, such as Myron Brenton (1964) Vance Packard (1964), Edward Long (1967) and Jerry Rosenberg (1969), brought these concerns to the public's attention and congressional hearings that adopted these images kept the public focused. Although the public attention was initially not sufficient to lead to legislation, these earlier images were quickly linked with the abuses of Watergate to effect legislative action in 1994. And most analysts do credit Watergate as being pivotal in the passage of the Privacy Act of 1974.

Throughout the history of privacy legislation critical events, highlighted by press attention, have served to focus public and congressional attention on privacy issues and serious policy formulation and adoption. Examples abound. Attempts in the early 1990s to strengthen the 1970 Fair Credit Reporting Act can be attributed to a 1989 *Business Week* cover story for which a reporter easily gained access to the credit history of the vice-president. The adoption of the 1988 Video Privacy Protection Act followed a Washington DC paper's publication of a list of the videotapes rented by Robert Bork, then a nominee for the Supreme Court. Press coverage of the California actress's stalking and murder by a man who obtained her home address from the Department of Motor Vehicles was pivotal in passage of the Driver's Privacy Protection Act of 1994. Passage of the privacy protections in GLB was similarly affected by concerns about identity theft, brought home to members of Congress by Representative Anna Eshoo who herself was a victim, and telemarketing excesses, voiced by Representative Joseph Barton's complaints about receiving a Victoria's Secret catalogue with an address supplied by his credit card company (Swire 2002, 27).

Such stories provided the personal, human connection that made for good press coverage, heightened public concern, and gave members concrete reasons to vote for privacy protections. And press reports of online privacy issues have also fueled support for privacy protections in that environment. This was dramatically illustrated when a failing dot.com, Toysmart, placed a 'for sale' ad in the *Wall Street Journal* listing as assets its databases and customer lists, despite the fact that its privacy notice stated that personal information 'is never shared with a third party' (Sandoval 2000).

Several instances have goaded grassroots action in response to privacy threats. For instance, in 1990 Lotus and Equifax developed Lotus MarketPlace: Households, a CD-ROM and software product containing personally identifiable information about 120 million people and 80 million households in the United States – including name, address, estimated household income, lifestyle, and shopping habits – that was designed to help small businesses in marketing their products. A slew of phone calls, letters, and emails to Lotus's CEO criticizing the privacy implications caused Lotus to cancel the product (Gurak 1997).

Similar online protests occurred in 1999 when Intel announced its Pentium III processor containing a Personal Serial Number (PSN), which could function as a unique identifier. Several privacy advocacy groups, including EPIC, Junkbusters and Privacy International, initiated a boycott and posted information on their websites. This generated media attention and provided people with information to contact Intel directly. In response, Intel made two modifications.

In 1999 DoubleClick, a major online advertising company, announced that it planned to combine its online customer profiles with personally identifiable information from the Abacus direct database. A barrage of negative publicity and complaints to the FTC resulted. The Center for Democracy and Technology (CDT) offered its website as a place to 'opt-out' of DoubleClick's tracking, to send a message to its CEO, and to send messages to companies using its services. In less than 72 hours, 13,000 people opted-out, 6000 sent messages to the CEO, and over 4400 sent messages to affiliates (Mulligan 2000). A *Wall Street Journal* article compared the public reaction to the DoubleClick/Abacus proposal to that of the 'colonials to the Stamp Act' (Bushkin 2000).

## NATIONAL CULTURE AND TRADITIONS

As I have argued elsewhere (Regan 1995), the formulation of privacy policy in the United States has been profoundly shaped by its liberal traditions emphasizing individual rights and a limited role for government. John Stuart Mill informed American policy discourse, not Michel Foucault. This has

meant first that the emphasis has been on achieving the goals of protecting the privacy of individuals rather than curtailing the surveillance activities of organizations or of the state. Although surveillance has been an important, and recurring, theme in the literature on privacy (Rule 1973, Burnham 1983) policy concern has been directed at the effect of surveillance on individual privacy, not on society in general. This emphasis on privacy and individual rights has made for good political rhetoric and helped to capture the attention of the public and policymakers. But it has not provided a sound basis upon which to formulate public policy. Time and time again, privacy issues appear on the public and congressional agenda. But only rarely does privacy legislation pass.

And the legislation that does pass is responsive to a rather limited concern. In comparison to legislation in many other countries, the US response has been a patchwork of protections (Bennett 1992, Flaherty 1989). American policymakers have eschewed an omnibus approach to privacy problems, favoring instead a preference for sectoral policies and incremental change. In each instance proponents have to have compelling arguments in order to convince policymakers that legislation is necessary. The natural inclination of policymakers is to avoid regulation and state action. Proposals to establish some form of privacy agency, either of a regulatory or advisory nature, have been roundly defeated time and time again.

Instead, suggestions of 'self-regulation' from opponents of legislation resonate quite successfully. This can be seen most clearly in the case of proposals to legislate to protect privacy online. The theory of self-regulation as applied to privacy issues is that if privacy is important to consumers, then online organizations will respond to the perceived consumer demand and will provide privacy protection. The market will respond and outside regulation will not be necessary.

The counter-argument, in part, is that the information world does not represent a perfect market and that market failures, in particular asymmetries, need to be corrected. Advocates of self-regulation recognize the legitimacy of some of these concerns but respond that the online marketplace is still evolving and that the threat of government regulation, largely provided through media and public interest oversight, will provide additional incentives for effective self-regulation. As demonstrated by the lack of legislation and weakness of FTC responses, concerns about stifling market and technological innovations have trumped concerns about the commodification and misuse of personal information in the online environment.

Two other cultural or traditional aspects of privacy policy require mention. The first is that action on privacy issues occurs when the middle class becomes concerned. This is first illustrated by the passage of the Fair Credit Reporting Act in 1970, which is sometimes defined as the first 'privacy' legislation

(despite the fact that the concern was not motivated by privacy and the legislative scheme does not fully embrace the code of fair information principles). The middle class, which was seeking credit for a range of purposes, became concerned about the information upon which decisions would be made and concerned about who would have access to that information. The credit card industry, which wanted to expand its customer base, acquiesced to legislative requirements. This pattern continues for all subsequent privacy issues. It is not sufficient that policy elites and privacy advocates support legislation. Such legislation also needs broad based public support. As I have noted, such support is often garnered as a result of human interest stories in the media. Current public anxieties over identity theft fit the pattern discussed here.

The second cultural aspect is the American distrustful attitude toward government and generally more trustful attitude toward the private sector. Traditionally, and as certainly occurred during debates on the appropriate scope of the Privacy Act in 1974, Americans feared the 'big brother' Orwellian features of government computer systems. The fact that government *compelled* the collection of certain information, especially financial information for tax purposes, added to the fear that government might use information in ways that people did not realize. Similar private sector collection of information appeared less threatening because people believed they had some choices as to what they would disclose (keeping money under the mattress rather than banking it) and that the private sector was fragmented in its information collection. This cultural aspect began to be less compelling in the late 1980s and 1990s as people recognized the vast and myriad exchanges of information that were occurring between the public and private sector, and within the private sector. At least until 9/11, the 'baby brothers' are perceived as being equally powerful and threatening as 'big brother'.

## WINNERS AND LOSERS

There is something of a 'David and Goliath' character to the privacy policy landscape in the United States. In almost all instances, privacy advocates are challenging large organizations. Generally, privacy advocates do not win. But sometimes they do. When they win, several factors appear important.

First, privacy advocates may align themselves with other groups which for independent reasons support privacy legislation. Politics does make for strange bedfellows and one-time coalitions can be quite effective in achieving passage of legislation. For example, passage of the Electronic Communications Privacy Act depended on a coalition of privacy advocates and new industry entrants who realized that consumers would not use their new systems unless industry could ensure a certain level of privacy.

Second, trade-offs may be possible where a group realizes that it needs to compromise in order to achieve goals. For example, the financial industries knew that in order to achieve their goal of modernization and consolidation they would need to accept some restrictions on their personal information practices and provide some rights to individuals – leading to the passage of GLB.

Third, privacy advocates may align themselves with broad based public interest groups leading to more long-term coalitions and working relationships. This was particularly true in passage of the Children’s Online Privacy Protection Act where privacy advocates worked with media and consumer groups. Groups with broad ‘good government’ interests, such as the Free Congress Foundation and Public Interest Research Group, have been part of the alliances advocating more protection for online privacy. Privacy advocates are increasingly seen as mainstream with an issue of increasing public appeal rather than as fringe groups with a narrow perspective. This, however, may come at some cost to the privacy community as groups such as EPIC and CDT differ at times on questions of strategy and tactics.

Fourth, the ‘big guys’ are not always unified in their position. In the area of online privacy, for example, the big guys are not all big. Industry leaders have been very attentive to privacy concerns and have tried repeatedly to respond to those concerns in a way that best suits their interests, that is to champion ‘self-regulation’ and to engage in activities that represent self-regulation, such as the formation of the Online Privacy Alliance in 1998. However, if the ‘bad guys’ among these big guys do not follow the industry leaders then the missteps of the bad guys will hurt the industry leaders as well.

Fifth, a policy entrepreneur on the inside of the political system appears to be a necessary ingredient for legislative action. In the late 1960s and early 1970s, Senator Sam Ervin played a pivotal role in keeping the issue of information privacy on the congressional agenda and in securing passage of the Privacy Act of 1974. Given the number of initiatives and forums, leadership is necessary to overcome inertia and the tendency to wait on the actions of others. In Congress, Senator Leahy and Representative Markey have both been long-time champions of privacy generally and online.

## INFORMATION FLOWS AND CONSTRAINTS: SUCCESS AND FAILURE

Even where privacy protections have been legislated, there is little evidence that they have worked to the advantage of individuals. In most instances, the costs associated with protecting privacy are shifted to the individual in terms of time to monitor privacy notices and practices and time and often money to

pursue redress of grievances, which rarely benefit the consumer in a meaningful way. Additionally where legislation requires organizations to behave in certain ways, for example provide notices, organizations have often done so in a manner that is indecipherable to or burdensome for the individual. This is especially true with the way the financial industry has implemented GLB and the health care industry has implemented HIPAA.

In early 1999, Scott McNealy, the Chief Executive Officer of Sun Microsystems, stated that : 'Privacy is dead. Get over it.' Despite being widely quoted and with some reported despair, privacy concerns are not dead political issues. The public remains concerned about many uses of personal information and, as has been true throughout the last 40 years, can be energized to take action. A recent example of this is with the enormous public participation in the Federal Trade Commission's 'do not call' list which restricts telemarketers' use of phone numbers on that list.

## PROSPECTS FOR THE FUTURE

At the current time, the primary issue for the future is likely to be the balance between security and privacy that has been renegotiated in the USA PATRIOT Act and its reauthorization. Related to this is the debate about about a National ID system and proposals to standardize drivers' licenses for national identification purposes. Since 9/11 there have been several proposals for the creation of a national identification system, most notably that of Larry Ellison, the head of Oracle Corporation, who immediately after 9/11 offered to donate the technology for such a system. On Memorial Day in 2004 *The New York Times* editorialized in support of a 'serious discussion of how to create a workable national identification system without infringing on the constitutional rights of Americans' (*NYT* Editorial Board 2004). The *Times* took note, as others have before (EPIC 2002), of the inappropriateness of the driver's license as a *de facto* national ID. The American Association of Motor Vehicle Administrators convened a Special Task Force on Identification Security which recommended that Congress require states to standardize driver's licenses in terms of eligibility, proof of identity, license content, and document security. Such a proposal was introduced in Congress as the Driver's License Modernization Act of 2002 (HR 4633).

Proposals that look anything like a national ID card have been broadly and consistently rejected. National ID cards are generally seen as 'solutions in search of a problem' (EFF 2002). Suggestions to use the SSN as a national ID were rejected in the early 1970s by the Nixon and Ford administrations, again in the late 1970s by the Carter administration, and yet again in the early 1980s by the Reagan administration. The Clinton administration's health care reform

revisited and again rejected the idea of anything that might be seen as a national ID card. In each of these cases opposition to a national ID card came from liberals, who are concerned primarily about the civil liberties implications, and conservatives, who view the cards as representing big government. And in each of these cases debate centered on whether the card addressed an actual problem and was a solution to that problem, whether it was cost effective, whether it could be protected against abuse, and whether its use would creep into other, unsuitable, areas.

And so the idea for a national ID card has been resurrected in the wake of 9/11. This time the debate is beginning with a more sophisticated understanding of the complexity of what an ID card would entail. The focus is less on the 'card' aspect and more on the 'system' aspect. A committee of the National Research Council issued a short report on some of the policy, procedural and technological questions that should be carefully addressed in even thinking about designing and implementing nationwide identity systems. The title of that report, *IDs – Not That Easy*, captures the committee's sentiment that 'more analysis is needed . . . [beginning with] a clear articulation of the system's goals and requirements' (National Research Council 2002, 46). The more recent proposals for a national ID card also tend to include a requirement for some 'biometric' identifier generating additional policy and value issues, as well as technical questions about whether such identifiers are unique for such a large population (Waymann 1997).

The idea of a national ID card and system is likely to receive more policy attention over the next several years. Airlines are considering a version of a frequent-flier security pass so that frequent fliers could go through a rigorous security pre-screening process and obtain a card to reflect that which would then speed them through security lines. Such a proposal for a voluntary, biometric-based ID card called the V-ID, has recently been advocated by Steve Brill, the founder of the American Lawyer and Court TV, in partnership with ChoicePoint, TransCore, and Civitas Group (Cotts 2003). In addition to various questions of design and effectiveness, as *The New York Times* editorialized, such a card would create 'a two-tiered security world where the haves zip through lines and have-nots wait endlessly and endure personal searches' (NYT Editorial Board 2004, A16).

In testimony before Congress on the proposal for a tamper-proof Social Security card that looked like a national ID card, an economist at the CATO Institute noted 'bad ideas never die in Washington; they wait for another day' (Moore 1997). The debate over information privacy in the United States has by no means been brought to a close. Good ideas and bad ideas will continue to be presented, and incremental change will continue most likely to chip away at privacy, but not kill it.

## 3. Germany

### Wolfgang Kilian

---

For post-war Germans, sensitivity to the need to protect personal information came easily. Recent historical experience of totalitarian government combined with long-standing intellectual and cultural themes made Germany one of the first countries in the world to adopt privacy protection codes. To this day, concern over treatment of personal information remains acute among Germans. The growing familiarity with information technology among the German population facilitates the understanding of the concept among citizens and consumers. Public awareness of the data protection issue is high.

Early evidence of these sensitivities came in the unexpectedly indignant public response to the planned census of 1983. Under a new federal statute (Census Act of 1983), every family was to respond to an extensive questionnaire requiring personal data on matters ranging from living conditions to education to leisure activities. Data so provided were to be used both for government planning and for population registers used by local government administrators.

As it turned out, these demands on Germans' privacy triggered stiff resistance – from left-wing activists, consumer protection groups, civil libertarians and others. Many called for civil disobedience; media coverage was intense.

In a nearly unprecedented action, privacy advocates filed a complaint with the Federal Supreme Constitutional Court, demanding suspension of the Census plans. To widespread surprise, they won. The Court declared the Census statute partially unconstitutional (BVerfGE 65, 1 – *Census Case*). The immediate result was to reduce some 40 million questionnaire forms to a heap of worthless waste paper.

The Court based its findings on a novel interpretation of two guarantees in the German constitution – the 'right to free development of one's personality' (Article 2, paragraph 1), and the 'right to human dignity' (Article 1, paragraph 1). The Court accepted arguments by two law professors<sup>1</sup> on behalf of the activists that these constitutional rights must include what they termed a right

---

<sup>1</sup> Prof. Wilhelm Steinmüller/University of Regensburg (later Bremen); Prof. Adalbert Podlech, University of Heidelberg (later Darmstadt).

to ‘informational self-determination’ (‘informationelles Selbstbestimmungsrecht’) – a doctrine the appellants held central to a free society. In this view, everyone should be able to know what other people or institutions know about him or her, and should be permitted to control the flow of his or her personal information. No one should be deterred from exercising basic freedoms by fear of having personal data stored in public databases.

Because even seemingly trivial forms of personal data can be combined in ways that are troublesome for the individual, the reasoning in the *Census case* yielded some important repercussions in privacy law and policy. A mechanism for guaranteeing the right to individual self-determination emerged involving several legal principles: every use of personal data intrudes upon personal freedom and therefore requires legal justification. Such justification of the processing of personal data must be obtained only with respect to a certain purpose and either from statutory law or from the individual’s informed consent.

This corresponds to earlier rulings of the Federal Civil Court on the unauthorized disclosure of private photos, letters, or documents (BGHZ 30, 7 (*Caterina Valente*); BGHZ 50, 133 (*Mephisto*); BGHZ 131, 332 (*Caroline v Monaco II*); BGHZ 143, 214 (*Marlene Dietrich*)).

The Court also introduced some additional side aspects: a digital profile resulting from the combination of data on one’s behaviour, relations, living conditions, financial status and similar characteristics would mirror a person’s total personality and would therefore conflict with the right to individual self-determination. No objection was made where personal data are anonymized, if they bear a low probability for being re-personalized. For all kinds of personal data, technical measures should be introduced in order to prevent misuse.

The significance of this decision was far-reaching. The Constitutional Court essentially affirmed people’s right to control use of information about themselves unless compelling general interests require legislation to limit a state’s prerogative of limiting such freedom by laws. All in all, the case was a major victory for civil libertarians. In the following years, this decision formed the context for all sorts of personal data use by federal and state government agencies – including those engaged in health care, policing, education and research.

Even intelligence services were bound, for the first time, to observe these rules. True, subjects of police or intelligence files were not permitted access to ‘their’ data in these cases. But the holders of such information were subject to systematic external monitoring by parliamentary commissions and personal data protection commissioners.

To date, the *Census case* remains the most important legal precedent in German privacy protection law. It is widely cited in other court decisions as well as in privacy protection literature more generally. Its logic had considerable

influence on the framing of the European Directive on Privacy of 1996, which now forms the basis for privacy codes throughout the European Union.

## DIMENSIONS OF GERMAN PERSONAL DATA SYSTEMS

As in other prosperous countries, both state and private organizations in Germany maintain a vast variety of data systems on private persons.

In the public sector, the biggest system is that maintained by the Deutsche Rentenversicherung,<sup>2</sup> the state social security administration. This association of pension schemes maintains files on some 51 million persons (2003), each record containing data on contributions throughout the person's working life and on pension schemes. These data are subject to detailed regulations aimed at protecting people's rights over data on themselves.

In the private sector, the biggest system is that maintained by the 'SCHUFA', holding data on some 63 million consumers (2005). Owners of this system are the country's banks, credit institutions, retail traders and other service providers. In 2005, the SCHUFA sold some 1,069,000 credit reports; about 53 per cent of these included credit scores. As in the United States and other countries where credit reporting flourishes, these reporting activities serve to identify consumers whose habits make them bad credit risks for the participating businesses.

Another major private-sector data-base is that maintained by 'Payback',<sup>3</sup> a marketing company. Payback collects data on German consumers' spending habits, organizes rewards in the form of discounts to customers and provides consumer relations data to the cooperating big enterprises. Five hundred million transactions per year have been documented.

Both Schufa and Payback require consumers' formal consent in order to store their data. But it is not clear whether the structures, purposes and kind of exploitations of personal data in these systems are transparent to the consumers. Some elements of both systems may actually be unlawful (LG München 1.2.2001 12 O 13009/00; Weichert 2000).

German law requires that both major enterprises and state agencies appoint privacy officers responsible for the safekeeping of personal data held by them. Groups of companies often name a '*Konzerndatenschutzbeauftragten*', or group privacy commissioner, who is responsible for co-ordinating privacy policy for the group worldwide. These responsibilities extend activities to enterprises having their place of business in countries without privacy codes of their own.

---

<sup>2</sup> [www.deutsche-rentenversicherung.de](http://www.deutsche-rentenversicherung.de); [www.vdr.de](http://www.vdr.de).

<sup>3</sup> [www.payback.de](http://www.payback.de).

The nation's highest privacy protection officer is the Federal Data Protection Commissioner, a high-level civil servant. He is elected by the Federal Parliament by a two-thirds majority decision and is therefore independent in privacy matters. His annual reports to the Federal Parliament (*Deutscher Bundestag*) always gain special consideration in press and on TV. The same is true for the 16 data protection commissioners at state (*Land*) level. Their reports describe cases, conflicts and solutions and give recommendations – thus creating public awareness. A famous example was the German Railcard Case in which the State's and Federal Data Protection Commissioners went public and achieved transparent procedures for obtaining the consent of customers for the processing of their data.

## HISTORICAL DEVELOPMENT

The idea of creating a special data protection law in Germany (and in the world) was born in the State of Hessen in 1970 (*Hessisches Datenschutzgesetz*). The first Data Protection Act of the world was put into force on 30 September 1970 (*Gesetz- und Verordnungsblatt für das Land Hessen*; Osswald 1970; Birkelbach 1974). The purpose was to protect all digitized material of public agencies within their responsibilities against disclosure, misuse, alteration or deletion by civil servants. The aim was not to set special terms for the obtaining and storage of personal data. However, if personal data became part of an official document, they had to be accurate; if not, the data-subject was granted the right to rectification. A key innovation was to create an independent institution named data protection officer (*Datenschutzbeauftragter*) whose responsibility was to uphold the confidential handling of citizens' data. This independent institution later became a success story and remains an integral part of the European data protection legislation today.

On national level, the first bill for a Data Protection Act in Germany was launched in 1972 (Bundestags-Drucksache VI/2885; Bundestags-Drucksache VII/1027). The bill was made the subject of a scientific conference in 1972 with support of the Deutsche Forschungsgemeinschaft (German Research Council) (Kilian/Lenk/Steinmüller 1973). It took until 1977 for the first national Data Protection Act in Germany to come into force, four years after the respective Swedish Act (Datalag, SFS 1973, 289). By 2005, at least 50 states in the world had enacted data protection legislation (Privacy International 2004). Some international agreements came into existence (Council of Europe 1985). Data protection turned out to become a worldwide phenomenon.

Data protection in Germany has philosophical, political and legal roots. Sensitivity to human rights in personal information has a long pedigree in the German philosophical tradition. Immanuel Kant (1724–1804) and his successor Johann Gottlieb Fichte (1762–1814) developed a theory of individualism: Human beings own an individual ‘autonomy of will’ (Kant 1903, 433). That ‘will’ ought to be ‘reasonable’, which requires indispensable regard to the dignity of man without pursuing certain purposes or advantages (Kant 1903, 439). Only deliberate human acts, which are based on freedom to express an autonomous will (Kant 1903, 448), are permitted, otherwise they are prohibited (Kant 1903, 439). This concept has persistently influenced the structure of the German civil law system in the nineteenth and twentieth centuries up to the right to ‘individual self-determination’ relating to personal data.

In the early twentieth century – in the period long before the computer became a tool for processing personal data – police and other state agencies collected person related data of trade unionists, social democrats, homosexuals, disgraced scientists, Jews, gypsies, disabled persons, or other politically suspected persons. Those data, documented in manual files or paper registries, often led to prosecution, dismissals or the destruction of careers. As the world knows, the consequences of such destructive record-keeping could include death. Particularly during the National Socialism regime, disabled persons, Jews and other groups were eliminated in concentration camps.

The end of the Second World War brought sweeping transformation of public values in Germany. The German Constitution of 1949 embodied defenses of the ‘dignity of man’ (Article 1, sec. 1) and ‘freedom to evolve one’s own personality’ (Article 2, sec. 1). German courts subsequently ruled that insults to a person’s honour, private life or reputation should require monetary as well as other immaterial compensation. In light of such principles, courts have often awarded damages for media stories or mandated withdrawal of photographs, statements, reports or stories concerning artists, well known persons or others whose images or other personal information were disclosed without their prior consent.

The rise of computing added a whole new dimension to these legal precepts – triggering the first personal data protection legislation in today’s sense. In the context of the German legal system, traditionally based on statutory law, computerization raised questions of how to cope with information technology, which created both hopes and fears. While the introduction of computers promised many benefits, the potential for misuse was intensely debated.

The first decade of data protection (1970–1980) in Germany was largely devoted to formulation of principles and rules governing data protection. The

second decade (1981–1990) was dominated by struggles between privacy interests and state collection activities. During the third decade (1991–2000), data protection in private companies came under scrutiny. The theme for the current decade (2001–2010) thus far appears to focus on the proper processing and use of personal data in global computer networks.

### **Decade One (1970–1980): Principles and Rules of Data Protection**

The first decade yielded a data protection paradigm defining a right to control information on one's personality, life or behaviour. At this stage data protection was not aimed at protecting data as such ('data security') but protecting those depicted in the data files.

The rationale of data protection law as it was developed by researchers and recommended for legislation (Steinmüller/Lutterbeck/Mallmann, 1972) turned out to involve the following five key principles:

- Processing of personal data encroaches upon a person's freedom (encroachment principle)
- Any encroachment must be lawful (legitimacy principle)
- The processing of data must be committed to specified purposes (specified purpose principle)
- The collection of personal data must be minimized in order to prevent misuse (caution principle)
- Effective control of the lawfulness of data processing must be maintained (control principle).

Under the 'encroachment' principle, each processing of personal data is considered an infringement on somebody's rights. Such use imposes a restriction on individual freedom to decide who should be entitled to access or benefit from one's personal data, and under what conditions. Since the German Constitution – like many others – defines and defends personal liberties, the encroachment by means of processing one's personal data generally conflicts with constitutional freedoms. To counterbalance those encroachments the principle of 'individual self-determination',<sup>4</sup> has been developed as

---

<sup>4</sup> The denomination 'individual self-determination' (informationelle Selbstbestimmung) was invented by Christoph Mallmann, *Datenschutz in Verwaltungs-Informationssystemen*, München/Wien 1976, S. 47–79, and later clarified by Adalbert Podlech, *Kommentar zum Grundgesetz für die Bundesrepublik Deutschland*, ed. by Rudolf Wassermann, Neuwied/Darmstadt 1984, Art. 2 Abs. 1, 66, from a constitutional point of view Textno. 44f., 77 ff., who introduced the term into the proceedings of the Census case, where he was one of the plaintiffs.

an embedded constitutional right. The new term seems to exclude tasks carried out in the public interest or in the exercise of official authorities' duties based on personal data. But legitimate interests never have been excluded by individual self-determination. However, conflicts of interests between private and public interests may evolve.

Under the 'legitimacy' principle, any appropriation of personal data requires specific legal authority. Such authority can be forthcoming either from a legal statute or the explicit consent of the person concerned.

In a democratic state, where the rule of law prevails, a restriction of personal freedom requires legal justification. For uses of personal information, such justification may be provided either by statute, or by the explicit consent of the data subject.

In addition no legitimacy justification was considered for organizations developing codes of conduct for data protection. From a German point of view self-given rules of organizations are not capable of replacing explicit consents or statutory laws. Codes of conduct may be deployed as complementary instruments creating legitimacy.

Lawful processing requires that the uses of personal data must be known and publicly stated at the time of collection. Uses that go beyond these stated purposes require new legal justification. Otherwise, the data processor and not the person who the data are related to, would decide upon the use of the data. But such 'purposes' can be stated in many ways ranging from the explicit to the utterly vague. Therefore, the definition of a certain purpose must be determined in relation to a respective subsystem of application.

The following examples may illustrate the point at issue:

In a recent decision of a District Court the demand of a public prosecutor investigating a criminal case (purpose 1) to access personal data stored on a GSM-SIM card of an on-board-unit in a truck was denied (LG Magdeburg DuD 2006, 375). The reason was that the Federal Toll Collect Act (*Mautgesetz*), on which the collecting of GSM-SIM card data are based, restricts the use of toll data to the control of toll payments (purpose 2). A similar discussion is pending whether 'data mining' – and 'data warehousing' – techniques which involve sophisticated profiling methods on a large scale are authorized by a consent related to 'marketing' or 'advertising' purposes (Podlech/Pfeifer 1998; Bull 2006; Weichert 2003).

The 'caution' principle holds that the best way to prevent misuse of personal information is to avoid collecting it in the first place. Thus organizations must only collect the minimum amount necessary to comply with legal obligations or to achieve a legitimate purpose.

The 'control' principle requires that personal data use be subject to supervision in the interest of individual rights. Data subjects should be able to access the database and insist upon disclosure, rectifications, erasure, or blocking of

data if the workings of the system are not lawful. Moreover, an independent data protection commissioner must be responsible for monitoring the database and its use.

\*

The first federal Data Protection Act of 1977 sought to implement the above principles (Protocol No. 37) as developed by scientists consulted by the Federal Parliament (*Deutscher Bundestag*) (Steinmüller/Lutterbeck/Mallmann 1972) as well as in public hearings of scientists and interest groups. The Act, applying to both public and private sector personal data systems, follows the principle that every institutional use of personal data involves an intrusion on privacy and hence requires justification. Such justification may derive either from explicit legislation or from the informed consent of the data subject. But the Act also added an additional requirement:

As far as possible, personal data should be kept anonymous; identifying elements should be removed in order to prevent intrusions.

The range of application of this principle turned out to be narrow. Some databases in the medical field exist where the identifiers are kept separately. They are recombined only if knowledge of them is necessary for treatment of the patient or for research.

The anonymization requirement was a reaction to attempts since 1968 to introduce a so-called general personal identification number (*Personenkennzeichen*). It was originally planned to support passport issuance and to serve as 'general identifier' of a person in public and private life. The identification number was designed to comprise 14 digits including storage locations for birthday, gender, religious affiliation, area of living and some other information. Contrary to the common use of social security numbers in the United States of America or in Sweden, many Germans feared that the number might serve to cross-reference and connect diverse databases. However, while the national Parliament of the Federal Republic of Germany had rejected the introduction of a general personal identification number as early as 1968, the Parliament of the former German Democratic Republic introduced a comparable number in 1971 which was abolished after the reunification of both parts of Germany in 1990.<sup>5</sup>

---

<sup>5</sup> Actually it took until 1999 to phase the GDR identification number out. In Germany at present there exist substitutes to general identification numbers at the level of subsystems (health care; pension insurance; taxation) which bear the potential for pooling.

In the course of the introduction of the first federal Data Protection Act in 1977, the Federal Parliament imposed another far-reaching decision: it should not be possible to link data systems across affiliated, but legally independent enterprises. Insurance companies, for example, may not merge their databases of life insurance information with those on auto insurance. The risks involved must be separately calculated – so that consumers do not find themselves paying more for auto insurance, for example, because of their record of claims on their homeowners' policies. Thus, it became illegal to set up one centralized database for a group of companies or to link databases between economically cooperating, but legally independent enterprises. This structural decision was also aimed at preventing an easy disclosure of personal data out of different fields of activities.

Data security, a topic in which computer scientists show a major interest, was of relatively minor importance in the Data Protection Act. One provision stipulated the introduction of some technical precautions to prevent theft or other mishandling of personal data. The level as to which technical measures should apply was left undefined.

### **Decade Two (1981–1990): the Battle Against Public Administration**

In Germany as elsewhere, the Cold War period saw intense left–right conflicts in domestic politics. Activities of the 'Red Army Fraction' and other terrorist groups triggered enormous efforts to track and apprehend their members. In this atmosphere of widespread suspicion, privacy advocates struggled to create safeguards against excessive surveillance. Students, consumer organizations and civil libertarians warned of the dangers of totalitarianism, often referring to Orwell's *1984*. These groups often based their appeals on the principles laid down in the Supreme Constitutional Court decision in the 1983 census case (Podlech 1984, p. 85).

Well known is the judicial battle against the application of screening search methods ('*Rasterfahndung*') for identifying potentially suspected persons. The Federal Criminal Office demanded for example that private energy suppliers provide names and addresses of customers who consumed significantly less energy per square meter in their residences than the average. The presumption was that those customers were moving around for the purpose of planning terrorist attacks. The inventor of these screening methods, the President of the Federal Criminal Office, Horst Herold (his slogan was: 'We get them all') was removed from office therefore in 1981 by the Federal Minister of Interior (Hauser 1998). In a case from 2006 concerning the screening of personal data by police the Federal Supreme Constitutional Court approved an appeal of a Moroccan student. The Court ruled that even in the wide context of the events of 11 September 2001 a general threat does

not legitimate the preventive application of screening methods unless a concrete danger appears (BVerfGE 115, 320 ff.). The interpretation of the term 'concrete danger' was not specified by the Court.

### **Decade Three (1991–2000): Private Business and Data Protection Law**

From the beginning the German Data Protection law addressed the processing of personal data in public administration as well as in private businesses. The same principles as developed in the Census case and as transposed into the second German Data Protection Act of 1990 apply. Unlike the Anglo-American law tradition the amount of self-regulation allowed under German and European law is rather small, never replacing state regulations.

During the third decade of data protection law in Germany special consideration was given to data processing in private businesses (Killan 1982). All major companies converted their paper files into databases and deployed powerful IT-systems. This development resulted in fears that the companies would process and evaluate personal data not only for legitimate purposes but also for data mining, unfair supervision, unsolicited marketing, illegal profiling or circumvention of works councils' participation in plant decision-making.

Particular anxieties surrounded company use of employee data – collected for a variety of routine administrative purposes. Some of the company-held data are compiled in connection with obligations to state agencies, such as taxation or social security. Combined with other data held by companies on their employees, such information could have serious repercussions on the lives of the latter. Dismissals may be based on sophisticated electronic evaluations of behaviour, attitude, skill, education or health status without employees having knowledge.

In one well-documented case, a company in Bavaria wanted to reduce its labour force without obtaining the obligatory consent of the works council. Based on data collected in their information system in their personnel system, the company terminated its bus connection to a remote residential area. The aim was to force resignations by young mothers who, without the bus, would no longer be able to combine family care and employment. Since the employees and not the company had given notice of the termination of their labour contracts, the company could avoid the intervention of the works council which could have been expected if the dismissals had been filed by the company. No lawsuit was initiated, but public awareness of potential misuse of information systems in personnel increased.

The Data Protection Act has no special provisions for labor market issues. But the Works Council Act of 1972 embodies some such protections.

It guarantees employees access to files on themselves held by management, and entitles works councils to be informed about administrative and planning matters concerning employees. One provision of the Works Council Act establishes the right of the councils to bargain over, or indeed to veto, introduction of technologies (like computer systems) used for employee surveillance.

The works councils entered hundreds of enterprise agreements stipulating terms for the introduction and application of hardware and software suitable for processing employees' data.

The result was to reinforce individual workers' rights over the processing of their data, making such protection an institutional matter, rather than a strictly private concern of workers. These protections have not prevented the introduction of computerized systems for employee records, but they have blocked uses of such systems for certain particularly privacy-invasive practices like secretly profiling of employee health status. The health status of an employee is a crucial aspect for decision making on plant level.

\*

Other private-sector uses of personal data triggering privacy concerns have to do with marketing. Any consumer using the telephone, fax, computer, interactive television or the internet automatically leaves traces of personal data. These data have come to have much commercial value – and clearly require protection of consumers against misuse of their data.

This may be realized by viewing the so-called 'SCHUFA-System' or the so-called 'Bonus-System'.

The SCHUFA, a private company, compiles records of consumers' financial status and credit use in much the same way as North American credit reporting agencies. Data from bank records, retailers' accounts, mortgages, insurance accounts and other financial relationships are compiled in SCHUFA's centralized systems – where they can be accessed by businesses. It is impossible to open a bank or personal credit account without granting the bank in question permission to access one's SCHUFA file.

Data held by the SCHUFA can have severe consequences for consumers. SCHUFA creates and disseminates credit scores on consumers, ranking their desirability as credit risks on a scale from zero to 1000. German data commissioners have intervened against this system and secured the addition of a 'SCHUFA clause' in line with the Data Protection Act. This provision makes the activities of the organization more transparent to consumers and grants them the right to access their SCHUFA files and correct false information.

But the status of the SCHUFA's allocation and dissemination of personal credit scores to 62 million consumers is still unsettled. The SCHUFA claims that this scoring system is statistical, rather than consisting of personal data – and hence not subject to the Data Protection Act. This disingenuous interpretation is still under legal challenge.

In another SCHUFA-related case, a consumer brought a suit against the organization for reporting data from another consumer with an identical name. The first consumer claimed damages because the faulty report portrayed him as an unreliable credit risk – a report that the SCHUFA submitted to a bank without adequate verification. But the Federal Civil Court denied compensation to the first consumer, on the grounds that the SCHUFA was not obliged to verify data submitted to it from its institutional sources (BGH NJW 1978, 2151).

This decision has triggered much criticism, on two grounds. First, it demonstrates a weakness in the Data Protection Act – its lack of a rule establishing liability for damages resulting from misuse of personal data. Second, the finding that the SCHUFA had no obligation to verify data that it transmits is not convincing, as it allowed the bank that reported the faulty data to the SCHUFA to evade responsibility. In this case, if the consumer who suffered from the mistake had sued the bank that originally provided the erroneous data, he would probably have prevailed.

Another private-sector operation generating much privacy concern is the Schober Information Group<sup>6</sup> a publicly-traded German company devoted to collecting and selling direct marketing data. Its more than 600 employees store addresses of some 50 million private consumers, 5.5 million companies, and some 3.7 million managers. They compile data from 'lifestyle questionnaires' submitted by ordinary consumers, geo-coded evaluations of the worth of some 19 million houses based on nine criteria, and some 5 million private email addresses. The company's annual turnover is some 130 million Euros. The Schober Information Group relies heavily on scoring and data mining.

Another major private-sector compiler of personal data is Germany's 'Bonus Card System'. This system tracks consumers' spending at most shops and qualifies them for discounts on the basis of their expenditures. Advantages to consumers are usually not great; a consumer has to spend 2000 Euros to obtain a discount of ten Euros. Participation in the system is of course voluntary, but consumers do participate, as there is no alternative source of discounts on these purchases. The former German Discounts Act (*Rabattgesetz*) entitled consumers to bargain for up to 3 per cent, which was

---

<sup>6</sup> <http://www.schober.com>.

three times more. The new Bonus Card System curtails German consumers' option for a discount.

In the year 2000 entrepreneurs founded clearing houses<sup>7</sup> to create transferability of points earned for expenditure at one establishment for discounts elsewhere. These enterprises now compile data on some 25 million consumers, collecting personal data on participants' shopping activities in many locations. Thus the clearing house is apt to store information on purchases at gas stations, shoe shops, hotels, dental clinics, nightclubs and countless other establishments.

Consumers generally do not understand the workings of these data systems. All that most Germans notice is that purchases in various places eventually generate small discounts much later. In the meantime, it appears that the holders of the consumer information are using the data to profile buying habits and to exploit them for marketing purposes. Thus far, these practices have not been subjected to court challenge.

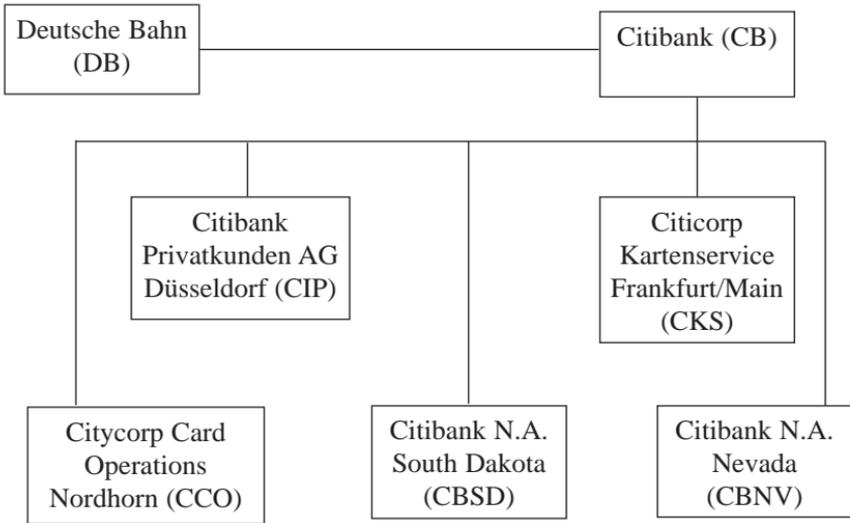
Perhaps the most dramatic and revealing confrontation between German data protection expectations and private-sector practices came through the activities of Citibank. This major New York bank, seeking to establish a marketing position in Germany, proposed a joint venture with the German National Railway in 1996 (Dix 1996). Citibank would issue rail travelers a card combining several attractive features. The card would afford reductions of 50 per cent on the cost of train tickets, *and* provide a Citibank Visa credit card. Because Citibank expected some 10 million travelers to accept their offer, they were prepared to issue the cards at no fee. But as part of the deal, applicants for the cards were expected to accept additional collection of personal information on themselves including income, profession and job status, financial obligations and the like. These data were to be stored and processed in the United States.

Citing the inadequacy of privacy protection under American law, German data commissioners intervened, explaining to customers that they had a choice of purchasing railway discount cards with or without the added Visa card. Those consumers preferring not to provide their financial status data (and therefore remain ineligible to receive a Visa card) could still obtain the railroad card.

It turned out that only 15 per cent of the railroad card holders were willing to contract for the Visa card – despite the fact that it was offered free (for the first year), and despite Citibank's statements that it would follow German data protection laws in processing consumer data in the USA. Ultimately, Citibank terminated this project, because of insufficient response.

---

<sup>7</sup> [www.payback.de](http://www.payback.de); PAYBACK Rabattverein e.V. Munich.



*Figure 3.1 International Data Protection contract, German Train (DB) – Citibank (CB) and subcontractors*

Clearly German consumers mistrusted this American-style marketing scheme as well as the protection of their financial data in the USA.

\*

In the first decade of the new millennium, data protection involves coping with remote databases, global networks, global positioning systems, ubiquitous computing, sophisticated software and clashing values. How are people to invoke rights over ‘their own’ data, when it is unclear who (if anyone) is formally responsible for their safe-keeping, where the data are located, or what law applies to its use and what court has competence to decide? Shopping on the internet may involve transmission of personal data to distant and unknown locations – to be used according to unknown ground rules. Concealed imposition of ‘cookies’ for profiling internet activities may be forbidden by national data protection law, yet almost impossible to avoid technically. Law and policy need to be adjusted to meet these new realities.

One might conclude, in view of these facts, that data protection is an outdated legal concept. But the contrary is true. Existing concepts and codes must be adjusted to technical developments if we want to preserve human dignity and freedom.

At the national level, legislators may seek to define criteria that serve as connecting factors indicating the legal systems to which the factual situation under consideration is related because the activity takes place there (*lex loci actus*) or the good is located or presented there (*lex rei sitae*). According to German law the latter principle applies for example if an offer on the internet was placed in German language and appeared on a screen located in Germany, independent of the location of the server. The German Private International Law (Conflict of Laws) includes provisions like the 'ordre public' (Article 6 EGBGB) which prevents the application of inadequate foreign law in case of conflicting basic national legal principles.

In the 'global village', the range of application of national law is limited. German data protection law is embedded in European law. European law to some extent depends on international law for example the World Trade Organization General Agreement on Trade in Services (WTO-GATS).

At present, four different data protection regimes prevail in different parts of the world. In Europe, the EC 1995 Privacy Directive (95/46/EC) governs practice among all 27 member states. In addition, Iceland, Liechtenstein and Switzerland have also transposed this important code into their own national legislation according to the European Economic Treaty. In a second zone, one might locate countries judged by the European Commission to provide an 'adequate level of protection', in the language of the Directive. These countries include Canada, Argentina, Guernsey and the Isle of Man – all of which may now accordingly receive personal data collected within the European Union without problems.

A third zone is made up of countries with data protection legislation not meeting EC standards of adequacy, notably, the United States. Personal data may be transferred to those countries only under special circumstances, like the war against terrorism, or if special privacy safeguards are provided by appropriate contractual clauses.

The fourth zone includes all states lacking data protection legislation unwilling to provide safeguards in contractual terms. Those states may be excluded from the transfer of data originating in Europe.

Whether the four zones with respect to data protection will divide the world and will function in practice may be questioned. However, the differentiation conforms with Article XIV lit. c ii of the WTO-GATS Treaty according to which restrictions on trade in services are permissible for data protection reasons. Thus, data protection principles take priority over the principles of free trade in services. But from a practical point of view the division into different data protection zones will hardly prevail within a technical environment of world-wide open communication networks. Geographical differences in data protection law which range from zero regulation to a high level of protection provide an inadequate response for a global network society.

## PUBLIC OPINION AND DATA PROTECTION

As New York's Citibank learned to its chagrin, collection of sensitive personal data triggers alarmed reactions in most Germans. If well informed, the majority hesitate to consent to appropriation of their data unless the advantages of doing so are conspicuous. The reports and other public statements by German data protection commissioners attract much interest.

The annual 'Big Brother' awards conferred by privacy watchdog organizations target a range of practices that many Germans find anxiety-provoking (Big Brother Awards 2007).

'Awards' were granted for 'future stores' employing RFID techniques<sup>8</sup> for the storage of IP-numbers of flatrate clients,<sup>9</sup> for a digital rights management system,<sup>10</sup> for breaching the confidentiality of addresses<sup>11</sup> and for an intensive questionnaire for ordering tickets for the World Soccer Cup in 2006.<sup>12</sup>

\*

One recent such award went to companies that include RFID chips in their products. The RFID technique is an innovative technology developed by SAP, IBM, Intel and some 60 other cooperation partners in the IT, consumer goods and service industries to develop the retail business of tomorrow. The Radio Frequency Identification (RFID) makes it possible to identify objects unequivocally and without optical contact using radio waves. A numerical sequence called Electronic Product Code (EPC), which is stored in a chip attached to any product, encodes details of the associated product. The chip is equipped with an antenna and communicates with a RFID reading device. Via a connection to the company's merchandise management system the supply chain as well as the customers' shopping records are documented. Data generated by post-purchase transmissions reveal buyers' shopping behavior and product preferences. In so doing they help target the customer for direct marketing. Whether the coming into existence of huge databases may be prevented by use of so-called 'de-activators' of RFID chips after a purchase takes place or whether, on the contrary, electronic agents based on the customer's record will advise him after shopping is under discussion.

---

<sup>8</sup> Metro AG, 2003.

<sup>9</sup> T-Online, 2003.

<sup>10</sup> Microsoft Inc., 2002.

<sup>11</sup> Tchibo Direct GmbH, 2004.

<sup>12</sup> World Soccer Games Organisation Committee for the German Soccer Association, 2005.

Privacy activists have challenged such practices, on the grounds that they may fuel vast databases without the consent or even knowledge of consumers. Courts have not yet ruled on such challenges.

The storage of Internet Protocol (IP) numbers of flatrate customers was introduced by Deutsche Telekom, a private telecommunications provider of which the government is the biggest shareholder. IP numbers make it possible to link via internet service providers the use of a computer to the communications data of a user. Because of the flatrate regime the identity of a person or the time he spent in internet communications do not matter at all. The competitor of Deutsche Telekom, Lycos Europe, does not resort to IP number storage. The storage of IP numbers of Deutsche Telekom AG customers therefore serves for the supervision and control of their communications, which may be of interest to Deutsche Telekom AG, the police and secret services but not for the internet user. One lower court in Germany ruled that the storage of IP numbers of flatrate clients violates the Tele Services Data Protection Act because neither statutory law nor a consent of the internet user authorizes storage.<sup>13</sup>

Digital rights management systems are software programmes aimed at controlling the use of copyright licenses. The introduction of Microsoft's 'Media Player' was combined with a Digital Rights Management System (DRM) called 'Palladium', which is appropriated to control the proper use of content in the Media Player in accordance with licensing rules. Thus, the Media Player not only affords the reproduction of music and pictures but at the same time the compliance of the Media Player's owner with Microsoft's licensing conditions. The control mechanism as embedded in the DRM software may conflict with the user's right to download a copy for private use.

In another novel appropriation of personal data, sports fans seeking tickets to the 2006 Soccer World Cup were required to fill out questionnaires. These required the applicants' names, date of birth, nationality, phone numbers, email addresses, passport data and supporter relationship to a football club for security purposes. The data were stored in a database and an RFID chip integrated into the ticket made it possible to refer to that database electronically. An intervention by consumer protection agencies forced the organizers to include a special question in the questionnaire as to whether the applicant agreed to commercial exploitation of the personal data they provide (Mayer 2001). In fact, commercial use of the data was planned, in addition to their use for security.

---

<sup>13</sup> *Teledienstedatenschutzgesetz AG Darmstadt*, 30.06.2005, 300 C 397/04, see: [www.ag-darmstadt.justiz.hessen.de](http://www.ag-darmstadt.justiz.hessen.de), homepage (last accessed 25 June 2006).

All tickets were sold exclusively by order and on account of the German Football Association (*Deutscher Fußball-Bund* – DFB). The tickets were electronically controlled ‘to guarantee security and to prevent ticket sales on the black market’.<sup>14</sup> However, a black market came into existence and the electronic turnstile barrier control finally served to check the validity of the ticket and to prevent unauthorized double access. Whether a commercialization of the soccer fans’ data has occurred remains unknown so far.

Contrary to other evidence of German privacy-consciousness, one detects a growing indifference to such values among younger Germans. I have in mind a generation who do not share the historical experience of the majority of the population and who are willing to expose even their personal feelings and sexual behavior without reservation to the public. The reality TV series, aptly named ‘Big Brother’, may serve as an example, since much money was paid to participants who were willing to exhibit their most intimate moments via the mass media. The resulting controversies on that topic did not result in any legal action. Therefore, the question remains undecided whether disclosures in these media productions are consistent with the interpretation of the German Supreme Constitutional Court in the Census case that human dignity is an overriding value.

If sexual behavior, pictures, feelings, attitudes, addresses, financial status and other personal data can be sold on the market, we may end up understanding data protection not as a matter of human rights but as a form of property rights. Personal data may become viewed as a commodity and a property rights system concerning personal data where license agreements about the use of personal data and the control of the use by digital rights management systems could come into existence. The existing distinction between personal rights and proprietary rights would be set aside.

## NATIONAL CULTURE, TRADITIONS AND VALUES

Again, German law recognizes a ‘right to informational self-determination’, a principle which is not laid down expressly in privacy codes. But this principle continues to manifest itself in German court cases.

German Supreme Courts, particularly the Supreme Constitutional Court, often refer to the constitutional ‘right to informational self-determination’ as protected by Article 2, paragraph 1 of the Constitution according to its interpretation. Recently, conflicts over information on medical patients, consumers and others have turned on the interpretation of this right.

---

<sup>14</sup> <http://fifaworldcup.yahoo.com/06/en/tickets/dpr.html> (last accessed 25 June 2006).

In one such case, a prisoner held in a psychiatric clinic was denied access to his health records. He wanted to identify the reasons for the revocation of the ease of his custody conditions.

The clinic was willing to grant access to individual 'hard facts' (laboratory data, electrocardiogram, electroencephalogram) but not to the diagnosis it had made of the prisoner's mental condition because of potential impacts on the results of his therapy and on the rights of the therapist. The court confirmed an earlier ruling that in principle all patient data including diagnoses are subject to the informational right to self-determination (NJW 1999, 1777). These considerations trumped the clinic's claim of an interest in restricting access for therapeutic reasons, on the grounds that a prisoner in a psychiatric clinic is forced to undergo medical treatments. An efficient legal protection of a prisoner as a patient outweighed the interest of the therapist or the clinic in preventing access to the diagnosis (BVerwG NJW 2006, 1116).

It is widely known that DNA screening, which can be based on the analysis of a single human hair, may reveal blood relationships. The German Federal Civil Court had to decide whether the exploitation of a collusively obtained DNA identification of a child could be taken into consideration for excluding the presumption of paternity.

This use was denied for the reason that every investigation and exploitation of a DNA identification causes an intrusion into the right of informational self-determination as protected by Article 2, paragraph 1 of the German Constitution as well as by Article 8 of the Human Rights Convention, Article 5 of the UNESCO Universal Declaration on the Human Genome and Human Rights and Article 16 of the UN Convention of the Rights of the Child (BGH RDV 2005, 62).

In another case, the German Federal Administrative Court ruled that mobile phone providers are not obliged to document their customers' identity card information for the benefit of state authorities, if those customers purchase prepaid phone cards which do not require that the user be identified (BVerwG 22.10.2003 NJW 2004, 1191). The decision invokes the 'caution' principle mentioned above, according to which the best way to prevent misuse is to avoid unnecessary collection of personal data.

\*

After the events of 11 September 2001, the German Federal Supreme Constitutional Court ruled several times against preventive empowerment of the police and secret services for screening, collecting or tapping personal data. The right to informational self-determination was held a constitutional right, subject to limitation only if concrete facts indicate a potential danger of planning or executing of terrorist attacks (BVerfG 4.4.2006 1BvR 518/02;

NJW 2006, 1939–1951). Regulations concerning supervision of communications must be concrete, well defined and proportional to counteract anticipated serious criminal offenses (BVerfG Urt. v 27.7.2005 1 BvR 668/04, MMR 2005, 674).

A provision allowing state agencies to place concealed microphones in private living rooms was held unconstitutional (BVerfG NJW 2004, 999; Stender-Vorwachs 2004). The use of global positioning systems against suspects in order to combat drug dealing or organized criminality, if approved by a judge on a case-by-case basis, was held constitutional (BVerfGE 112, 304 (GPS-Observation)).

However, the events of 11 September 2001 in the United States of America reversed the preferences for the power of use of personal data to some extent, even in ‘old Germany’.

If public security is deemed to be at stake, parliaments tend to give priority to state interests over civil liberties or individual interests. The number of statutory laws facilitating surveillance has increased. Even the core principle of informational self-determination is fading so far as state activities are concerned. No fewer than 26 amendments since 11 September 2001 have relaxed conditions for investigation, public surveillance, transfer of records or provisional detention of persons. Such measures obviously increase the power of the police and secret services. Many new provisions or amendments to existing Acts passed the German parliament in a rush, all facilitating the collection of information about people who may have or may not have any connection to terroristic activities.<sup>15</sup>

A new wave of Supreme Constitutional Court decisions permitted state monitoring of letters and phone calls (BVerfG NJW 2004, 2213 = BVerfGE 110, 33), seizure of data files from law firms (BVerfG NJW 2005, 1917 = BVerfGE 113, 29), surveillance of phone calls by national intelligence services (BVerfG NJW 2000, 55 = BVerfGE 109, 279), or locating persons via global positioning systems (BVerfG NJW 2005, 1338 = BVerfGE 112, 304; BVerfG NJW 2006, 1939). Transmission of personal data obtained by the German secret service to other state agencies is permitted where those transmissions are necessary to fight against money laundering, international terrorism and similar serious crimes, and if the principle of proportionality is observed (BVerfG NJW 1999, 55). Telecommunications data stored on private computers are governed by informational self-determination, which may be restricted, if a detailed, precise and proportional warrant has been issued (BVerfG NJW 2006, 976). Monitoring of electronic communications without having concrete

---

<sup>15</sup> *Gesetz zur Bekämpfung des internationalen Terrorismus vom 9.1.2002* (Law on the fight against international terrorism) BGBl. I 2002, p. 361.

facts against a certain person is illegal (BVerfGE 113, 348). The German Supreme Constitutional Court has proved so far to be the best data protection commissioner of citizens.<sup>16</sup>

Other courts followed the precedents and have ruled on wiretapping, fishing expeditions, broad searches on flimsy ground<sup>17</sup> or genetic analysis of a child for determining paternity without the consent of the child or its mother (BGHZ 162, 1). A big surprise was that nearly all decisions tended to restrict, to narrow or to control state power to enact extensive security regulations or demanded the introduction of procedural safeguards.

Thus, democratic and constitutional countervailing powers are asserting themselves. If we in Germany (and probably in other countries) wish to avoid a slippery slope towards totalitarianism – towards a state which recognizes no limits on its authority and seeks to control every aspect of its citizens' lives – we need counter-strategies in order to grant autonomous choices of objectives. For preventing a growing disfavour of data protection and for achieving an equilibrium between legitimate state interests and individual freedom the following measures are under discussion at present:

1. *Sunset-provisions*

Provisions introducing restrictions on individual self-determination should expire after a time limit.<sup>18</sup>

2. *Control of success*

New legislation including restrictions to individual self-determination should be monitored for success and potentially revised.<sup>19</sup>

3. *Reporting*

The number and sort of measures which limit individual self-determination should be reported.

4. *Transparency*

Notice should be given to persons who come unjustified under suspicion without being aware of the fact.

---

<sup>16</sup> The current vice-president was the former Data Protection Commissioner of the State of Hessen.

<sup>17</sup> OLG Frankfurt CR 2005, 830; LG Berlin CR 2005, 530; OLG Düsseldorf DUD 2005, 171; VGH Kassel NJW 2005, 2727; BVerwG NJW 2004, 1191; BGHZ 162, 1 (the latter case concerned the exploitation of a collusively obtained human genetic analysis of a child for determining paternity).

<sup>18</sup> First introduction: § 47 *Zollfahndungsdienstgesetz*.

<sup>19</sup> The efficiency of the new legislation is rather limited, see: Hans-Jörg Albrecht/Claudia Dorsch/Christiane Krüpe, *Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b. StPO und anderer verdeckter Ermittlungsmaßnahmen*, Freiburg 2003.

Parallel to these precautions it seems to be necessary to introduce and strengthen institutional control mechanisms, like class actions. In a global information society, a single person will not be in a position to defend his rights as granted in the Data Protection Act. Therefore, safeguarding individual rights by performing rights societies and mandataries may be favored. The protection of copyrights may serve as an example.

## WINNERS AND LOSERS

The roughly 35 years since the birth of data protection legislation in Germany have seen some gains for privacy interests, and some losses.

In the public sector, the period began with strong legal protections for personal data, many of which have been eroded by subsequent exceptions and qualifications. Hundreds of acts at the federal and state level have narrowed the informational self-determination of ordinary citizens – for example, in social security, taxation, health care or state security. Whether these measures have demonstrably contributed to state security is a matter for debate. But by any standard, they amount to a gain for state surveillance over individual privacy rights. The new acts provided legality not only for administrative purposes but also for various state actions against suspected or (increasingly) unsuspected citizens. From a libertarian point of view they did restrict personal freedoms.

In the private sector – that is, in their roles as consumers, employees, students, patients, drivers, and so on – citizens have benefited by creation of new advantages, if they are willing and able to assert their rights. They may gain access to ‘their’ data and control its processing.

Enterprises, on the other hand, have had to adapt to new demands – especially demands to make their personal data practices more transparent and to bring them into conformity with data protection legislation. Enterprises have to provide access to reporting and proper handling of personal data.

The most controversial sector in public discussions is the credit information and service industry – companies that report personal data. The sources are sometimes dubious, the procedures for processing and transferring data less than transparent. Because their activities are hard to monitor, the organizations involved have a good chance to evade data protection rules through scoring methods, data mining or presumption of consent from data subjects.

In the early days of privacy as a public issue, the greatest fears focused on government record-keeping and exploitation. Slogans such as describing the state as ‘big brother is watching you’ or books titled ‘private lives and public surveillance’ (Rule 1974) were well known. Later it turned out that, in the most advanced societies, the empowerment of enterprises rather than states

became the primary concern. Today's greatest privacy dangers stem from private sector activities like appropriation of data from electronic transactions and from rising state demands for personal data following the 9/11 attacks.

The transnational character of many private and public sector activities aggravates these problems: in the private sector global electronic markets demand transborder exchange of personal data and worldwide databases for customers of multinational companies have grown widespread (Scheja 2006).

In the public sector, cooperation among States on police, intelligence services and border control has dramatically increased the exchange of personal data within the European Union (for example, the Schengen Treaty and Schengen Information System) as well in transatlantic relations (as in the Passenger Name Record Agreement between the European Union and the USA).

Some claims on personal data, both in the government and private sector, stem from administrative needs that no one would deny. Those who administer tax or health care systems can hardly get along without some systematic recording of personal information. Companies obviously have little choice but to keep payroll records or data on job qualifications. But there is no reason to conclude that all personal information collected for any purpose must necessarily be made available for all purposes.

What we must develop is a realistic concept of data protection, which comprises the following components:

- Availability of personal data for well defined public demands without individual consent: the collection of tax data can not depend on the consent of a citizen. The amount of data collection for security reasons should depend on the assessment of concrete dangers and on the importance of values at risk.
- Availability of personal data for well defined private use in companies with consent of the person concerned: if a person gives an informed consent, the processing of personal data is covered as result of informational self-determination.
- Availability of a variety of scaled data security measures: strong security measures should govern highly sensitive data.
- Employment of intermediaries like performing rights societies for the protection of legitimate interests of the individual: in global networks individuals will rarely be able to execute their rights properly. Special service providers and agencies managing the identity rights of individuals could investigate and authorize use of personal data according to the individual's intent.

These realistic measures hardly amount to abandoning data protection. They

do, however, wear away at expectations that privacy can be secured strictly by initiatives of the data subject. The complexity of today's computer networks demands enforcement by data security measures, data protection commissioners, trade unions, consumer protection agencies, supervision by third parties and market mechanisms.

The EU–US dispute culminating in the so-called 'Safe Harbor' agreement shows that informational issues like data protection have the power to trigger trade wars. To prevent such disputes, third states should view data protection legislation as a part of quality standards for electronic transactions in goods and services which include personal data for promoting data protection. Such standards could ensure a certain level of protection in the processing and transfer of personal data; would assist the data subject in maintaining his individual rights; would provide transparency in the processing procedure; and could be exploited as marketing strategy for gaining advantages in competition.

\*

In an agreement concluded in 2004, the European Union Council of Ministers and the US government agreed to certain US demands for personal data on air travelers to the US. After much dispute, European airlines committed themselves to providing 34 forms of personal data on each passenger bound for the US – data which would be available to the US Bureau of Customs and Border Protection from the airlines' databases. These data included all contact addresses in the US, intended stops with the US former no-shows (absence without prior cancellation), contact addresses at home and in the US, email addresses and the like. According to the EU Council, American procedures reached the level of 'adequacy' required by the EU Privacy Directive to justify export of these data. The EU Council Decision of 17 May 2004 approved the bilateral agreement with the USA negotiated by the EU Commission, holding that the passengers' information was sufficiently protected according the adequacy criterion.<sup>20</sup>

On 30 May 2006, the Grand Chamber of the European Court of Justice overturned this agreement for the reason that the European institutions do not possess the legislative power to enter into such an agreement because the transfer of passengers' data concerns public security and activities of the states in areas of criminal law, which are not covered by the Data Protection Directive 95/46/EC (C-317/04; C-318/04; NJW 2006, 2029). The effect of this judgment is to withdraw the designation of US personal data protections as

---

<sup>20</sup> Joint cases 2004/496/EC OJ 2004 L 183, p. 83; OJ 2005 L 255, p. 168, [2006] ECR I- 04721

'adequate,' effective 30 September 2006. An interim agreement, which expires 31 July 2007 (Court of the European Union 2006) provides legal certainty until a new permanent agreement was reached, which reduced the amount of personal data to 19 categories.<sup>21</sup> The absence of such an agreement could have resulted in retaliation by the US government against the European airlines – including blocking of their flights into the US. Without a compromise between the US and the EU individual travelers may have been required to provide their own, individual consent to American scrutiny of data on themselves stored in Europe.

This devolution in the protection of data on airline passengers is simply one example of many losses to privacy following directly from the terrorist attacks of 11 September 2001. Overall, one can observe a devolution from rule of law guaranteeing individual freedoms on the basis of constitutional rights to a legal regime specifying permissible state demands for personal data.

## PROSPECTS FOR THE FUTURE

The erosion of data protection by extensive application of its underlying principles, above all the principle of legality of data processing if based on statutory law in the public sector, may end up in adverse effects to the freedom of persons. But the protection of individuals was the original idea for data protection legislation. The proposal to anonymize person related data or to use more pseudonyms (Roßnagel/Pfitzmann/Garstka 2001) may help to reduce potential misuse, but does not solve the core question, who should be empowered to dispose on personal data at all (Bizer/Luterbeck/Rieß 2002, 151–160).

As regards legislation in the public sector the German Federal Court decisions on data protection should be taken into account, which are generally more reluctant to grant state agencies to collect personal data for the purpose of preventing crime or to reduce all kind of potential harm. In a 'risk society' (Beck 1986) everybody should bear a burden of risk if he/she wants to preserve individual freedoms. Otherwise we may end up in an overprotected society in a state which neglects to grant freedoms.

With regard to the private sector the economic effect of personal data can longer be denied. Expectation of monetary gains leads many to consent to commercial exploitation of their information. The ethical value of human dignity serving as a basis for data protection principles is not denied, but differently weighted. Thus, in modern German society, even the voluntary exposure of sexual behaviour of individuals in TV-reality shows like 'Big

---

<sup>21</sup> Passenger Name Record Agreement (2007 PNR Agreement), OJ 2007 L 204, p. 18 [2007].

Brother' did not, despite some uproar, result in any legal proceedings. The borderline between individual self-determination to expose oneself for commercial reasons and restrictions granted by the German Constitution to preserve the dignity of man was not tested.

The years to come could bring the emergence of a two-sided doctrine of personal data protection. On the one hand, we could see the rise of individual market rights over one's own personal data – where each individual might have the right to keep or disseminate data on one's self in the marketplace. One could then license the use of one's 'own' data – to direct marketers, for example – much as song writers license the right to perform their songs.

The German Federal Court recently confirmed earlier rulings that the right to personality may include elements which are subject to market transactions.<sup>22</sup> Therefore, I expect in the years to come a two-faced data protection development between dignity aspects and the market economy. I would not be surprised if we end up in the private sector with an organizational structure where the right to use commercially valuable data may be licensed to and executed by service providers and performing rights societies on the basis of conditions put forward by the individual. An artist may be proud on getting his individual skills and profile marketed, a manager may restrict the distribution of personal data to career information. 'Managed' data protection by use of digital rights management systems may be the market response to data mining and data warehousing procedures that take place unknown to the subject.

The confidence implied in the German and European data protection legislation that an individual should personally be able to monitor and defend his individual privacy rights is fading. But this does not necessarily imply that the whole concept of data protection is fading. On the contrary: the importance of data protection law is widely accepted and firmly anchored in the post-war German society. The means and methods of protection have to be adjusted to the demands of the modern information society and to ICT (Information and Communications Technology) developments. The impending introduction of ubiquitous computing methods and RFID technology will provide new tests for the adequacy of data protection principles.

Etzioni, a well known author who is pleading for 'communitarianism', finds 'that privacy is privileged over the common good' (1999, 9) and 'undermines' common goods (1999, 199). He wants to balance individual rights and social responsibility (1999, 5, 198), but in fact concludes that all common

---

<sup>22</sup> BGHZ 143, 214 – *Marlene Dietrich*; The German Federal Civil Court ruled similarly to courts in the USA, who created a 'right of publicity' as a property right for controlling the commercialization of personal identity (*Haelan Laboratories, Inc. v Topps Chewing Gum, Inc.*, 202 F.2d 866 (2d Cir. 1953)); see also: Maglio 2003 and Whitman 2004.

goods take precedence over privacy (1999, 203, 215). Buchanan (1989) attacks Etzioni and his objection 'that liberalism devalues, neglects and/or undermines community' (1989, 856) and proves how liberal individual rights protect community (1989, 858 et seq.).

Individual rights are not necessarily individualistic in its negative connotation. Buchanan argues convincingly that 'self' is already embedded and partly constituted by communal commitments and values which are not objects of choice (p. 853).

Thus, the future of data protection laws oscillates between the promotion of state interests to ensure public security, private interests to preserve individual rights, and commercial interests to exploit individual data for reducing transaction costs.

Modern constitutions include a wide range of values – but no hierarchy for those values. Therefore, data protection principles have to meet with approval by each society based on its historical experience, law tradition and future expectations. It is hard to discern any world-wide harmonization of these disparate traditions.

A world-wide harmonization of data protection laws looks rather unlikely at this point. A rather low level of data protection policy concerning the exchange of personal data among companies of the same group having their place of business in states with or without a data protection regime may be advantageous if a private Code of Conduct is introduced and supervised by a group privacy commissioner.<sup>23</sup>

---

<sup>23</sup> See: Daimler-Chrysler AG's Code of Conduct on Data Protection for their world-wide group of companies: [http://www.daimlerchrysler.com/projects/c2c/channel/documents/916654\\_dex\\_corp\\_2002\\_docs\\_cocprivacy\\_e.pdf](http://www.daimlerchrysler.com/projects/c2c/channel/documents/916654_dex_corp_2002_docs_cocprivacy_e.pdf)

## 4. France

### Andre Vitalis

---

The implementation of a system called SAFARI<sup>1</sup> in the early 1970s first brought to light in France the dangers of data processing for individual liberties. Through that system, the *Institut national de la statistique* (INS) intended to turn the social security number – which was being computerised at the time – into an exclusive individual identifier. Adoption of that identifier by the various public administrations, together with data matching between their networks, was to enable the aggregation of all information retained on an individual in areas such as schools, the military, health, taxation and employment.

On 21 March 1974, *Le Monde* sparked things off with an article entitled *SAFARI ou la chasse aux Français*,<sup>2</sup> which pointed to the threat of comprehensive file link-up and data matching. The daily newspaper portrayed an all-powerful *ministère de l'Intérieur*,<sup>3</sup> akin to Big Brother and which, equipped with a giant computer, would be able to watch each individual's every move. The highest officials in the country thus learned first through that article, published in a greatly respected newspaper, about the existence of a system which, under the pretext of a technical modernisation, would drastically transform individual data processing. The secrecy surrounding the operation gave credit to the most alarming hypotheses and fuelled public concern. By dramatising the situation, the press revealed to the public the dangers of file computerisation, a question that had so far been confined to parliamentary circles.

In 1970, during the debates about two bills concerning automated processing, deputies and senators had expressed some reluctance and even flatly rejected the setting-up of a national health database. In November of the same year, however, a bill aiming to create a watchdog committee and a data processing tribunal had raised little interest. Meanwhile, the government had

---

<sup>1</sup> For *Système automatisé pour les fichiers administratifs et le répertoire des individus*, which could be translated as 'Automated System for Administrative Files and Directory of Individuals'. [All footnotes are from the translator.]

<sup>2</sup> 'SAFARI or hunting down the French'.

<sup>3</sup> The *ministère de l'Intérieur*'s responsibilities are analogous to those of the Department of Homeland Security in the United States or the Home Office in the United Kingdom.

commissioned a series of reports from the *Conseil d'État*<sup>4</sup> and a Department of Justice workgroup in order to outline legal measures which could protect a threatened privacy. The proposals stemming from that effort had no impact. Until they could receive a definite assessment of its risks, government officials were reluctant to impede the development of such a promising technology. The automation of administrative files therefore continued in a most disorderly fashion, without any public debate or any safeguard for the individuals affected by data computerisation.

That was the situation which the SAFARI scandal brought to an end (Vitalis 1980). By focusing previously vague fears on the specific threat of comprehensive link-up and matching, this affair forced the government to accept public scrutiny and to act. Eight days after the publication of the article in *Le Monde*, on 29 March 1974, the Prime Minister issued a circular banning any link-up between computer systems belonging to different departments. The SAFARI acronym was dropped and the *Institut national de la statistique* changed the name of the database it had set up for the more neutral *répertoire national d'identification des personnes physiques*.<sup>5</sup> Above all, on 9 November 1974, the President of the Republic appointed a commission of inquiry on 'Computerisation and liberties', which operated transparently and whose conclusions were made public in September 1975. The fundamental text in the French data protection regime, the legislation of 6 January 1978, would only be adopted three years later.

This law on 'computerisation, files and liberties', revised in 2004 in order to comply with the EU Directive of 24 October 1995 regarding personal data protection, stipulates in its first article: 'Computerisation must serve each citizen. Its development must be undertaken within the framework of international cooperation. It must not be prejudicial either to human identity, human rights, privacy, or individual or public liberties.'

The legislation as enacted presents the two main features which nowadays characterise the European approach. First, it has a general scope, covering all types of personal data processing. Second, it completes individual means of defence with the setting-up of collective control mechanisms entrusted to a specialised public body. Data processing is subject to a number of rules, which persons or groups in charge of files must comply with: preliminary formalities to be carried out at the time of setting up automated processing, determination

---

<sup>4</sup> The *Conseil d'État* has no equivalent in the United States or British constitutional and legal systems. It acts *inter alia* as a controller of the legality of all bills and other legal instruments to be considered by government, it is the court of last resort regarding administrative law issues and it can be consulted by government on any legal or administrative issue.

<sup>5</sup> Or 'National physical person identification catalogue'.

of and compliance with the purpose of the processing, fairness in the collection of such data as is relevant, limitation of the period during which data may be stored, ban on the collection and conservation of sensitive data (racial origins, political, religious or philosophical opinions, trade union membership, data pertaining to health or to sexuality), limited disclosure of stored data, security measures. New rights are granted to data subjects: right to preliminary information regarding data processing pertaining to them, rights of access, right of opposition, right to rectification, right to oblivion. An independent public body, the *Commission nationale de l'informatique et des libertés*<sup>6</sup> (CNIL), is assigned the task of ensuring the implementation of the legislation, by informing the various stakeholders of their rights and duties and controlling computer-related applications.

The effectiveness of this protective mechanism rests upon data controller compliance with the enacted rules regarding the creation and operation of data processes, and upon the exercise by data subjects of their new rights concerning the use of their data. In actual fact, one finds that compliance is far from being widespread and a huge gap exists between what ought to be and what really is. The 1978 legislation has too often remained a 'paper tiger'. As a Minister of Justice declared in 1999: 'We have extremely strict rules on paper, but we are sometimes lax in reality'. In a substantial number of cases and especially in the private sector, data controllers failed to disclose the setting-up of automated processes to CNIL. Whereas this body has recorded around the setting-up of one million data processes to this day, it is estimated that this amount represents a mere 20 per cent of existing processes.

The simplification or outright elimination of preliminary formalities, which came about with the 2004 alteration to the legislation, appears to have acknowledged both this situation and the formidable increase in computerised applications.

Citizens themselves do not seem to have shown a great deal of interest in exercising any control over the data processing that concerns them. The new rights which they were granted remain unused for the most part. For instance, the right of access, which was of prime importance to the lawmakers, is exercised by a mere few hundred persons per year. As for litigation generated by the legislation, it has remained scarce. Judicial action, while seldom called for, was usually disappointing, especially during the first years after the legislation came in force. Judges have often seemed to forgive violations of the law and clearly failed to understand the seriousness of the matters brought to their attention. This explains the difficulties met by the CNIL when turning to prosecution. In 1998, after 20 years of the legislation being in place, out of 14

---

<sup>6</sup> Or 'National commission on computerisation and liberties'.

referrals to the courts, seven have been closed without conclusion, four are still pending and three have led to light convictions. A slight increase of contentious affairs has since been observed.

Despite providing important symbolic gains, this regulatory framework has not significantly weighed upon the course of events, and especially on the balance of powers between data subjects and controllers. CNIL has of course provided a regulating function, thus preventing the most dangerous drifts against individual liberties, but it has been unable to question and limit the ongoing development of personal data collection, conservation and processing, even though such development embodies a threat to the safeguarding of privacy and democracy. The legislator had aimed at protecting individual liberties without hindering the development of information technologies which were viewed as a token of economic and social progress. Here as elsewhere, this dual aim – which one may well think unreachable – jeopardises the effectiveness of the regime put in place.

## THE HISTORY OF KEY DEVELOPMENTS FOR DATA PROTECTION IN FRANCE

### **Awareness of the Dangers of Computerisation and the Setting-up of a Legal Framework for Processing**

It was during a debate concerning two bills, in 1970, that parliamentarians first showed some reluctance regarding the use of computerisation by public administration. They requested that the confidentiality of data held in a database centralising driver information be guaranteed. They flatly refused the setting up of a national health database, which they considered an infringement on people's most intimate privacy. Even then, it was generally considered, in political and media circles as well as among major computer producers, that database computerisation ought not to be undertaken in a disorderly fashion. The public might otherwise develop fears which, in turn, could penalise the expansion of computer technology. These stakeholders were therefore well disposed towards regulation in order to avoid any excesses which might affect the development of computerisation.

One had to wait for the controversy sparked off by the implementation of the SAFARI system in 1974 before the government actually took the 'Computerisation and liberties' problem seriously, banning data matching throughout the public administration and appointing a commission of inquiry from which it expected proposals for solutions. This commission worked transparently, consulting employers' organisations, trade unions, public associations and experts. It requested a study from the *Conseil d'État* on the extent

of administrative file computerisation, which clearly indicated the level of modernisation that had been reached. On the whole, in its report published in September 1975, the Commission seemed pessimistic (Commission Nationale de l'informatique et Libertés 1975). It expressed the view that 'the major threats seem to be an increase of social control and a worsening of already unequal relationships within society'. In order to defend against intrusions into privacy, and after having considered the few experiments being carried out abroad at the time, it advocated protective legal measures but also suggested other measures, such as worker participation in key computerisation decisions or the introduction of courses on the social impact of computerisation, in programmes where this technology was taught.

The adoption, by Parliament, on 6 January 1978, of one of the first data protection laws in Europe, after Sweden and the Land of Hesse, ushered in a new period. From then on, personally-identifiable information processing would be subject to certain amount legal rules, data subjects given new rights and a specialised regulatory body set up under the name of *Commission nationale de l'informatique et des libertés* (Frayssinet 1992). The text as enacted benefited from the considerations of international organisations, such as the Council of Europe and the OECD, and from Swedish experience in this area. A common approach to the dangers of computerisation characterised these considerations and safeguarding measures. Starting with the notion of an isolated individual whose right to privacy is recognised, the legislative aim was to regulate computerised processing in order to avoid intolerable infringements of this right. The second and main inspiration of the French legislation was the report provided by the 'Computerisation and liberties' research commission, published in September 1975. Based on the proposals made in this high quality report, the Senate modified the government's bill regarding two essential issues. Whereas the government wished to choose directly the members of the specialised controlling body to be established, the senators imposed nomination and election procedures that guaranteed their independence. Moreover, they extended legislative coverage to all files.

The 1978 Act can be viewed as cornerstone legislation insofar as the protective framework it set up is still considered relevant more than 30 years later. Its broad principles, its main rules, the specialised body in charge of enforcing them, all still seem valid and well-adapted to the present situation. Yet, because it was not perfect and because necessary European harmonisation required that it be revised, successive alterations have since been made. The 1981 Convention of the Council of Europe on the protection of personal data, closely related to the French legislation in its provisions, provided the opportunity for the addition to the category of 'sensitive data' of information concerning sexuality and health, which the French legislator had omitted. An Act of 16 December 1992 was supposed to include issues involving sexual

behaviour to that list. With regard to health, a new chapter was added in 1994 to the legislation, introducing a specific regime for automated processing in the area of medical research. CNIL no longer provides recommendations regarding such processing but, after considering advice from a consultative committee to the minister responsible for research, decides whether or not to grant an authorisation.

These new provisions offered a solution to difficulties which came to light in 1985 in relation to a cancer database, and concerning information and opposition rights of patients: insofar as their code of ethics authorises doctors to withhold information from patients about their condition, it was therefore impossible for patients to oppose the use of their medical data. This specific regime reaffirmed the patients' right to oppose the use of their nominative data for research purposes in the field of healthcare. If a doctor considers that a patient should be kept in ignorance of a severe diagnosis or prognosis, it is now established that this data may not be used. Another addition was provided by 1999 legislation, concerning data processing set up for evaluative purposes.

The most significant modification made to the 1978 legislation was provided by the transposition of the European Directive of 24 October 1995, regarding the protection of personal data. Harmonisation was necessary in order to ensure free circulation of personal data, considered as a commodity, and to avoid regulatory disparities which could entice operators to relocate processing to the more lax member states. The circulation of information must not endanger individual liberties in a Union where the protection of personal data is established in the Charter of Fundamental Rights. Indeed, Article 8 of this charter stipulates: 'Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.' Data transfers and assignments outside the Union can only take place if the recipient countries and undertakings offer an adequate level of protection.

It is paradoxical that although France was the main instigator of the 1995 European Directive, it was in fact the last member state to transpose it, through the legislation of 6 August 2004. In this new text one can easily recognise the general protection layout, with the rights of data subjects, duties of data controllers and the intervention of CNIL (CNIL/Paris 2 University 2005; Girot 2005). Two main modifications were introduced in order to comply with the Directive. The first concerns preliminary formalities, a simple declaration becoming the normal regime regarding data processing in either the private or public sector. *A priori* control is limited to processing that presents a specific

risk, with a consultative regime for public processing regarding security or using social security numbers, and an authorisation regime for ten processing categories which present risks due to the sensitive nature of the data, the purposes of their use or particular characteristics. The second modification is related to the reinforcement of on-site controls and sanctions, granting new powers to CNIL, which can impose administrative (including financial) penalties.

The new text was not unanimously welcomed. A few days after the vote, the socialist Senate group referred to the *Conseil constitutionnel*,<sup>7</sup> considering that the new provisions constituted a regression and gravely threatened several fundamental rights. The *Conseil constitutionnel* decided otherwise, merely striking out the right for business undertakings which considered themselves victims of fraud to constitute offence registries (or 'blacklists'), although allowing organisations in charge of intellectual property rights to do so.

### **The Essential Role Played by CNIL in the Application of the Law and its Interpretation**

Described by the legislation as an 'independent administrative authority', CNIL is the keystone of the protective framework. It is responsible for ensuring compliance with the legislation and recommending modifications where required. Its role has been all the more crucial since compliance control by the data subjects themselves has not been as effective as expected (Braibant 1998). Thanks to data controllers complying with the notification requirements associated with the setting-up of data processing, CNIL has been able to monitor on an ongoing basis the computerisation of files and data collection and processing systems. Without its opinions and recommendations, its simplified norms and counselling, this computerisation would most certainly have been less respectful of individual privacy. A significant task has been carried out: almost one million registered processes, 2000 to 3000 complaints examined on average each year, approximately 1000 replies to official advice requests, over 5000 replies to requests for indirect access, not to mention the hundreds of deliberations, for which annual activity reports provide an account.

The Commission has opted for a more educational than repressive role, which explains why, in 25 years of activity, one counts a mere 45 warnings, 30-odd referrals to the public prosecutor and, yearly, a dozen inspections or so. It is through compromise and negotiation that CNIL has exercised the greatest

---

<sup>7</sup> The *Conseil constitutionnel*, or 'Constitutional Council' is, *inter alia*, responsible for determining the constitutionality of French legislation.

influence and obtained the best results. It has tabled few unfavourable decisions as, before being called upon to decide an issue, it has been able to obtain through prior negotiations the removal or alteration of the more questionable aspects of data processing proposals. Favourable decisions are often accompanied by numerous reservations. In a vast majority of cases, a compromise between opposing interests has been sought after: for example, the needs of research and the respect of medical secrecy, the necessary control of welfare benefits and the respect of individual privacy, the interests of direct marketing and each person's right to not be troubled. The limited powers of the Commission with regard to the private sector, subject to a mere declaration, has not allowed it to set up the greater controls it had hoped for. The *Conseil d'État* considered it necessary to remind the Commission, in a decree of 6 January 1997, that it was not authorised to prevent the setting-up of private data processing, even if it violated legal provisions.

In 1998, for its twentieth anniversary, CNIL published the 20 deliberations it considered to be the most representative of its activity (CNIL 1998). Through these, CNIL has limited police surveillance by preventing the creation of a database which could have led to a generalised control of the population when the computerised ID card was introduced. With other European commissions, it successfully asked that the rights of each individual on file remain protected in the Schengen police information system. A warning was issued to the mayor of a municipality that was using data protected by statistic secrecy measures in order to monitor persons of foreign origin. The regulatory body showed the greatest firmness so as to prohibit discriminatory processes. Through a warning to a hotel owners' professional organisation, it hunted down the creation of broadly distributed blacklists, which identify people as 'undesirable'.

When a bill dealing with overindebtedness was debated, CNIL recommended that only the *Banque de France* should be allowed to set up a national database covering credit delinquencies. In the related field of insurance, it obtained the elimination of a database listing people with 'increased risks' that all insurance professionals could use, and which identified clients who had suffered an insurance refusal or the imposition of a supplementary premium because of their health condition. CNIL has also striven to limit or to exercise some oversight over the use of profiling techniques. It issued an unfavourable opinion regarding the Ministry of Health GAMIN system, which pre-selected so-called 'risk-prone' children through automated means. It supervised the use by banks of behavioural segmentation techniques, enforcing the customers' right to know which segment they are put in. CNIL also acted to impose business compliance with declared processing purposes, in order to ensure that adequate safeguards are provided with regard to personal data transfers to other countries or to defend consumer rights.

## **Adapting to Continuous Technical Innovation and Searching for New Forms of Regulation**

Over the last few decades, we have been faced with a constant development of information technologies dedicated to controlling populations. At the beginning of the 1980s, microcomputers started to supplement mainframes, to be followed in turn some years later by image and sound sensors and observation satellites (Cadoux 1996). The greatest innovation, emerging from the early 1980s, resulted from the multiplication of electronic information supports (bank cards, mobile phones, data communication systems), used for various purposes, which paved the way for a universe of traceability now perfected by the internet (CREIS 1991). Aside from any consent to collection and without concerned persons even being aware of it, these supports automatically produce an enormous mass of data which has been calculated to double every 18 months! The recent legislative amendments, transposing the 1995 European Directive, should make it possible to better face the threats coming with the current context, through the alleviation of preliminary formalities and the establishment of identical procedures for both private and public sectors.

One could worry that a regulatory framework designed in an era of 'heavy', centralised computer technology would quickly become obsolete in a field where technical progress and innovation have been unceasing. Thanks both to the generic scope of the legislation's notions and principles and to CNIL's efforts regarding its interpretation, the original level of protection has been gradually adapted to new technologies (Maisl and Vitalis 1993). The notion of nominative information has been given a broad construction. Any information which in any way, directly or not, allows for the identification of a person is included within that notion. Therefore, private branch exchanges (PBX) or switches used by businesses and public administrations to manage communications have been deemed subject to regulation insofar as they process indirectly nominative information.

By the same token, the notion of automated processing is not linked to a given technological state, but is applied extensively. It applies to files, databases and meta-databases, or even image sensors. A motorway company was refused authorisation to set up this type of image sensor, capable of identifying a car's license number, in the name of the liberty of movement. New telecommunications services also had to comply with the new norms. Distant identification of minitel users without their knowledge, which could have led to the creation of consumer profiles, was made technically impossible.<sup>8</sup> A

---

<sup>8</sup> Minitel is a videotex service available through telephone lines which was launched in 1982 by the French public telecom operator and was extremely popular; although largely upstaged by the internet, it still serves millions of subscribers.

medical analysis transmission system through minitel was not authorised, as it did not offer all the necessary security safeguards. The respect of anonymity was enforced for cable TV networks, just as the regulatory body made sure subscriber identification did not constitute a requirement to setting up a communication on integrated services digital networks.

Memory cards were subject to many experiments in the field of healthcare, and were subjected to a number of conditions: prior information to users regarding their rights, free consent to participate, sufficient security measures, and requirement of a proper authorisation to access the contents of the card.

With the construction of the so-called information society and the development of a worldwide network like the internet, adaptation has become increasingly difficult. The possibility that the network offers for instant data transfer from one place to another, all across the planet, limits the effectiveness of local protection measures. The disparities between regulatory frameworks can only entice operators to relocate their data processing operations in countries where requirements are weakest. Faced with an unsatisfactory situation where, for commercial reasons, internet users are closely tracked and subject to numerous solicitations, CNIL has stepped in and asked professional operators to be more respectful of internet users' rights. It has hunted down spammers and, in November 2002, referred to the public prosecutor cases against five of them. That same year, the European Union passed a directive on privacy and electronic communications, in order to protect internet users from devices allowing for personal data collection and conservation and to require prior user consent for all commercial communications initiated by an enterprise.

Because of the insufficiencies of the existing legal framework, other forms of regulation have been considered. In the year 2000, a French parliamentary report suggested 'co-regulation' as a means to address problems brought about by a worldwide network. Beside legislative efforts, the idea was to promote the adoption of codes of practice or codes of ethics by business and to set up quality labelling procedures. Such regulatory and self-regulatory efforts cannot be sufficient however and the vigilance of internet users themselves was also called for, as they were invited to enforce their own rights. Following this report, an association called the *Forum des droits sur l'internet*<sup>9</sup> was set up in 2001, offering an environment for debate and proposals from all internet stakeholders. Publicly financed and composed of a college of professional agents and a college of users, the Forum holds no compulsory power. By easing the dialogue between public agents, private enterprise and members of civil society, it aims to contribute to developing civility on the internet and especially at making recommendations regarding privacy on the network.

---

<sup>9</sup> The 'Rights on the internet forum'.

## PUBLIC OPINION

### The Lack of Public Mobilisation

Only a minority – a little less than a third of the population – actually perceives the threat that the expansion of information technology may pose for individual liberties, and that proportion rather tends to decline. In an opinion poll carried out in May 1999 on a representative sample of the French population (*L'événement* magazine, No 761, June 1999), 32 per cent of persons interviewed considered that the development of computer technology aimed at collecting nominative data constitutes a danger for liberties; conversely, 60 per cent considered this development, which reinforces the security of citizens, to be rather positive. Over 20 years earlier, in an opinion poll carried out in 1976 in similar conditions (*Statistique et développement* review, No 24, March 1977), 38 per cent of respondents considered that file computerisation was a threat for privacy and democracy, whereas 51 per cent declared themselves in favour of operations offering more efficiency and greater knowledge about the population.

The population groups most sensitive to the threat in the latter investigation were persons under the age of 25 or over 50, the categories with the highest level of education and those rather 'to the left'. The 'computerisation and liberties' theme is too abstract a notion to attract widespread public attention. Public opinion seemingly only becomes aware of dangers on an *ad hoc* basis, when the press reveals particularly liberty-threatening data processing operations. Individuals perceive the drawbacks of data processing insofar as these procedures touch them as workers, consumers, patients, welfare receivers or tax-payers. In this respect, the thousands of complaints lodged to CNIL represent a precious testimony of the difficulties which arise from data processing and the sometimes very adverse consequences it can have in a wide range of areas. These complaints testify to the reality of the problems and the relevance of an issue sometimes presented in too generic terms.

Data subjects are not very concerned with exercising any control over the operations affecting them. The new rights which they were granted have for the most part remained unused. For instance, the right of access, which was of prime importance to the lawmakers, is used by a mere few hundred persons a year. The lack of attractiveness of these new legal possibilities, the weight of habits and a certain form of fatalism can explain such passivity.

Other explanations must also be considered, such as the lack of information and the failure to understand what is at stake. The mainstream social discourse does little to improve the situation, as it would rather emphasise the benefits of new information technology than point to its drawbacks. In June 2004, a study conducted by SOFRES, with a representative sample of the French

population (25th CNIL activity report), showed that a third of French citizens only had a vague idea of what CNIL represents, and no more than a fifth of the population was aware of their rights concerning personal data collection and use. In the end, the new rights mostly allow, at any time, the pondering of the gap between an ideal, in which individuals would exercise control over their data, and a reality in which they are far too often treated, unknowingly, as mere informational objects.

### **Press Revelations and Militant Actions Against Processing**

Some incidents raised a true media feeding frenzy, finding such sympathy in the opinion that government was compelled to react urgently in order to calm the waters. Databases used by police and the *Ministère de l'Intérieur* were the principal targets of such campaigns. In June 1981, following an intervention by the Human Rights League, media headlines revealed the existence of illegal files held by the French *Gendarmerie* brigades. Contrary to the provisions of the 1980 statute on criminal records, these brigades were keeping files listing convictions in both the convict's place of residence and his place of birth. The news raised a ruckus. There was a commotion both in the public opinion and the judiciary. The affair soon took a turn for the worse, provoking widespread public outrage and legal confusion. A motion was presented to the court; CNIL intervened, and so did the Minister of Defence. The *Conseil d'État* finally had the last word, ruling that the *Gendarmerie* was in fact entitled to keep such files.

Greater still was the agitation when, in February–March 1990, two decrees were published on the processing of sensitive data by the French *Renseignements Généraux* national security services. The controversy took such a turn that the Prime Minister was forced to withdraw the texts, which he had himself signed only days before. Incidentally, that particular controversy clearly demonstrated a deep lack of understanding of the 1978 legislation by the public and its standard-bearers, since the decrees aimed to legalise police conservation of sensitive data following a special procedure before CNIL, with the processing purposes having been clearly established and the most questionable aspects of the proposal having been set aside beforehand. Various projects concerning ID card computerisation regularly caused public outcry. A 1980 project was withdrawn in 1981, after the left came to government and judged it contrary to civil liberties. Another project, in 1986, met with heavy criticism on the same basis and was significantly amended by CNIL. Another debate is currently being given press coverage, following announcements of the introduction of an ID card containing biometric elements. The media also relate on a regular basis the most spectacular and scandalous data processing scandals: employee files including

data concerning their sexual behaviour, worker surveillance, remote identification of minitel users or presence of spyware on computers, non-compliance with stated purposes for data processing, creation of population databases by local authorities and worldwide surveillance systems such as Echelon.

Political parties, trade unions and consumer associations show very little interest in the threat that the ongoing development of information technology may pose to civil liberties. Frontal objections to computerised systems are mainly raised by social and medico-social professionals or highly mobilised pressure groups, preoccupied with the decline of liberties. Public administrations have sought to modernise and rationalise methods and procedures via the computerisation of the social and medico-social sectors. This computerisation has met with considerable opposition from workers in these areas, who are asked to manage systems which have been designed without their participation. The most significant example of this resistance occurred in the mid 1970s with the setting up of a system named GAMIN<sup>10</sup> by maternal and infant protection services, which set off widespread militant opposition lasting several years (Vitalis 1981). This system proposed medical and social monitoring of all young children, through the early detection of so-called 'risk-prone' children, with their detection automatically carried out by machines, using medical as well as social criteria! Directly responsible for applying the new rules, doctors, social workers and child nurses considered that the GAMIN system had a negative impact on their work conditions, while it failed to serve public interest. Doctors' unions questioned its usefulness for children's healthcare and considered it brought no improvement. Going even further, the national association of social workers denounced it as an attempt to introduce a police-like outlook in their professional activity. Beyond articulating a corporatist critique centred on their work conditions, these professionals considered GAMIN to be harmful to the concerned populations and to be prejudicial to their freedom insofar as it was a means to discriminate, label and classify individuals from their earliest years onward. Groups appeared all over the country, demanding with increasing determination that the system be shut down. They petitioned the *Conseil d'État* to that effect at the end of the 1970s, without result. It was only in June 1981 that the system was condemned by an unfavourable opinion of a recently implemented CNIL, making that decision one of its first.

---

<sup>10</sup> *Gestion automatisée de médecine infantile*, or 'automated management of infantile medicine'. The program's name was a pun on 'gamin', roughly meaning a 'playful kid'.

Over 20 years later, in the same sector, the same professional categories were to engage in a new wide-scale militant struggle, questioning the ANIS<sup>11</sup> software, which several *départements*<sup>12</sup> had chosen to use. Also set up for greater rationalisation and to improve management, this software enables the establishment of a database on the people being assisted, which could be shared by all concerned professionals through a network of remote computers. All information concerning a family was therefore linked up in a single file! As soon as this new approach was implemented, a pressure group created in 1997 and called *Pour les droits des citoyens face à l'informatisation de l'action sociale*<sup>13</sup> clearly stated its opposition. Composed of about 20 professional organisations and trade unions, it demanded the removal of ANIS and similar software, for reasons linked to professional practice conditions (reinforcement of hierarchical controls, loss of professional secrecy, more bureaucratic approaches with standardised and predefined replies), as well as because of the dangers the system posed for assisted groups of population. These groups would indeed have become 'over-filed' through a 'social record', containing most sensitive data on psychological conditions and social integration challenges. Faced with opponents that would not let go, and although it had first authorised the program in 1997, CNIL had to revise its decision. At the end of 1998, it asked the regional authorities concerned to redefine the data categories being used and to use anonymisation processes, while making sure the database could not be accessed without proper control procedures.

As early as 1979, faced with the social dangers of computerisation, several associations, representing various militant positions, had organised a one-day seminar under a quite telling title: 'Society against computerisation?' That led in turn to the launch of a periodical called 'Terminal' – another rather telling title – in order to present arguments supporting opposition to a process that was affecting the whole of society and define a common oppositional line. In the following years, after this opposition to the computerisation of society had ebbed somewhat, other *ad hoc* militant actions appeared occasionally. In 1995, small and rather heterogeneous groups criticised the installation of CCTV cameras in city centres, devices which they accused of going against the individual's freedom to come and go in public spaces without being observed. In October 1997, a number of internet users set up an association called IRIS<sup>14</sup>

---

<sup>11</sup> *Approche nouvelle de l'information sociale*, or 'New approach to social information'. The name is a pun on the French name for anise or aniseed.

<sup>12</sup> In France, *départements* are regional administrations answering to the central government.

<sup>13</sup> Or 'For citizens' rights, facing the computerisation of social action'.

<sup>14</sup> *Imaginons un réseau internet solidaire*, or roughly 'Imagine a solidarity-enabling internet network'.

in order to promote non-commercial zones on the net and the respect of privacy. It was this association that alerted public opinion, after the adoption of an act on interior security in November 2001, about the obligation that internet service providers now have to keep trace of all traffic data for a period lasting for up to one year.

By their very nature, freedom defence organisations such as the Human Rights League or anarchist-inclined associations remain permanently on guard, ready to intervene at specific moments, according to the threat perceived. In this respect 1997 was an extremely critical year: the government intended to take advantage of the 1995 European Directive transposition into internal law in order to lower protection levels in the *informatique et libertés* legislation; at the same time, a bill was being prepared that would authorise data matching between fiscal and social service files. One could literally feel oneself swept back 20 years into the past! In this context of urgency and in order to face a very worrying situation, a pressure group called *Informatique, fichier and citoyenneté*<sup>15</sup> was set up by computer specialists, teachers and legal professionals. As events had it, a change of political majority quieted the concerns, although the issue of data matching remains on the agenda.

### **An Evolving Context and Changes in Public Perceptions**

Towards the end of the 1970s, opposition to the GAMIN system within the sensitive field of social assistance benefited from the support of a large trade union like the CFDT and was favourably considered by the general public. Twenty years later, in the same field, a similar type of opposition movement – this time regarding the ANIS software – gathered little response among the public and could only count on weakened unions. In between time, it is clear that the general context and public perceptions have changed. Two very different periods must be distinguished in this regard (Armatte 2001; Terminal 2002; CREIS 2004).

The 1970s and 80s were the heyday of a critique of a computerisation process serving the ruling interests. The only machines available at the time were large computers, used by specialists, and were exclusive to large organisations that could afford them. In an era of heated political combat, unions and opposition parties mainly criticised the use of computers which prioritised capitalist interests and in their view failed to take into account popular needs. From a liberal or libertarian viewpoint, transcending the classic left/right opposition, the increase in power for the state and its administrations resulting from computerisation was also being criticised. All in all, an Orwellian vision

---

<sup>15</sup> Or 'Computerisation, files and citizenship'.

prevailed and portrayed a computerised state which henceforth would hold in its hands the means to generalised population control. It is in that context that the legislation on computerisation and liberties was adopted in 1978.

A second period was to begin with the development of the use of micro-computers among the greater public and the expansion of network communication. It became apparent that information technology could serve all sorts of interests, and not only those of large organisations. Towards the end of the 1990s one began to observe the emergence of a true technophilia, which sees information networks and technologies, especially the internet, as a means of regaining strong economical growth and establishing a new basis for social progress.

The promotion of a so-called 'information society' systemised this favourable preconception by turning the growth of informational technology and networks into an articulated vision for the future of society. At the same time, economic globalisation and its underlying neo-liberal ideology continued to undermine and weaken the state's legitimacy and powers. This weakened state appears less frightening. The threats are increasingly amorphous and difficult to identify in an environment saturated with control technologies. With the economic hold ever more important, collection and use of consumer data become the new focus of critical attention (GRID et al. 1986). In order to be able to offer goods and services that are adapted to the needs of the individual, companies must establish in great detail his or her identity, behaviour, tastes and preferences. The results are the setting up of consumer mega-databases, minute internet-user monitoring and the development of a nominative data market. Indeed, such data has now become of prime strategic importance for commerce. It is no longer Big Brother which is the threat, but a multitude of Little Sisters, who wish only for the individual's own good and are constantly contacting them on the basis of their in-depth knowledge of individual personality and preferences. These changes in the very nature of the threats have put opposition groups in a difficult position. Moreover, the highly technical nature of questions also limits the amount of people who are actually able to participate in debates, as the low participation in discussions concerning the adaptation of the protection regime or regulatory measures to be introduced on the internet in order to safeguard privacy has shown.

## NATIONAL CULTURE AND TRADITIONS

### **A Single Personal Identifying Code at the Centre of Debates and Legislation on Data Protection**

A single personal identifier makes data matching a lot easier. Some countries have adopted this type of identification; others have not, even going as far

as to make such an identifier unconstitutional. The French situation is intermediate: although a single identifying number has been set up, the NIR,<sup>16</sup> more often called the 'social security number', its use is strictly controlled. The use of this number has always figured at the heart of the computerisation and liberties debate and, in the early 1970s, the concerns raised by NIR computerisation sparked the adoption of measures aiming at protecting privacy.

The reason why this identifying code has proven to be such a sensitive issue in France is that, unlike in other countries, the number is not randomly generated but rather provides information on the bearer's sex, age or place of birth, all of which takes one back to a dark period of French history: the pro-Nazi Vichy regime, which first set up the personal identifying code in 1941 (Hoffsaes and Vitalis 1995). Fortunately, this identifying code, established by the demographic services of occupied France, was not used by the occupying forces and therefore did not have the dramatic consequences it could have had, although some doubts still remain to this day in that regard. Officially, in 1941, this number was supposed to help in reconstituting administrative files that had been damaged in the course of the war and to collect statistics on the population's condition and labour potential. The true aim of the registration process was in fact of a military nature: statistical pretexts served to camouflage (from the German invader) the reconstitution of a military census, which might one day be used in order to mobilise a new French army. A far less honourable aspect of this registration system was that it also constituted the basis of a deliberately racist profiling of the population. The first number of the code associated the person's sex with data regarding one's religion, nationality or geographical origin. The ten values of this first number could be read as follows: 1 or 2 for French citizens, 3 or 4 for natives of colonies (with the exception of Jews), 5 or 6 for indigenous Jews, 7 or 8 for foreigners, 9 or 0 for ill-defined statuses.

Cleared of all reference to race or religion, the code was subsequently used by the welfare state. First adopted by social security administrations in order to manage namesakes, it gradually became commonplace before turning into an essential management tool. At the beginning of the 1970s, however, its computerisation suddenly alerted people to the dangers of digital identification. Insofar as there were other methods allowing data matching, the digital identifier was kept, but its use was strictly monitored under the 1978 legislation: a provision clearly stipulated that the use of the NIR required a *décret en*

---

<sup>16</sup> The *numéro d'inscription au répertoire national d'identification des personnes physiques*, or 'National Physical Persons Registry Inscription Number'.

*Conseil d'État*<sup>17</sup> adopted on the basis of a CNIL recommendation. Over the years, CNIL's commitment to limit the use of that identifier has as often as not been less than well-appreciated and governments and parliaments more than once tried to shove it aside. Changes to the legislation in 2004 finally restrained CNIL's powers in that area.

### **The Exercise of an Independent Regulatory Power within the French Administrative System**

A new institution for a new era, CNIL, with both regulatory powers and a good-sized staff, was the first ever independent administrative body to be set up in France. Its creation entailed a significant institutional innovation that was a direct blow to the French politico-legal tradition, used to a tripartite distribution of powers between the executive, legislative and judiciary. The main characteristic of the new institution is its independence, guaranteed by the way its 17 members are chosen. This independence and its being apart from the three traditional powers appear to create a specialised fourth power, which is difficult to accept and to apprehend within the national administrative system (Vitalis 1993).

CNIL has been put in the dock over two concerns: some doubt the reality of its independence and its actual capacity to weigh in on decisions; others question the legitimacy of its powers. According to the first group of detractors, the Commission lacks the means required for an effective intervention. It provides a justification for data processes, without being able to really safeguard the rights of data subjects. We would therefore be faced with a manipulation and camouflage operation providing significant symbolic benefits, but without any real influence on the course of events. Rather than actually being a counterweight, the Commission is therefore seen as acting as a power relay in a sensitive area that necessitates new modes of intervention. It would be incapable of opposing the prevailing logic; it could merely propose the odd adjustment in order to make this logic seem less repulsive and more acceptable for the public. Its intervention would therefore be negative on the whole: it prevents direct action by data subjects, feeding a false illusion of safety and keeping them from becoming aware of the situation and taking appropriate action.

The second form of criticism does not focus on the effectiveness of the regulatory body, but on its legitimacy to act in the stead of more legitimate

---

<sup>17</sup> The notion of *décret en Conseil d'État* refers to a decree (or statutory instrument, or executive order) taken by government following a special procedure, slightly different from the usual one. It has no obvious equivalent in British or American administrative law.

authorities. That the existence of a counterweight might discount the unitarian logic of the state apparatus inspires concern in a country where regalian interests are often considered as overcoming all others. French political thinking holds a view of democracy which emphasises popular sovereignty and public will. It is difficult to apprehend an independent administrative authority within a tradition which considers universal suffrage elections and allegiance to a traditional form of state to be the only foundations of legitimacy. It is no surprise therefore that concern would be expressed regarding possible plutocratic drifts or even the eventuality of a 'wise-men's government'. This new institution is thus seen as lacking the legitimacy of a parliament democratically elected through universal vote and of a government that proceeds therefrom. Nor does it have the legitimacy of a judge whose independence is traditionally recognised and constitutionally approved. Neither does it have the legitimacy of traditional administrative bodies, which develop impersonal rules and are subject to political power. Any true independence accorded to such a body can only be at the expense of stripping it of all power and leaving it only with some capacity for persuasion.

These two forms of criticism, while utterly irreconcilable, have not necessarily been unfounded. CNIL has sometimes shown itself too lenient with data controllers, issuing favourable opinions regarding processes which, in the social sector for instance, then met with strong opposition. On the other hand, its intransigent attitude and will to extend its prerogatives have led to conflicts with established powers and organisations, which then questioned the grounds of its intervention. Nevertheless, on the whole, these two pitfalls have been avoided. Over the years, CNIL has become a respected institution whose status and means have been consolidated with the 2004 legislative amendments. Slowly but surely, it has been able to find its own place and gain acceptance from other powers by turning to approaches which are more educational than repressive. Aware of its limited means, the Commission has favoured compromise instead of frontal opposition. Adopting a unanimous position on an issue has also proven to be another way of consolidating its position. Consensus is all the more effective in that it expresses the common position of the 17 members, forming a sort of 'Academy of liberties'.

Although CNIL has elaborated flexible and original methods of intervention, it partakes in a classical administrative culture which has harmed its effectiveness (Flaherty 1989). Regarding logistic, financial and staffing problems, the strings were never cut with a state that did not always grant the Commission the resources it needed. The Commission's composition leaves too much space for that classical administrative culture. Among its 17 members, who are politicians, high-ranking magistrates and qualified public

figures, none are representatives of pressure groups and associations or of information technology professionals. This administrative culture shared by the majority of its members certainly accounts for deficiencies in terms of public information, as well as for a lack of implication in debates and controversies surrounding ongoing and significant computerisation projects. The institution's excessive centralisation also reflects a long Jacobine tradition. CNIL is exclusively based in Paris and does not have any regional offices outside the capital.

### **The Influence of Foreign Legal Cultures**

During the preliminary discussions prior to the adoption of the 1995 European Directive on data protection, various legal traditions (Latin, Anglo-Saxon, Germanic . . .) were compelled to come together so as to lead to a common draft. While many principles and procedures used in the French legislation found their way into the European text, the latter also includes other contributions. It is therefore unsurprising that such contributions then found their way into the French legislation as modified in 2004 to take the Directive into account. For instance, these amendments introduced a German institution which was totally unheard of in French law beforehand: the data protection correspondent. Established in 1977 in Germany, this correspondent, although chosen by the data controller, is responsible for enforcing with complete independence the controller's internal rules, for keeping a data processing registry and for making sure therefore that processings do not breach the rights and liberties of data subjects.

This institution, which clearly bears the mark of an auto-regulatory approach, is closely related to the German co-management culture. Insofar as it reduces preliminary formalities, this measure can help deal with the proliferation of files and computerised systems in organisations. Adapting such an institution in France will take time however, particularly since the idea of a correspondent is far from being unanimously accepted. A number of experts consider that adopting such an approach lowers the level of protection since they fear the correspondent's independence is not properly guaranteed. Whether a company employee or a freelance agent, this person is paid by the data controller and the question arises whether, in the absence of a professional order or a code of ethics, the correspondent could disobey an order from the controller's management. There is therefore a concern that large enterprises which can afford a correspondent will be advantaged and will quite lawfully escape the oversight of CNIL, which will remain uninformed of the creation of thousands of databases.

## WINNERS AND LOSERS

### Political Interventions to Make the Regulations Less Restricting

Not only have political powers acted to lift specific constraints but, turning the transposition into internal law of the 1995 European Directive into an opportunity of sorts, they have called into question the protective regime as a whole.

The NIR code was at the core of an unremitting struggle between CNIL on the one hand, seeking to limit its use, and government and various administrations on the other, which sought to broaden its circulation. CNIL's restrictive doctrine concerning how that code could be used was very quickly criticised by a number of administrative officials. For instance and after CNIL had objected numerous times to the use of the NIR for its surveys, the *Institut national de la statistique* came to the view that CNIL's doctrine conflicted with the interests of statistical research. For its part, the fiscal administration considered that it made tracking down fraudsters more difficult. Starting in the mid-1990s, government and parliamentary circles have tended to consider that NIR-based data matching within the public administration would increase effectiveness in implementing public policy. Those views led to an attempt at stepping backwards and rehabilitating the notion and practice of data matching. In November 1996, a report issued by the *Conseil d'État* in preparation for the EU data protection directive transposition went as far as advocating a broad extension of the use of NIR and proposed to eliminate CNIL intervention in that area. In 1997, a bill was proposed to permit data matching between fiscal and welfare databases using the NIR. In November 1998, a parliamentary amendment, tabled during discussion of a finance bill, would have allowed data matching between all fiscal databases in order to combat fraud, using yet again the NIR.

The intervention of the *Conseil constitutionnel* allowed CNIL to limit the scope of this operation, by establishing a distinction between case-by-case consultations of the NIR registry for verification purposes on the one hand, and massive data matchings using the NIR on the other. After the 2004 legislative amendments, it is unclear whether the Commission is still able to oppose the extension of the uses of the national identifier. Today, some experts and ex-members of CNIL consider that the legislative modification has lowered the level of protection and reduced possibilities of controlling public files, particularly those dealing with security and public safety. Whereas beforehand, CNIL needed to issue a favourable opinion prior to some types of operations being allowed, it is now merely required to offer a reasoned opinion which must be made public. The data processing under consideration may then be implemented, whether that opinion is favourable or not.

By repealing section 12 of the *Informatique et libertés* legislation through

an act adopted on 11 March 1988 concerning the financing of political parties, political circles clearly privileged petty corporatist interests. This repeal, which allows extended communication of electoral lists during periods other than electoral campaigns, was obviously guided by financing and propaganda interests rather than by the wish to preserve data confidentiality.

Regulation of video-surveillance systems in public areas has been taken out of CNIL's hands, although the Commission considered itself competent (Heilmann and Vitalis 1996). Following a recommendation from the *ministre de l'Intérieur*, the Balladur government was able through legislation on security issues adopted in 1995 to establish a distinct regime, which delegates the greatest part of regulatory powers in that area to prefects, assisted by departmental commissions. Even though its ability to intervene was marginalised, the means of monitoring video-surveillance practices established in the 1995 statute were largely inspired from CNIL recommendations (information to citizens, limitation of the period during which data may be kept, access rights).

The preparation of the transposition of the 1995 EU Directive on data protection allowed political authorities to criticise CNIL's role and vent their hopes of remodelling data protection on a less constraining basis. A report commissioned from two members of the *Conseil d'État* at the time is most significant in this respect. The authors of this unpublished report, handed to the government in October 1996, considered that the protection regime as it had evolved no longer truly corresponded to the legislator's intent back in 1978. They faulted CNIL for having an overbroad conception of its role, leading it to seek an increase of its control over private sector activities and to become a joint decision-maker regarding public sector activities. Fearing unpopularity as the issues touch highly sensitive individual freedoms, governments would have been politically unable to decide against unfavourable CNIL opinions, even though the legislative framework allowed them to. That would have resulted in turn in difficulties and delays to government action, but also in the creation of a non-regulated sphere, since a great number of data processing activities had not been duly declared because of the associated constraints. Starting from the provisions of the European Directive, the report recommended a full review of the framework so as to make it less constraining, especially with regard to *fichiers de souveraineté*<sup>18</sup> and data matching programs involving databases from different administrations, as long as they came under a well-defined public interest purpose. Lost elections and the institution of a left-wing coalition government reshuffled the cards, however, and put an end to that project.

---

<sup>18</sup> So-called *fichiers de souveraineté* are now mostly regulated under section 26 of the 1978 legislation as amended and include databases related to defence, national security and criminal prosecutions, thus to issues having to do with national sovereignty.

## Reducing and Bypassing Data Protection in some Professional Sectors

Three sectors are characterised by a use of computerised technology that is only lightly constrained by the new data protection norms: the police, the fiscal administration and the banking sector.

One of the most threatening sectors for individual liberties, police activity, is paradoxically one of the least controlled. In the name of *raison d'État* and France's regalian tradition, the police are often exempt from ordinary obligations. The *Informatique et libertés* legislation bears the mark of this police exception. All data processing activities concerning state safety, defence and public security benefit from a less burdensome framework. For the police, files and databases have always represented essential tools, just as they represent a threat to citizens' civil liberties. The computerisation of these files, aimed at increasing police effectiveness, worsens the threat. The list of police databases has only grown longer in the last few years, as they multiplied. To the 'classics' such as the files held by the *Direction de la sécurité du territoire* (DST), and the *Renseignements généraux* (RG) or the 'Most Wanted' and antiterrorism databases were added STIC<sup>19</sup> (with records on 5 million people), the national genetic profile database, the database concerning persons agreeing to shelter foreigners, the visa claimants' fingerprinting database and soon, perhaps, any number of databases related to the new biometric ID card.

Control over these databases is all the more tenuous in that severe inroads have been made into the protective framework by legislators and that the applicable rules have been poorly applied. The legislation stipulates that data processing can only be implemented on the basis of a statutory decree, taken after CNIL consultation. For data processing activities set up before 1978, the legislation provided a period of two years during which the administration was supposed to take the necessary decrees. It sometimes took over ten years for the main police and defence databases to be regularised: defence, foreign safety and territorial surveillance databases were only put in order in 1986, RG and antiterrorism databases in 1991. In 1986, in accordance with the law, statutory decrees authorising data processing were not published and thus escaped public scrutiny.

So that sensitive data can be included in such databases, the act also allows derogations through the adoption of a *décret en Conseil d'État* taken after obtaining a favourable opinion from CNIL. Thanks to that provision, the Commission became in effect a joint decision-maker and was therefore able to

---

<sup>19</sup> The *système de traitement des infractions constatées*, which records personal data about both the victims of criminal offences and suspects against which, at the least, significant and tallying clues linking them to an offence have been discovered (whether or not they have been formally accused or found guilty).

request that some rules be implemented: manual records may not be kept without some control, nominative lists must not be established on the basis of sensitive data, proper authority is needed in order to have access to files and databases must be regularly updated. This power granted to the regulatory authority explains why authorisation procedures could take several years, since the Commission would provide a favourable opinion only after having obtained guarantees over the implementation of a minimal safeguards through preliminary negotiations.

This process explains the existence of many illegal police databases. With its principle established by legislation adopted in 1995, the STIC mega-database, listing all persons having been concerned in a penal procedure, was set up that very year, although the decree authorising the system was only taken in 2001. In order to by-pass the hurdle represented by the regulatory body, the government occasionally chose the legislative path, as it did when setting up the national genetic database for persons having committed sexual offences. The 2004 legislative amendment has now removed all existing obstacles. CNIL has lost whatever joint decision-making powers it might have had regarding the creation of such a database. It is still required to express an opinion, which is made public, but the government may decline to consider CNIL's views. This marginalisation of the Commission may be all the more prejudicial since data processing for security purposes tends to be on the rise.

One last relaxation of the protective framework concerns individual access rights to police files, which can only be exercised indirectly. The legislation requires that the access request be dealt with by a CNIL magistrate. This indirect procedure is frustrating both for the individual, to whom the contents of the file is not always transmitted, and for the magistrate, who is quite often only given access to incomplete information. There are only 100 such requests per year. Following the setting up of STIC in 1995, and after it started being used in pre-hiring investigations related to certain positions, the number of requests rose sharply. There were 671 requests in 1999, which led to 1100 verifications, since one individual can be listed in several files; five years later, in 2004, the number had risen to 1970, with 2500 required verifications. All in all, since it was set up, CNIL has received around 10,000 indirect access requests and has undertaken 17,000 verifications which, in many cases, led to the erasure of inaccurate data. It is worthy of note that internationalisation of police files (Interpol, Eurodac, Shengen information system and Europol files) does nothing, despite the safeguards provided, to simplify control (Elmajzoub 2004).

The fiscal administration has turned to computerisation more systematically than any other. All its large national databases have been computerised in order to better establish and manage the different taxes it collects. In order

to better assist fiscal controls, it has also set up diagnosis support and collection support programs. These various data processing systems all comply with the individual's right to privacy and the new rules concerning personal data protection. The decisive advantage that this administration benefits from, considering the restrictions these rules establish, is not obvious at first. It takes the form of a right to disclosure, which allows the fiscal services to access – and, if necessary, copy – information that was not primarily intended for their use. When a data process is set up, the legislation requires that a list of users be drawn on the basis of its purpose. Its status of 'authorised third party' exempts the fiscal administration from the requirement to figure on such a list even though it may access the data for a purpose wholly different from the one which was declared by the data controller.

With the multiplication of centralised systems and the development of their processing capacities, this right to disclosure has become of prime importance. Without anyone quite realising what was happening, the investigatory powers of the fiscal services have hugely increased. CNIL stepped in to ensure that access to databases be restricted to a case-by-case basis and therefore to avoid the transmission of whole databases or chunks thereof. This temptation remains strong, however, as shown by the tax administration's attempts, in 1991 and 2004, to access the Canal+ pay-TV subscriber database in order to track down fraudsters who were not paying their audiovisual tax. Since 1997, such fraudsters have also been sought through the dwelling tax. This crack-down on fraud explains why data matching is of such interest for the fiscal administration. Although the tax services stopped using the NIR for taxpayer identification in 1984 at CNIL's request, they have repeatedly requested to be allowed to use the NIR ever since.

As private law undertakings, banks benefit under the 1978 legislation from lighter prior requirements regarding data processes, which simply need to be notified to CNIL. Control is therefore somewhat undermined. Banks, which are massive users of nominative data and hold considerable powers, showed very early on their reluctance to bow to CNIL's control over their practices. The Commission's decisions have constantly been attacked in court, especially when it set standards concerning 'scoring' techniques and behavioural segmentation (Huet and Maisl 1989).

As soon as the 1978 legislation came in force, CNIL turned towards a sector well known for its extensive use of nominative data, either for account management, canvassing-related profiling or borrower risk assessment. After consultations with the industry, the Commission drew up two simplified standards in order to streamline preliminary declarations concerning account and loan management. The latter standard also specified the type of information that could be processed and forbade data transfers to third parties. It also indicated that an annex to each declaration must describe the factors used by the

scoring technique used for automated risk evaluation and prohibited using this technique to fully automate the credit decision. Following several complaints, CNIL undertook audits which revealed that the standard had not been applied: data had been shared between credit providers, information had been added to files and the provisions regarding scoring techniques had been ignored. Moreover, delinquent debtor files had been set up without providing legally required safeguards.

In 1985, after consulting again with the industry, CNIL modified the standard in order to exclude scoring techniques and make them subject to an ordinary declaration. At the same time, it published a recommendation guiding banking establishments on their obligations in the field of data protection: providing information to customers regarding their rights prior to obtaining or using data, disclosure of reasons for refusing loans, compliance with limits regarding the conservation or disclosure of data pertaining to borrower delinquency. Yet again unwilling to apply either the simplified standard or the recommendation, several banks referred the matter to the *Conseil d'État*, claiming CNIL had acted beyond its powers. The resistance of the banking sector paid off, as CNIL then altered its stance in a way agreeable to the industry. The period during which data could be kept was revised; credit providers being of the view that there is no 'right to credit'; disclosure requirements to customers who are denied credit were reduced. The Commission subsequently reaffirmed the ban on banking establishments to use data that did not originate with their commercial relationship with the customer, and especially sensitive data. A recommendation on credit, updated in 1998, requires banks to provide CNIL with the parameters used for scoring so that it may exercise some control. For instance, nationality cannot be used as a discriminating criterion by granting for instance, as had been observed, ten points to French nationals or two to EU nationals, and taking away ten points from other foreigners. Once again, CNIL's decision was challenged as exceeding its powers and, in 2001, the *Conseil d'État* quashed it.

Following a complaint lodged in 1993, CNIL attempted to monitor behavioural segmentation techniques, which consist in establishing client profiles based on analysis of their accounts. These sometimes questionable profiles being potentially discriminatory, the Commission specified that they could not base automated decisions and that customers were entitled to be informed of both the information and the reasoning behind a negative decision. It also concluded that as customers have access to all the data concerning them, they could also know which segment they were put in. This last conclusion was strongly opposed by the bank involved in the complaint but its claim before the *Conseil d'État* that the Commission was exceeding its powers was denied in 1995, the *Conseil* siding with the Commission.

## Recognised Data Protection in Other Areas of Society

The new data protection rules provided a legal basis for professionals of the social sector who were seeking to protect the secrets of assisted persons and limit administrative indiscretion. While they could not prevent increased workplace control based on new information technology, they at least succeeded in preventing some abuses.

In the social and medico-social sector, concern over the protection of data confidentiality existed even before the adoption of the 1978 legislation. In the late 1970s, doctors and social workers opposed automated data processing systems which worsened working conditions for personnel bound by professional secrecy and, above all, placed assisted persons at risk of discrimination as their handicaps became less thickly veiled. The adoption of the *Informatique et libertés* Act was to provide a stronger foundation to their struggle as well as an *a posteriori* acknowledgment of its relevance.

In 1981, the recently created CNIL issued an unfavourable opinion regarding the GAMIN national system designed to identify so-called 'risk-prone' children, and so brought to a close a controversy that had lasted several years. Almost 20 years later, doctors and social workers once again raised issues with new and decentralised systems, now based on a network architecture and data sharing. The watchfulness shown by these professionals made it possible to limit 'overcoding' of the populations, by nature fragile, that require support and to step back from methods such as profiling, distributed computing and database multiplication in an area where human contact must remain essential. A pressure group called *Pour les droits des citoyens face à l'informatisation de l'action sociale*,<sup>20</sup> set up in 1997, and which is largely composed of professionals, advocates for a computerisation of data related to social action that shows respect for people's rights. Its actions facilitate CNIL's oversight of compliance with the legislation and have sometimes prompted the Commission to show more firmness.

The multiplication of assistance and social integration mechanisms throughout the 1990s has led to increased control over the most destitute people, in order to monitor their resources and fight fraud. CNIL has been unable to oppose either the creation of numerous databases including information on those persons or data sharing between the organisations involved in that sector: prefectures, local councils, communal social action centres or departmental directions of social and sanitary action. It ensured, however, that those processes would come with appropriate safeguards, regarding in particular the relevance of recorded data and the length during which it could be

---

<sup>20</sup> Or 'For citizens' rights, facing the computerisation of social action'.

kept, security measures and proper information to affected people. It sometimes put a stop to inquisitiveness by issuing unfavourable opinions. For instance, it opposed a project thought up by a local council which sought to undertake a non-compulsory statistical survey so as to be the first to gather data on the population benefiting from the *revenu minimum d'insertion* (RMI).<sup>21</sup> The survey intended to collect data on respondents' membership of political associations or their inclination to contact a clergyman in case of hardship. Very specific health-related questions went as far as enquiring whether and when the person had undergone a gynaecological examination.

In other areas and especially in the public sector, over which CNIL can exert more oversight, computerisation took into account data protection, which thwarted some projects. Telecommunications provide a quite telling example. While managing an infrastructure of prime importance, the telecommunications industry carries out large public investment programs, implements new technologies or markets phone directory data. Data protection is involved in all such activities.

Following a 1985 request by the *Direction générale des télécommunications*, CNIL determined the conditions associated with the use of automatic diallers, subjecting message transmission to written prior consent by addressees. On integrated services digital networks (ISDN), it opted for freedom of choice, a position that went against the telecommunications administration's wish systematically to provide caller identification (Caller-ID) to the called party so as to allow them to manage incoming calls and deter malicious callers. Based on respect for individual freedom, CNIL's advice in another area was followed, with important consequences for the future. The development of activities related to phone directory data marketing and the creation of new types of directories sharply raise the issue of the right of the subscriber to object to having personal data so peddled. The regulatory body authorised phone data marketing but imposed a number of conditions: the subscriber must be able to oppose inclusion of his own data; the database as marketed must only enable sorting by alphabetical, geographic or professional criteria; and the purchaser must be made aware of the restrictions associated with using the list. In 1987, CNIL strictly limited directory improvement through the addition of information on services and types of terminals used by subscribers. Again in 1987, it forbade business database 'improvement' through data matching with directory data, which would have essentially served telemarketing purposes. In 1990, CNIL issued a negative opinion following a request by France Télécom, which hoped to use the full phone subscriber database (including the *liste rouge* of unlisted numbers) to promote its own products.

---

<sup>21</sup> RMI is a type of welfare allocation.

Lately, CNIL has also called into question the traditional way of doing things, according to which a subscriber is in the directory unless he or she requests to be unlisted, by concluding that universal directories should only include data from mobile subscribers who expressly request their inscription. Legislation on electronic commerce which was adopted in 2004 endorsed that position.

## INFORMATION FLOWS AND RESTRICTIONS

Abuses flowing from what information technology has to offer frequently dictate the shape of protective efforts, as is clear in the consumer protection and labour fields. Businesses using those technologies for commercial or surveillance purposes quickly find that the new possibilities come with new constraints. It is also possible, however, to ensure that technical innovation better serves the individuals' control over their personal data, as happened in the health sector.

Direct marketing is especially adapted to increasingly personalised consumer habits. It supposes knowledge about the targeted individual and the use of sophisticated information technology. It represents a highly asymmetric form of communication and is often perceived as an aggression and an intrusion into the right to be left alone. With e-marketing and even more with spamming, its most questionable iteration, such aggressions and intrusions have become unbearable (Belloeil 2001; Barrier 2003). Spamming is email's true bane. After capturing millions of email addresses, numerous businesses take advantage of the possibilities provided by the internet to harass consumers with unsolicited advertising. Spamming, which has spread in France just as elsewhere in the world, cares nothing for borders: in fact, most spam messages sent to French internet users are in English.

The genuine pollution of the network by messages whose content is often illegal and whose deletion wastes significant time has sparked reactions. The French internet service provider association has decided to shut off customers known to be spammers. CNIL ran an anti-spam campaign in 2002, opening a 'spam box' to which internet users were invited to transfer unwanted messages which clogged their in-box. The European legislator stepped in, followed by the French parliament. In the context of the review of the 1997 telecommunications directive, a new *Directive on Privacy and Electronic Communications*, adopted in July 2002, extended through its Article 13 an opt-in regime to the use of email for direct marketing purposes. This clarification put an end to restrictive interpretations of a provision in the 1997 Directive which set aside the opt-out regime and superseded the 1995 data protection Directive, whose section 14 creates an 'opt-out' right regarding data processing for business purposes and data transmission to third parties. The new regime does not apply

where a subscriber's contact details have been obtained in the context of a business relationship with the entity that would use them, but the subscriber may oppose subsequent uses of his or her email address.

The 2002 Directive was transposed in France by legislation adopted in June 2004 on 'confidence supporting the digital economy', which some have nicknamed the 'anti-spam' legislation. Like the European text, the legislation forbids business email-based direct marketing using a physical person's contact details unless that person has expressed prior consent to receive such messages. The legislation specifies that such consent, which must be express, may not be drowned in general sale conditions. Direct marketing professionals, who had already adopted a code of ethics in 1993, drafted a new code in 2005 to reflect these new legislative provisions. This code, approved by CNIL, provides examples of consent procedures, such as checking a box on data collection forms. Those measures should surely limit email commercial harassment even if they cannot completely block messages which scoff at national borders.

Information technology's progress provides employers with a broad range of workforce control procedures (CNIL 2001). Abuse has happened, especially with regard to staff evaluation and the monitoring of daily life in the workplace. Video-surveillance cameras installed in large commercial retail stores in order to monitor customers are also used in order to keep an eye on staff, although that purpose is seldom acknowledged. Video-surveillance is often used as a work and productivity control tool, as several dismissal cases taken to court have shown. Under the pretence of business security requirements, microchip cards and electronic badges are imposed upon workers and soon become a means of recording the employee's every movement. Private branch phone exchanges (PBX) allow for thorough control of telephone usage. With email communications, the potential for indiscretion increases tenfold.

The 1972 and 1992 statutes on labour relations postulate that, as a citizen, the employee is granted fundamental rights that must be enforceable within the enterprise. All the provisions of the *Informatique et libertés* legislation apply to any personal data processing which requires notification to CNIL. The *comité d'entreprise*<sup>22</sup> must be informed and consulted prior to any decision introducing technology that might be used to control employee activity. Two fundamental principles have emerged that guide the use of such technology: a transparency and information principle, and a proportionality principle

---

<sup>22</sup> French law requires the creation of an enterprise committee in any undertaking with more than 50 employees. The committee is chaired by the enterprise's highest manager or his delegate and usually includes a majority of elected employee representatives. It must be consulted on a number of management issues and has sole responsibility for social activities within the enterprise.

(Lyon-Caen 1991). The enterprise is thus allowed to monitor private use of internet by employees at work, as well as their phone conversations, provided that employees have been informed beforehand and that the methods applied are proportional to the purposes for which they have been introduced.

Medical data is extremely sensitive information that can cause discriminatory behaviour in the employment and insurance areas. It is therefore strongly protected: the data protection framework creates a specific regime with reinforced safeguards, while doctors are bound to professional secrecy. This framework complicated the use of such data for epidemiological research, which led to legislative changes in 1994. The institution of a fully computerised personal medical dossier (the 'DMP'), which proceeded from the August 2004 amendments, marked a significant change in the way protection is conceived. Whereas up to that moment responsibility rested primarily on health professionals, who controlled the files where health data was kept, henceforth the patient stands as the prime person responsible. Legislation on the rights of patients and aiming at improving the quality of the health system granted patients a direct right of access to the DMP in 2002, thus eliminating the previous indirect access policy, which reserved direct access to doctors. Henceforth, the patient may have complete access to his or her own file through the internet. Moreover, patients are granted the right to control the access of health professionals to their file.

The creation of the DMP, which should be finalised by 2007, aims at getting the very best out of information technology in the field of healthcare. It is part of a European Commission plan of action to establish a European online health community. The aim is to improve the quality of healthcare and the productivity of medical workers, as well as to increase the information system's rationalisation. The DMP, which carries all the patient's antecedents, will be stored on the internet by an authorised host, which must demonstrate high proficiency in the fields of data safety protection and confidentiality. The micro-chip *Vitale* card, currently used for social security payments, will act as the key allowing access to one's file. Its next versions will contain a zone storing the information most necessary in the event of a medical emergency. The patient will give the doctor his or her card in order to allow access to the DMP and that authorisation will be needed for the professional to be paid by the health insurance regime.

Data protection is obviously a critical issue in such an environment. There are safeguards provided by the legislation regarding access to the DMP. For instance, it will not be available for occupational medicine purposes or where a contract requires a health evaluation from one of the parties. Moreover, any commercialisation of the individual's health data is banned: 'Any financial transaction based on nominative health data, including transactions taking place with the consent of the person in question, is forbidden and would

constitute a reprehensible offence, with regard to article 226-21 of the Penal Code'. Doctors' unions have nonetheless challenged the very purpose of the DMP from a medical point of view, while other critics have pointed to a number of issues it raises regarding the preservation of medical secrecy in a health system that favours data sharing among a wide range of professionals and where computerisation, insofar as it makes access easier, increases potential risks for unauthorized disclosure.

## FUTURE PROSPECTS

The international dimension of the issues surrounding computerisation and liberties is acknowledged in the first article of the 1978 French legislation, which declares that the development of computerisation must take place within the framework of international cooperation. The absence of rules or their disparities obviously represent a threat for individuals' privacy, as 'data havens' can always welcome underhanded data controllers. With economic globalisation coupled to the development of information technology, state sovereignty over its territory is no longer what it used to be. The internet starkly illustrates how difficult it is to control the circulation and use of personal data on a planetary network. Behind the widely shared dream of a global information society hides the spectre of a surveillance society which has yet to be adequately considered (Campbell 2001).

Since 11 September 2001, numerous security-related information systems have been set up in the name of the fight against the terrorist threat. France saw new processes being created one after the other: access to the national police antecedent database was extended to support administrative enquiry purposes, the national genetic print database for sexual offenders now includes all persons suspected of a variety of other offences, a database collects the fingerprints of all visa applicants and another keeps track of French or foreign persons agreeing to shelter foreigners. The 'Interior Security' Act of 11 November 2001 compels internet service providers to retain all traffic data for a period of up to one year. An antiterrorist bill currently under discussion in Parliament would require the collection of more personal data (video-surveillance, transport data, telephone communications and internet traffic data). The European Union opted on 2 December 2005 for the adoption of a directive making the retention of certain telephone and electronic communications data compulsory. In the USA, directly after the 9/11 tragedy, the adoption of the PATRIOT Act showed how security considerations can overshadow all others. The 'Total Information Awareness' project (TIA), elaborated by the Pentagon and which Congress refused to support financially on 26 September 2003, illustrates just how far these considerations can lead. After all, the plan was to

organise total surveillance of information on every single one of the planet's 6.2 billion inhabitants!

The inadequacies of a strictly national protection regime led Europeans to adopt the 1995 Directive on data protection, which was completed by another one on telecommunications issues, adopted in 1997 and revised in 2002. This drive towards harmonisation must be pursued on a worldwide scale. For many years, the OECD and the UN have been working in that direction. The main hurdle is opposition between two different approaches: a European approach, based on legal intervention and the setting-up of specialised regulatory bodies, and an American approach, based on auto-regulation by the operators themselves and private sanctions. The first approach is more global and relies more on the state, as it raises privacy protection to the status of a human right that the state must guarantee. The second approach, under which law simply functions as a substitute in the limited areas where the market failed to solve problems, is more open to permitting information to circulate freely, with all due regard for individual rights.

Commercial activities and personal mobility have made it necessary to find a compromise between the two approaches. Since the 1995 European Directive only authorises data transfers outside the Union if the recipient country ensures a sufficient level of protection, a 'Safe Harbor' protocol was signed in the year 2000, which US companies have to adhere to in order to ensure that they provide the required level of data protection. The debate on data transfers concerning airline passengers travelling to the United States illustrates how difficult this harmonisation may prove to be. By an agreement signed in May 2004, the European Commission authorised such transfers on the basis that the United States offered adequate safeguards, despite the fact that the European data protection group and the European Parliament both opined otherwise. The Parliament has since referred the matter to the Court of Justice of the European Communities, which should render a judgment on the agreement's legality during the spring of 2006.

It is through the creation of an independent regulatory commission that data protection was able to take shape in France. The legislation would probably have remained largely unheeded without the intervention of a commission that could not prevent the spread of data processing and control techniques but that did help to minimise or avert altogether the most significant threats they presented to liberties.

Today, in a context of generalised computerisation, where data processing and personal tracking procedures are constantly spreading, it becomes more necessary than ever that all stakeholders shoulder the resulting responsibilities. Enterprises are obviously among the most deeply involved. In that regard, self-regulation based on codes of ethics may be quite useful provided it is supported by legislation which it supplements and customises. Without some

legislative buttress, there is a risk that an exclusively self-regulatory approach would lean too much towards operators and not protect data subjects adequately. Politicians and judicial authorities must also feel involved, as well as the media and the educational system. So far, data subjects themselves have shown insufficient concern over the way their data are used and it is time they faced their responsibility. Such is the case when one's consent is required and written consent is sought in order to use medical data for research purposes, or when one is asked to check a box on a form for marketing purposes. The creation of an individual healthcare file also points in this direction, giving individuals greater control over their medical data and allowing them to decide whether it should be disclosed to healthcare professionals. Citizens dealing with the now-electronic administration should also have more power over the uses to which the information they provide are put.

At the dawn of the twenty-first century, there is no point in hiding from the fact that there are hard times ahead for data protection. It must face accelerating innovation with the emergence of new and, from a risk assessment standpoint, poorly understood control technologies, such as biometrics or RFID chips, which make it possible to track not only objects, but also their owners. In addition, the economic value now given to personal data and the priority given by all states to security requirements make the respect of individual liberties look like a luxury that may seem rather quaint. The only reason to remain optimistic in such a context is to remember that privacy is never so valued as when it comes under threat (Baudry et al. 2002). Privacy only becomes a concern, and indeed is only truly prized when it is endangered.

# 5. Privacy in Australia

## Graham Greenleaf

---

### INTRODUCTION

The defining events in the history of privacy protection in Australia have had a great deal to do with politics, little to do with an orderly process of law reform, and nothing to do with the Courts.

### FORMATIVE EPISODES, 1987–1992

#### The Australia Card

In June 1987 a Federal Labor Government was triumphantly returned to office after an unprecedented dissolution of both houses of Parliament. That dissolution had been triggered by Opposition rejection of a Bill to introduce a national identity card, the Australia Card. Since the idea of an ID card to combat tax and welfare fraud was first floated in mid-1985, public support had stayed at around 68 per cent. But three months later it was down to 39 per cent and falling, and the intensity of the mounting opposition to the Card astonished everyone. Though it had rarely been a newsworthy item before or during the election, by September the media were preoccupied with the Card. Sydney talk-back radio journalist John Tingle claimed that for some weeks it was impossible to get callers to talk about anything else. *The Australian* newspaper editorialised (15/9/1987), when letters to the editor were running twenty to one against the Card:

There has never been a debate like it in the letters page; there has never been such a cry of opposition from the nation over one topic . . . It has dominated the mailbag to the point where today, for the first time, we present two pages on the topic.

With dissidents appearing in its own ranks (particularly in State Parliaments), Labor faced a totally unexpected political crisis. It received a dramatic face-saving exit when opponents found an apparent loophole in the Bill's drafting. This meant that the Opposition-controlled upper house could indefinitely

delay the effective introduction of the Card even though the government's election victory guaranteed passage of the Bill. There was considerable dispute over whether the drafting flaw was fatal (Starke 1987, Greenleaf 1987a), but the government quickly dropped the Bill rather than endure the politics.

What had caused the massive change in three months? With the election over (so government supporters were more willing to be anti-ID), and the reality of the Card imminent, potential opponents of the Card joined forces in a number of extra-Parliamentary opposition groups. The media-oriented Australian Privacy Foundation was formed as a coalition of public figures spanning the political spectrum, including rock singers, yacht designers, doctors and academics. By September, many grassroots local groups held significant anti-Card rallies, at a rate of more than one per day, with consequent continuous media attention. An important factor was a deep-seated distrust of the Health Insurance Commission (HIC), which was to operate the Card's computer system (Greenleaf and Nolan 1986, Greenleaf 1987a). The more people knew about the Australia Card, the less they liked it. It would in fact have been an extremely extensive information surveillance system with multiple uses from inception, no logical limits (or intended limits) to its expansion, and *de facto* extension as a principal identifier in the private sector (Greenleaf 1987b, Greenleaf and Nolan 1987, Clarke 1988).

Twenty years later, Australia still does not have a national ID card. It has become a ritual observance in Australian politics for supporters of any identification scheme to deny that it 'is anything like the Australia Card', because the opprobrium attached to that name is still so strong. Yet in 2007 the Australian government was once again proposing to introduce a ID system, the 'Health and Welfare Access Card', which opponents argued would be worse than the Australia Card, but the government insisted was not a national ID card. This ritual is so entrenched that the legislation to enable the proposed card contained a clause proclaiming that it was not intended to be a national identification system. We will now take the journey from the Australia Card of 1987 to the Access Card of 2007.

### **Public Sector Surveillance Emerges**

In the wake of the Australia Card, a political compromise was reached, comprising an enhanced Tax File Number (TFN) system, and the Privacy Act 1988, Australia's first enforceable privacy legislation. The original TFN legislation prohibited disclosure and use of TFNs beyond tax-related purposes (an essential part of the 'no Australia Card' bargain). However, only two years later, the federal Labor Government (with opposition support) reneged by extending it by further legislation, so that TFNs could be used for

cross-matching of taxation information with information concerning federal 'income support' benefits (social security, veterans' affairs, student assistance and first home-owners benefits) provided by four 'assistance agencies'. To check identification, electoral roll and Medicare identity information is also used. The matching is three way: between assistance agencies; from tax to assistance agencies; and from assistance to tax agencies. New legislation (the Data-matching Program (Assistance and Tax) Act 1990) authorised the new data surveillance regime (as it otherwise would breach the Privacy Act or TFN Act), set out very detailed operational rules for the surveillance system, and provided some procedural protections against its abuse, plus Parliamentary reporting obligations and Privacy Commissioner oversight. Such detailed and explicit 'data surveillance law' is still unusual.

This new system, often called the 'parallel data matching' scheme, was strongly but unsuccessfully opposed by privacy advocates. They took the view that if promises of privacy protection could so easily be broken once a surveillance system was established, then the TFN system was likely to become 'the Australia Card by installments' (Greenleaf 1990). This extension achieved some of the data matching aims of the original Australia Card proposals. Although it involves data surveillance on a massive scale, and in a relatively open manner, this data matching results in few if any complaints to the Privacy Commissioner (OPC Annual Report 2004–05, Tables 3.1 and 3.4). There have been some limited further legislative extensions of the TFN system, but 15 years later the TFN and the parallel data matching system has not been expanded further into one general purpose ID number and system. In this case 'function creep' was significant but not endless. However, as detailed below, other data matching schemes now pour data into the five key agencies, where it adds to the data used for 'parallel data matching'.

### **Positive Reporting's Negative Dividend**

The defeat of the Australia Card, and its TFN and data matching sequels, were key determinants of the shape of public sector surveillance for the next decade or more. The private sector equivalent was the defeat in 1991 of attempts to introduce 'positive reporting' by Australia's near monopoly credit bureau, the Credit Reference Association of Australia (CRAA). In 1989 CRAA provided over 95 per cent of consumer credit reports. CRAA and other Australian credit bureaux only provided 'negative reports', meaning that their credit provider members only reported when a consumer defaulted on a credit arrangement, by late payment or otherwise, plus details of applications for credit, but not whether credit was granted. In 1989 CRAA proposed to change to a system of 'positive reporting' whereby all major credit providers in Australia would provide CRAA with a monthly computer tape listing the

'payment performance' of each of their credit customers, whether or not there had been any default on the account. They claimed that this would allow credit providers to assess whether an applicant was over-committed. This resulted in considerable adverse media comment. Capitalising on this, the Australian Privacy Foundation (the NGO formed to fight the Australia Card) convened a 'Credit Reporting Summit' in early 1990, at the conclusion of which the federal justice and consumer affairs ministers jointly announced that the government would introduce legislation to prohibit 'positive reporting' and, furthermore, to comprehensively regulate credit reporting (Greenleaf 1992).

The resulting legislation overturned previous practices. Over the previous 20 years, in the absence of effective prohibitions in State legislation, CRAA had allowed real estate agents to check prospective tenants, government departments to check some occupational licence applicants (and applicants for telephone and other government services), insurers to check the credit history of suspect insurance claimants, and mercantile agents to search for debtors' addresses. Employment checking was not allowed. The new Act prohibited access to credit reporting files for any of these purposes. It added a set of information privacy principles tailored for credit reporting, plus a considerable number of criminal offences. CRAA had successfully extended the scope of its surveillance system for 20 years, but in attempting to further expand into 'positive reporting', it provoked far more extensive legislative control. The legislation therefore not only limited the future expansion of credit reporting in the private sector, it effectively 'rolled back the clock' by banning past extensions of credit surveillance which had become accepted practice in the private sector. It was described by CRAA as 'the most restrictive credit reference laws in the Western world' (Greenleaf 1992). It is rare for privacy legislation anywhere to attempt such a retrospective repeal of the extension of data surveillance. This legislation in effect destroyed CRAA's momentum toward becoming a comprehensive personal data register for the private sector. However, one downside was that from 1992 the practices such as tenancy checking that were forced out of the well-organised CRAA system in effect went unregulated until legislation caught up with the rest of the private sector in 2001.

Fifteen years later, personal information is still held by Australia's private sector in separate databases relevant to each industry sector, rather than in centralised multi-use repositories. CRAA's successors (Baycorp Advantage, now called Veda Advantage) revives the call for positive reporting every few years but without success as yet. Australia's 2001 privacy legislation for the whole private sector preserves the 'containment' of personal information within industry sectors (sometimes called 'silos'). This would not have happened if the key battle had not been won when CRAA overreached itself.

## KEY PERSONAL DATA SYSTEMS AND THEIR IMPACT

Here are some pieces in the Australian jigsaw puzzle of surveillance, and the legislative context on which the practices depend.

Closed-circuit television (CCTV) saturates the infrastructure of Sydney and Melbourne, in city streets and train stations, on buses, trains and taxis, sporting venues and in crime hot spots (Chulov and Hodge 2005). The ostensible reasons are personal safety and crime prevention, but the anti-terrorist dimension became clear with the installation of 315 extra cameras with face recognition technology in public transport facilities for the purposes of the September 2007 APEC meeting in Sydney (Besser and Clennell 2007). One reason for this proliferation is that there is no legislation governing visual surveillance in public places. Australia spends more money per capita on workplace surveillance equipment than most other industrialised nations (Bromberg 2004, cited in Cripps 2004). There is State-level legislation governing some workplace surveillance (by video, tracking devices, or computer), but it places few limitations on overt surveillance (for example, Workplace Surveillance Act 2005, NSW).

Telecommunications interception ('wiretapping') is under stricter legal control in Australia. It is illegal to intercept the content of calls except where authorised by a judicial warrant (Telecommunications (Interception) Act 1979). Legal intercepts quadrupled from 1998 to 2003, to more than 2500 per year (T(I)A Annual Report (2002–3) and earlier years).

An increasingly sophisticated system of financial transaction surveillance has been developed over nearly 20 years. Almost anyone dealing with \$10,000 or more in cash is required to submit financial transaction reports to AUSTRAC (a federal agency), resulting in over 10 million reports per year (Financial Transactions Reports Act 1988).

The statutory 'parallel data matching' system, already explained, is augmented by a huge amount of government data matching that takes place outside the controls of the data matching legislation. All of these compulsory extractions of data are 'authorised by law' exceptions to the non-disclosure requirements of the Privacy Act 1988. Mass surveillance of taxpayers and benefit recipients is a vast and complex enterprise by federal agencies. Its sources include uncounted private sector organisations and State government authorities (PCO Annual Report 2004–05, Table 3.7). Furthermore, this extra matching feeds data into the files of the five agencies involved in the parallel matching system, and therefore into its matching processes.

Since Australia does not yet have a national or state ID card or ID number, identification systems in Australia are usually built on the basis of production of alternative, or multiple, identification documents. The key federal numbering systems, the tax file number (TFN) and the Medicare number and card, are

little used outside their intended domains. The Medicare card is often asked to be produced as part of a '100 point system' proof of identity, but there is no 'TFN card' to produce. The main ID systems in current operation are: driver's licences (which are administered at State level); passports (held only by a minority of Australians); birth certificate copies (for particularly important events) and after that a profusion of different benefit cards, student cards, employer-provided IDs and so on. There is no requirement to carry ID in Australia, except that drivers must carry their licence when driving. Credit cards will usually be accepted without any other ID being produced, but it is common for a driver's licence to be requested when cashing cheques, and for the licence number to be noted on the cheque. Post-2001, ID is requested more frequently, for example in order to post a parcel. Some states now issue 'non-driver' photo ID cards to serve the same identification function as a driver's licence.

Private sector data surveillance of Australians is still characterised by personal data held primarily within industry sectors. Such data are aggregated very efficiently within particular sectors, but with limited 'crossover' either between private sectors or from the public sector. In credit reporting, Veda Advantage's service (formerly the industry-owned CRAA) claims to hold personal data on more than 14 million consumers, out of a total adult population of 21 million in 2007 (Veda Advantage's Consumer Credit Enquiries). It has had over 90 per cent of all consumer credit reporting business since at least the late 1970s. Credit bureaux can only store a legislatively-defined range of 'negative' information (excluding information about rental history, insurance defaults, reasons for job changes etc). Default information other than 'clearouts' and bankruptcies only stays on file for five years. In insurance reporting, Baycorp Advantage also runs Australia's largest insurance claims database, separate from its credit files. It claims it is contributed to by almost all of Australia's insurance companies and contains more than 18 million insurance claims of individuals and companies dating back ten years, complemented by public registry sources. Access is limited to the insurance industry.

The health services sector, which more than any other straddles the public and private sectors, does not have any single national or regional method of surveillance of medical histories as yet. Employers, insurers and others seeking details of a person's medical history are therefore forced to obtain the patient's consent to obtain reports from their most recent treating doctor, and do not have any comprehensive source.

Private sector access to personal information in registers held by public agencies varies widely across States and Territories because of varying legislation (or lack of it). At the 'accessible' end of the spectrum, there are open online registers of bankrupts and company directors, land ownership, and encumbrances over motor vehicles. Vehicle registration records are normally

only accessible for good cause (eg locating parties to accidents). Local councils have open registers of property development proposals, but usually only for inspection in person. Australia adopts the practice of other common law countries of allowing public online access to fully identified court decisions, and allows republication by third parties. At the 'inaccessible' end of the spectrum, access to records of convictions or criminal charges is generally prohibited.

Some new companies are attempting to aggregate publicly available personal information, particularly Acxiom which claims that its InfoBase product is the largest collection of Australian consumer and business data available in one source (Acxiom website, 2005). It is provided to clients principally for customer relationship management and direct marketing. For example, they sell lists of 'Pre-movers', people who are about to move and therefore whose loyalty to existing businesses may be weakened, as well as 'New Movers', 'Renovators', 'Affluent Homeowners' and so on.

The domestic direct marketing industry operates carefully compared with some countries. Direct marketers are generally required to offer an opt-out in marketing communications (Privacy Act 1988). Do-Not-Call list legislation commenced operation in mid-2007. There has never been significant domestic email spamming. Nevertheless, the federal SPAM Act 2003 imposes severe penalties on any activities resembling spamming. Its main effect is probably to prevent anyone using Australia as a base for international spamming operations. The first prosecution under the Act resulted in financial penalties of \$4.5M for the company concerned, and \$1M for its principal (*Clarity1 Case*, 2006).

## MAJOR PRIVACY MEASURES AND INSTITUTIONS

The Courts have not yet developed any general common law protection of privacy. Privacy Commissioners have been so mild and technical in their enforcement of privacy legislation that they rarely win public attention. Compared with the essentially political events outlined at the outset of this chapter, the enforcement of privacy laws by Courts or privacy Commissioners have lacked defining moments which shape public or elite consciousness about privacy.

By 2007, Australia has seven major information privacy laws: the federal law covering the private sector; and the laws covering the public sectors of the Commonwealth, NSW, Victoria, the Northern Territory, the Australian Capital Territory (ACT) and Tasmania (plus a Bill in passage in Western Australia). This leaves only South Australia and Queensland without such a law but only non-enforceable government administrative rules. In addition there are some

sectoral laws with customised sets of information privacy principles for credit, health and telecommunications data. These numerous laws vary a great deal in their exceptions and exemptions and in the effectiveness of their enforcement. Each contains a set of information privacy principles based substantially on the OECD privacy principles (OECD 1980). They are variously entitled 'Information Privacy Principles', 'National Privacy Principles' and 'Information Protection Principles'. They contain many variations which provide grist for lawyers and disappointment for complainants. Nevertheless for the purposes of this chapter their content is substantially the same and they will be referred to generically as 'information privacy principles' or 'IPPs'. None of these laws contain general definitions of 'privacy': breaches of these laws are defined to require breaches of their IPPs.

In a federation like Australia, State and Territory governments control more important personal information than the Federal government, including births, deaths and marriages registers, drivers' licences, education records, some building approvals, prison records, and criminal records. It is therefore important that data protection laws be effective at all levels of government. Where State and Territory privacy laws exist, they include local governments in their scope.

## KEY DEVELOPMENTS IN PRIVACY PROTECTION

### **The Australian Legal Context – Privacy Rights and the Courts**

The determining factors in Australia's privacy history have been political conflict, the media and their effective use, and legislation (both its passage and its defeat). Unlike elsewhere Courts have played a minor role. Why is this so? Australia's very boring history, constitutional structure, and legal history provides much of the explanation of why privacy is protected in Australian law principally by a patchwork of specific legislation, not by any broad remedies developed by the Courts.

The political context is that of unbroken 'normality': Australia's peaceful achievement of independent nationhood, her continuous democratic history since Federation in 1901, her almost entirely peaceful internal political development, and the relatively low level of external threats due in part to Australia's lack of land borders. Perceptions of both internal and external threats to security continue to have adverse effects on privacy protection, but Australian democracy and privacy have never had to 'recover' from authoritarian rule as has happened in other countries. But as we will see, such a boringly happy history provides no guarantees against the emergence of a surveillance state in the twenty-first century, and could prove to be a disadvantage.

Australia is a federation of eight states and territories, all of which have a common law tradition. It lacks any significant constitutional protection of privacy at Federal or State level. There is no entrenched 'Bill of Rights' in the constitution of any Australia jurisdiction, so there is nothing there on which Courts can build privacy rights. The closest thing to a constitutional right of privacy is that common law courts, when interpreting legislation, will do so in ways which avoid interference with 'fundamental rights' unless the statutory language clearly directs them to. On the other hand there are no 'first amendment' problems: there are no constitutional freedom of speech rights which can prevent legislative restrictions on disclosures of personal information, other than some very limited protections of political speech. If governments want to prevent access to Court records, limit who can access credit bureau, or forbid disclosures of any personal information, there is no constitutional bar to their doing so.

Following a sentencing hearing of YZ for rape within marriage of Jane Doe, ABC radio broadcast details including the name of YZ, that the offence was rape, the suburb in which the rapes took place, and in one broadcast the real name of Jane Doe. Many listeners subsequently attempted to contact her and her family. Evidence was given of the substantial and long-lasting psychological damage that this caused to her. Two ABC journalists subsequently pleaded guilty to breaches of legislation prohibiting identification of rape victims. Ms Doe then sued both the journalists and their employer (the broadcaster), and one of her grounds was a breach of a common law right of privacy. A District Court found in her favour on this and other grounds, and awarded her A\$234,000 damages (*Jane Doe v ABC case*, 2007). The case is now on appeal. Many lawyers had believed that an old High Court case (*Victoria Park Case*, 1937) established that there was no such common law right of privacy, but in 2002 the High Court said this was still unresolved (*Lenah Game Meats Case*, 2002). The appeal cases in *Jane Doe v ABC* may resolve this question.

Nicholas Toonen, gay rights activist from Tasmania, objected to his State's Criminal Code which made all sexual contact between consenting male adults in private a crime. Instead of trying to protect his sexual privacy through Australia's Courts, he took his case to the Human Rights Committee of the United Nations. How did he get there? The only treaty imposing obligations on Australia to protect privacy is the International Covenant on Civil and Political Rights 1966 (ICCPR 1966), Article 17 of which requires privacy protection. While this has no direct effect in Australian domestic law, Australia is one of the few countries in the Asia-Pacific to have also acceded to the Covenant's First Optional Protocol allowing for individual complaints ('communications') to the UN Human Rights Committee (UNHRC). So the first complaint made against Australia under the ICCPR was on a privacy issue under Article 17 (*Toonen's Case*, 1994). The UNHRC held that adult consensual sex was within

the meaning of 'privacy'. The Tasmanian legislation meant it was not properly protected, and Australia was in breach of the ICCPR. Although countries cannot be compelled to implement UNHRC findings, the Federal Labor Government subsequently legislated, relying on its constitutional power over foreign affairs, to make the Tasmanian legislation ineffective. *Toonen's Case* shows that the protection of privacy in Australia through international law, while very limited, is possible.

### **The Australian Legal Context – Legislative Powers to Protect Privacy**

As a result of these limits in Australia's constitution, common law rights and international obligations, Australian law's protection of privacy has principally involved legislation, or attempts to legislate. In a federation with nine jurisdictions, the question of which Parliaments have the constitutional power to legislate to invade or protect privacy is important. The Australian Federal Constitution gives the States the residual powers to legislate where there is no specific head of Federal power, and there is none in relation to privacy. The Federal government has wide constitutional powers to legislate in relation to many areas especially telecommunication, corporations, and foreign affairs. It has relied on these heads of power to legislate generally in relation to privacy in the credit industry (1991) and the private sector generally (2000). Some States have also legislated in relation to surveillance, health information and other privacy issues affecting private sector bodies located in their jurisdiction, but can do so where these laws are capable of operating concurrently with the federal legislation. These potential clashes in legislative competence have not yet become an issue in Australia.

In recent decades governments have rarely controlled the upper houses of Australian Parliaments, due to the electoral successes of minor parties. This political fact has been very significant. It has given civil society organisations opportunities to defeat or modify government proposals, and helps explain their active role. The federal Privacy Act, its extension to the private sector, the NSW legislation and the federal data matching legislation have all undergone major modifications as a result. In NSW the government's attempt to abolish the Privacy Commissioner was defeated by the upper house in response to a NGO campaign.

### **The Very Slow Rise of Information Privacy Legislation**

Privacy as a public issue in Australia is usually traced to a series of radio lectures by Professor Cowen, published later as *The Private Man* (Cowen 1969). Throughout the 1970s and 1980s many bills to protect privacy in various ways were introduced into Australian parliaments (see Jackson 2001), but

except in New South Wales (and some unimportant credit reporting laws elsewhere) they all failed to be enacted.

The Privacy Committee of New South Wales (Australia's largest State) appeared to be innovative when established in 1975, the third permanent privacy protection body in the world, following Sweden and the Land of Hesse, Germany. It was enacted after recommendations in a law reform report (Morison, 1973). From 1975 to 1999 the Privacy Committee Act 1975 empowered the Privacy Committee to act as a 'privacy ombudsman', which could investigate any alleged invasions of privacy in the public or private sectors. It had strong powers, which it never used, to conduct such investigations and then to attempt to conciliate, and to make recommendations. The Act did not contain any definition of privacy, nor any information privacy principles, nor any enforceable rights or penalties. The Committee consisted of 12 statutory appointees largely independent of government, but dependent upon it for staffing etc. Over its nearly 25 years of existence the Committee conciliated numerous complaints, and influenced NSW legislation (particularly concerning workplace surveillance) and government proposals to be less privacy-invasive (see NSWPC Annual Reports, 1975–99). It had a high public profile in the late 1970s and played a significant role in raising elite and public awareness of privacy issues, but left a limited legacy. It failed to publish any useful details of its complaint resolutions, so the instructional value of its long history was lost. For some years it had a perverse policy of opposing enforceable privacy legislation. The Committee's 'Voluntary Agreement' with the credit industry in 1976 gave individuals a non-statutory right to access and correct their credit bureaux files, and was the basis of credit reporting practices until the Federal legislation of 1991. It played a courageous role in opposing the Australia Card in 1986–1987. But the NSW Privacy Committee was a dead end, emulated briefly in Queensland and by an irrelevant non-statutory committee in another State.

Enforceable rights of correction of records of personal information held by federal agencies were included in the Federal Freedom of Information Act (FOI) 1982, in advance of general privacy legislation. They then became a standard feature of FOI Acts in every Australian jurisdiction, even those that still have no general information privacy laws. Privacy Commissioners have usually left access and correction complaints to be resolved by the FOI system.

The Australian Law Reform Commission (ALRC), chaired by Justice Michael Kirby, received in 1976 a reference on the protection of privacy, as a result of an incoming government's election platform. In 1978 Kirby was also appointed as the Chair of the expert group asked to make recommendations on privacy to the OECD, which resulted in the 1980 OECD Privacy Guidelines (OECD 1980). The ALRC's report on *Privacy* (ALRC 1983) took seven years to produce but in the end only recommended non-binding OECD-influenced

Information Privacy Principles for the Federal public sector. By 1983 this approach had already been overtaken by enforceable privacy laws in many European countries, and was to a large extent a wasted opportunity. Politics had to perfect the ALRC's incomplete solution.

Australia symbolically agreed on New Year's Day 1984 to 'adhere' to the OECD Privacy Guidelines (OECD 1980), but the Federal government made no moves to introduce privacy legislation. In 1985 the Hawke/Keating Labor Government introduced its Australia Card proposal, and the Privacy Bill 1986, which like the ALRC's proposed Bill did not include any enforceable provisions, was introduced to Parliament as part of the 'package'. As we have seen, the defeat of the Australia Card proposal in 1987 resulted in a political compromise. The opposition parties, supported by consumer and advocacy organisations, agreed to passage of legislation for a strengthened TFN surveillance system, which the government promised would only be used to stop tax evasion. They did so on the basis that it was 'balanced' by the simultaneous passage of the Privacy Act 1988, based in part on the ALRC's recommendations, but which would now include *enforceable* information privacy rights stated in 11 Information Privacy Principles and a Federal Privacy Commissioner to enforce them. Australia's first enforceable privacy legislation thus resulted from hard-fought mass campaigns against surveillance, followed by elite negotiations over a compromise.

### **Privacy Principles – Many Laws, Similar Content**

So Australia obtained its first information privacy law, the federal Privacy Act 1988, with 11 Information Privacy Principles at its core, and applying only to the federal public sector and that of the Australian Capital Territory. It took another decade before NSW enacted the first similar State legislation covering its public sector (1998), followed by Victoria (2000), the Northern Territory (2002), and Tasmania (2006), and in a Bill introduced in Western Australia (2007).

What rights do these Acts create, and are they enforced? The content of the Information Privacy Principles (IPPs) is not very surprising, particularly as most can be traced to the OECD Guidelines, with some later influences from the EU Directive. There is as yet such a scarcity of authoritative interpretation by Courts, Tribunals or Privacy Commissioners that the interpretation of many of the key provisions of all Acts is speculative. The description below is relevant to the IPPs in all seven jurisdictions with information privacy laws except where major variations by jurisdiction are noted.

### **Key Terms**

All of the Acts apply to 'personal information', which means information or an opinion about an individual whose identity is apparent, or can reasonably

be ascertained, from the information or opinion itself, or with other information that can be expected to be used in combination with it. Most uses of information about a person which affect privacy will be caught by such definitions. However, they will not catch uses of data which are sufficient to allow an organisation to interact with an individual in a personalised manner even though they do not know the person's identity, such as telephone numbers and Internet Protocol addresses (which may be correlated with consumer behaviour) (Greenleaf 1996).

When a university lecturer disclosed personal information about a student to another university without following the correct procedures, it was not in breach of the legislation because the information about the student was only ever held in the mind of the lecturer, and had not been written down (*FM v Macquarie Case*, 2005). All Australian legislation requires that personal information must have entered into a 'record' of an organisation before the law applies. Information only ever held in the minds of employees of a business, or a public servant, falls outside the Acts. However, once the information has entered a record, visual or verbal disclosures may constitute breaches.

All the Acts exclude information contained in a 'generally available publication' (or some similar expression) such as a newspaper, book or public register. This does not, however, exempt the databases or other records from which the 'generally available publication' is derived, and the question then becomes whether it is an allowable use of the information in the database to include it in a generally available publication. For example, an agency may hold a database of adopted children, but this does not mean it could publish a book listing such children.

### **Collection Limitations**

Information may only be collected for purposes related to the objective functions of organisations, but within this relatively weak limit there is no requirement that the purpose be socially justified in some way. There is no provision for Privacy Commissioners or anyone else to require privacy impact assessments (PIAs) before systems involving particularly sensitive collection and use are built. Collection must be of the minimum information necessary for the purpose of collection, and by fair and lawful means. An additional limit is the Anonymity Principle found in all State and Territory laws (except that of NSW), which requires that individuals be given the option of anonymity in a transaction wherever it is lawful and reasonable to do so. This potentially radical principle remains untested, but could be used, for example, to attack the development of tollways or road tunnels which do not provide any option for payment by cash or some other method preserving anonymity.

Notices must be given to the individual on collection from him or her (and in some Acts even where the information is collected from a third party), specifying purpose, likely disclosures, and means of access and correction. These notices have done more than anything else to make Australians aware that they do have some privacy rights, because they see 'Privacy Notice' on so many forms, even though the content is often prolix, in fine print, and unread.

### **'Finality' Limits on Use or Disclosure**

All Acts allow only four means of using or disclosing personal information beyond the primary purpose for which it was collected. The first is consent. Australian laws generally allow implied consent in addition to express consent, with the likely result that in some cases a failure to opt out will be taken to be consent. Second is typically that the use is related to the purpose of collection and is such that the individual would 'reasonably expect' the use. Third is where it is necessary to avoid harm to the individual or another, or (generally) for various purposes of prevention or detection of crime or other wrongdoing. Finally, Australian legislation generally has an exemption where 'the use or disclosure is required or authorised by or under law' including common law principles. This final exemption means that any data controller can, if it wishes, comply with any legislatively authorised request for information. The extent of legal data flows between organisations is impossible to calculate. This exemption has been rightly criticised by Europeans for being unacceptably broad (A29 Working Party, 2001). In the private sector law there is an exception, similar to the one found in EU law, which allows direct marketing by an organisation to its customers, provided it gives them a means to opt out of further communications.

The corollary of notices on collection in creating public awareness is refusals to disclose information 'Because Of The Privacy Act'. 'BOTPA' is a mantra that is now recited by desk and telephone clerks whenever you visit or ring an agency or company and request details from (or actions in relation to) your own files, and even more so if you ever ask for any information about another person. In the former case you must go through a sometimes elaborate and formal process of answering a number of questions to establish your identity. In the latter, people are becoming familiar with the irritation of being unable to obtain information about spouses, children or parents (ostensibly BOTPA) where it is perfectly reasonable for them to do so. Some noted BOTPAs were claimed in justification of the lack of anti-theft cameras in aircraft luggage holds; in the refusal to disclose details of \$300 million of unlawful payments in Iraq; in refusals to release details of the roles of military personnel in Australia's worst military disaster in a decade; and in an attempt to make a journalistic briefing about abuse of a departmental client

confidential, where the effect was to cover up the malperformance of the Department and its contractors (APF 2007a).

Access and correction rights, already available in the public sectors through FOI laws, only became common in the private sector after 2001. They are of course central to any IPPs. Their operation in Australian FOI and privacy laws is similar to other countries (Waters and Greenleaf 2005).

With theft of personal data now becoming a far more serious problem, the security principle is a particularly valuable right against data controllers who may negligently allow personal data to be stolen, particularly as substantial claims for compensation may be available, such as the A\$25,000 settlement discussed below (Waters and Greenleaf 2004). Some Acts add a deletion requirement to 'take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed' (from the private sector law).

### **Data Exports and Australian Consumers**

In August 2005 a television documentary revealed that information on Australians was being sold on the Indian black market after being outsourced by the local agent of an Australian telecommunications company to a call centre provider in India. Its staff had been collecting excessive personal details (such as passport numbers) without authority of their client, then selling them and other details ('Four Corners', 2005). The Privacy Commissioner promptly launched an 'own motion' investigation of both Australian companies. What can she do when personal data of Australians is exported and misused in countries with no privacy laws?

Australia prohibits transfers of personal information to any recipient in a foreign country unless one of six conditions apply. The six conditions are so broad that only a very disorganised business could fail to comply with them. They include obtaining express or implied consent to the transfer, or taking reasonable steps to ensure that the data is held, used and disclosed consistently with the IPPs. However if the apparently compliant Indian outsourcer turns out to be a rogue or to have inadequate security (even over its own staff), then the Australian consumer has no remedy against the Australian data controller under the Australian legislation. Little wonder that there are as yet no reported breaches of IPP 9. This is the only personal data export restriction law in force outside Europe, but it is weak protection.

### **Limited Effectiveness of the Federal Public Sector Law**

The Federal Privacy Act 1988 has been in operation for nearly 20 years, so there should be more evidence on which to assess its effectiveness than for more recent State and Territory Acts.

The Privacy Commissioner's role has significant limitations. The Commissioner is an independent statutory office, but is appointed by the executive government, not Parliament, for a renewable five-year term. He (or she in two of the four appointments to date) is dependent on the executive for a budget, and has no security of tenure in any position after the completion of his or her term as Commissioner, so it is a conditional independence. The Act has limited scope because it does not recognise any general notion of 'breach of privacy', but only deals with breaches of the IPPs discussed above. Outside the investigation of individual complaints, the Commissioner's powers are limited. He has powers to audit federal agencies' compliance with the IPPs, but this has stopped due to funding constraints. He cannot require 'Privacy impact assessments' (PIAs) for new information systems. However, he has a potentially significant 'watchdog' function of making statements on the privacy implications of proposed legislation or technologies including where their implications go beyond the IPPs. The Commissioner's office does make public submissions, usually to Parliamentary committees or in response to agency requests for submissions, and participates in many inter-departmental committees. In doing so, his views do not usually have special status or weight compared with those in other submissions. He does not have any power to sit in judgment on government proposals or actions, unless they become the subject of a complaint under the Act.

The essence of this Act is that enforcement of the IPPs is largely complaint-driven, as is the case with all Australian data protection legislation. The Act requires individual complaints of IPP breaches before enforcement action can take place. Enforcement of the Act is largely reactive: there are few if any means by which pro-active action is taken by the Commissioner to ensure it is observed.

Of over 1000 complaints investigated per year, about 17 per cent relate to the public sector (OPC 2004). Wide powers to investigate individual complaints, are rarely, if ever, used. Complainants are first required to attempt to resolve the complaint with the data controller. Most complaints are handled by mediation. The Commissioner has powers to make 'determinations' awarding compensatory damages or requiring apologies or remedial acts, if mediation fails, but has only done so four times against public sector bodies in 19 years. Almost all complaints are settled by mediation or otherwise disposed of. This does not indicate that most complainants are satisfied with the Commissioner's mediations, because he dismisses complaints where he is satisfied that a business or agency has dealt satisfactorily with a complaint, irrespective of what the complainant thinks.

The system is biased against complainants in other ways. There is no right of appeal to a Court against the Commissioner's determination. However, if a determination is unfavourable to a data controller, it can in effect appeal to the

Court because a complainant must go to Court to enforce the determination. The data controller can simply refuse to pay or comply and then have the whole matter heard again by the Court (Greenleaf 2001). The only appeal right complainants have is against the *amount* of any compensation ordered against a public sector body by a determination. The Commissioner has never ordered compensatory damages except by consent of the data controller.

Mr Rummery was a whistleblower whose personal information had been improperly disclosed by his employer to corruption investigators. The Commissioner considered that, while the agency was entitled to disclose relevant personal information about him to the investigator, this did not give them 'open season' and they had gone too far. But he then refused to award any compensation for the distress that had resulted. In the only case where a complainant has appealed against the Commissioner's refusal to award compensation, Rummery was awarded A\$8000 compensation (*Rummery Case*, 2004). Complainants with his tenacity are rare.

Of the approximately 200 public sector complaints in 2003–2004, investigations found a possible breach of the IPPs in 38 per cent (75). Over half the complaints were about agencies disclosing personal information, and the rest were about data security, failure to check accuracy, and collection practices. One indicator of successful operation of a complaints-based system is that it can demonstrate that individual complainants get the remedies that the legislation provides in theory. What happened in the 38 per cent of cases investigated where breaches were found? Unfortunately, the OPC did not publish any systematic information about remedies granted (but this has now improved), so we can only generalise from the few complaint summaries that are published. Since 2003, the Commissioner has published an annual average of 15 brief anonymised summaries of significant complaints which have been resolved without a determination, as well as the few determinations. Of the 19 complaint summaries published in 2004, only three related to agencies. Two of these were simply illustrative examples of where the Commissioner declined to investigate. In the one remaining case the agency's employee did disclose to the complainant's ex-partner that the complainant was to receive money from a court settlement, allowing the ex-partner to obtain a court order restraining the complainant from accessing that money. Because the complainant wished to pursue other action against the agency in the Courts, the Commissioner ceased investigation. 2003–2004 is a typical year: there is no substantial evidence that the Commissioner enforces the Act against Commonwealth agencies in any way that produces remedies for complainants. This non-reporting makes the office less accountable, and squanders the potential deterrent effect of the Act. Other Asia-Pacific Privacy Commissioners are also opaque in their enforcement practices (Greenleaf 2003), though perhaps not to this extent.

There are some innovative enforcement aspects of the Act, but they have been little used. First, the Commissioner can conduct ‘own motion investigations’, which do not require an individual complainant, but any recommendations made are not enforceable by determinations. Although 42 such matters brought to her attention by media reports or other sources were investigated in 2004–2005, few details of these investigations or their outcomes were published. Their potential as an avenue for public critique of system failures is lost. Second, individuals can seek a court injunction against breaches of the data protection principles, or threatened breaches (s. 98), but otherwise cannot enforce their rights in the Courts. The injunction power has only once been used, in a dispute between two commercial organisations. In practice, complainants go to the Privacy Commissioner, not a court, in part because of the risk of substantial legal costs being awarded against an unsuccessful litigant. The Commissioner can also seek injunctions from a court but has never done so. Third, NGOs, lawyers and others are allowed to make representative complaints on behalf of a class of complainants, and these can result in enforceable determinations (including damages) in favour of all members of the class. In the only published instance of this occurring, a consumer NGO represented the class of complainants against a private company (TICA determinations, 2005, discussed later).

### **Are the State and Territory Public Sector Laws Any Better?**

The experience of New South Wales, the largest State, shows that many factors can make privacy protection precarious, from exemptions to politics to costs orders.

NSW was the first State to legislate for enforceable privacy rights in a State public sector (Privacy and Personal Information Protection Act 1998). The Act contains reasonably strong IPPs and sufficient remedies including compensation up to A\$40,000. The problem with the Act is that it is riddled with exemptions and exceptions for particular agencies and practices, and contains provisions which allow Ministers or the Commissioner to create further exceptions with very little control on whether they are consistent with the purposes of the legislation (Greenleaf 1999). The NSW Privacy Commissioner was highly critical of this in a submission on a review of the Act (Johnston 2005, 2005a):

The ease with which the privacy protection afforded by Parliament in the PPIP Act may be overridden by the government of the day through subordinate legislation and other statutory instruments has ensured that the level of privacy protection is a moveable feast, but only moving in one direction – away from the highest standards of privacy protection.

The holes in the Act are so complex that the Privacy NSW website contains details of the 'matrix of exemptions' in the Act. Its effect is as much to legitimate surveillance and mollify public fears as to protect privacy.

Australian Privacy Commissioners have rarely come into direct conflict with governments. The first NSW Commissioner, Chris Puplick, was the exception, becoming involved in public dispute with a government minister. He resigned in 2003 after strong criticism by the NSW premier. The government then unsuccessfully attempted to abolish the office of Privacy Commissioner (Greenleaf and Waters 2003). It then reduced the staff of Privacy NSW by one third and refused to appoint a new Commissioner for nearly five years, effectively removing the office from public debate until 2008. The fragile independence of Australian Privacy Commissioners was never more apparent.

Despite this the Act continued to work to some extent because complainants have an alternative route to dispute resolution. They may seek internal review of their complaint by the agency concerned, and then appeal to the Administrative Decisions Tribunal if necessary. An average of three privacy cases per month have continued to be decided by the Tribunal since 2003. However, in recent cases the Tribunal's appeals division has started to require complainants to pay the costs of the agency in appeals where the complainant loses, even when the appeal has been brought by an agency. This may have a 'chilling effect' on complainants because of the uncontrollable risks of costs (Waters and Paramaguru 2007).

In 2000 Victoria enacted Australia's strongest public sector privacy legislation, the Information Privacy Act 2000 (Greenleaf 2000b). The first Privacy Commissioner, Paul Chadwick, was a former journalist with a reputation for independence. The Act's principles are based on those in the private sector Act. It provides for an extensive range of remedies including compensatory damages, with mediation by the Commissioner followed by the right of complainants to seek enforceable remedies from the Victorian Civil and Administrative Tribunal (VCAT). Although the complaints functions have only been operative since 2004 substantial compensation does result. For example a A\$25,000 settlement resulted when a government agency disclosed a woman's new address to her estranged partner despite the agency's file noting that she was 'at risk'. Her premises were broken into and vandalised the same day, and she was forced to relocate.

Other than in these two States, data protection in Australia's public sector is slow to develop, incomplete, and inconsistent. There has never been a push for national uniformity, although all State and Territory jurisdictions do provide access and correction rights to personal information held in government documents, as part of their Freedom of Information legislation. The Northern Territory has enforceable IPPs based on the private sector Act, and a

Commissioner (Information Act 2002). The Australian Capital Territory (ACT) applies the Federal legislation to its public sector. Tasmania's anti-diluvian legislation includes IPPs but no means of enforcement beyond investigation and mediation by the Ombudsman (Personal Information Protection Act 2004). Western Australia has introduced a Bill which is similar to the Victorian Act but allows the State's Ombudsman to be appointed as Privacy Commissioner (Information Privacy Bill 2007). South Australia and Queensland have non-legislative, non-enforceable and insignificant administrative instructions similar to IPPs applying to their public sectors.

Comparison of the enforcement of the federal, NSW and Victorian legislation suggests that effective privacy law enforcement in Australia might be better delivered by a quasi-judicial tribunal such as in NSW and Victoria, rather than by a Privacy Commissioner, although introduction of a right of appeal against the Commissioner's decisions might substantially change the federal system.

Australia's privacy laws have not forced significant information systems to be shut down or redesigned, at least to public knowledge. Yet they do give either Privacy Commissioners or administrative tribunals enforcement powers in individual complaints, including powers to award damages, that are unusual in many other countries. In a common law country where privacy protection is not founded on broad principles but on technical legislation, individual cases are potentially very significant. Their cumulative effect as a deterrent to privacy invasion could be very substantial. However, this potential has largely been squandered in Australia. There are too many impediments to complainants pursuing their rights in some jurisdictions. Privacy Commissioners have also failed to publish sufficient information to create a realisation of the potential of Australia's privacy laws.

### **The Rocky Road to Private Sector Legislation**

Why did it take 17 years from when Australia acceded to the OECD Guidelines in 1984, until the Federal Privacy Act 1988 was extended to apply to the whole of Australia's private sector in 2001 (Privacy Amendment (Private Sector) Act 2000)?

By the early 1990s there was some piecemeal private sector coverage, as already discussed: the NSW Privacy Committee had 'ombudsman' powers to investigate complaints against businesses in NSW; use of tax file numbers by businesses was regulated; and credit reporting was strictly regulated. Pressure grew through the first half of the 1990s for further private sector protections, influenced in part by increasing electronic privacy issues, and in part by the imminent EU Privacy Directive. In 1996 Liberal Prime Minister John Howard scrapped proposals by his Attorney-General for private sector privacy legislation

(A-G Discussion paper 1996), in favour of voluntary self-regulation, due to pressure from some sections of the business community and a general antipathy to regulation. He requested the States and Territories to follow suit, but Victoria continued to plan legislation. Privacy and consumer groups continued to campaign for legislation (Greenleaf 1997).

The Privacy Commissioner proposed a single national self-regulatory privacy code (OPC 1997). Consumer and privacy groups boycotted any discussions of voluntary self-regulation, but agreed to discuss the content of privacy principles. The Commissioner convened discussions between business and consumer representatives and then published the set of 'National Privacy Principles' (NPPs) she favoured (OFPC 1998). They were criticised by privacy advocates (Greenleaf 1998) as representing neither a high standard nor a consensus, but business groups were not overtly critical. Three years later, these NPPs, essentially unchanged, became the core of the private sector legislation. They were not designed for that purpose, and were never debated in Parliament, illustrating how accidents of history can shape law.

Privacy and consumer advocates continued to boycott discussion of voluntary methods of enforcement of the NPPs, and business groups lost interest in turning them into Codes of Practice. Meanwhile, perceptions that the European Union's Privacy Directive, in force since 1998, could lead to data export restrictions between Europe and Australia continued to mount. Whether self-regulation could satisfy these requirements was contentious. Privacy advocates found a ready appetite in media organisations for stories on these lines. The Victoria Labor Government offered to drop its proposed private sector coverage if the Federal Government acted instead (Greenleaf 1999).

In January 1999 the Federal Government abandoned its self-regulatory approach in favour of so-called 'light-touch' legislation including provision for co-regulation via industry codes of conduct. It admitted this was because key industry groups had changed their mind and now wanted legislation to achieve national consistency and certainty. The resulting legislation (Privacy Amendment (Private Sector) Bill 2000) was strengthened somewhat during the political process, but too little to satisfy the Bill's critics who claimed it would not deliver meaningful privacy protection (Greenleaf 2000, 2000a). The self-regulation road of 1997–99 had been turned into a dead end. The causes were complex, but it probably would not have occurred without a decade-long campaign by privacy groups, or without the belief that there were trade imperatives because of the EU Directive.

What rights did the 'private sector amendments' create? In most respects the NPPs are similar to the public sector IPPs that preceded them, but they included innovations that stemmed from the business-advocate discussions convened by the Privacy Commissioner. These included the 'anonymity principle', the principle limiting re-use of identifiers, the deletion principle, and

the limits on data exports, all previously discussed. These additional principles have subsequently been taken up in most post-2001 State and Territory public sector laws.

### **Is the Private Sector Legislation Effective?**

About 80 per cent of all complaints to the Commissioner are against the private sector (OPC 2005: Annual Report 2004–05). The private sector provisions of the Federal Act are enforced in much the same way as the public sector provisions, discussed earlier.

Tenants Unions made a representative complaint on behalf of their members against TICA, a database about tenants consulted by real estate agents (TICA determinations, 2005). They persuaded an initially reluctant Commissioner to make determinations that TICA had breached the NPPs in numerous ways, including by charging tenants merely to make a request to access their tenancy record; by charging excessive amounts for access; by failing to ensure data quality standards; by having excessively general reporting categories; by failing to advise tenants when they were listed; and by failing to destroy or de-identify information no longer needed. TICA was required to make systemic changes to its practices, to the benefit of many thousands of tenants.

In the six years the private sector provisions have operated, this is the only enforceable order (determination) made against a private sector body. There have also been occasional significant mediated disputes, notably when the Commissioner convinced Veda Advantage to delete 65,000 debts listed by a telecommunications company in liquidation, since it could no longer prove their validity. What happens to the rest of the thousand or so complaints received annually against the private sector? About 60 per cent are closed without investigation. In only about 5 per cent of cases does the Commissioner reach even a provisional view that there might be a breach of NPP, but subsequently ceases investigation after concluding that the respondent has dealt adequately with it, possibly after conciliation. No details of the outcomes of these conciliations were provided except that the resolutions include 'provision of access to records, correction of records, apologies, change to systems, [and] amounts of compensation ranging from less than \$500 to \$20,000' (OPC Annual Report 2004–2005). Of the 22 complaint summaries published by the Commissioner in 2004–2005 (OPC complaints 2004–05), none involved any financial compensation, let alone such a significant sum as \$20,000. They are mainly variations on how complaints are dismissed, and none involve significant systemic changes. This is a substantial failure of accountability.

The Federal Privacy Commissioner states that most business organisations consider that 'the overall level of compliance is good and the Office's

approach is working well', but notes that in contrast, 'the perceived lack of enforcement mechanisms in the Privacy Act especially in relation to determination enforcement is a matter of strong concern amongst the advocacy and consumer groups' (OPC Review 2005). This is an unduly self-satisfied conclusion. The Commissioner's own Review (2005, Appendix 14) summarises the results of a survey of satisfaction levels of 100 complainants and 41 respondents. On every criterion of satisfaction measured (timeliness, impartiality, process information, communication of reasons, satisfaction with service and satisfaction with outcomes) complainants were far less satisfied than respondents. In some cases, the disparities in satisfaction were large: only 43 per cent of complainants were satisfied with outcomes, but 86 per cent of respondents were satisfied. In addition, 41 per cent of complainants considered the service poor, and 56 per cent did not think they had been dealt with fairly. Unless the dissatisfaction of complainants is quite unjustified, these results suggest that the complaints process itself may be demonstrating to respondents that they have little to fear from the Privacy Commissioner. The Commissioner's failure to publish sufficient details of complaint outcomes reinforces such a belief.

The emphasis in this and preceding sections on complaint outcomes, compensation and reported complaints is perhaps typical of the empirical and inductive common law approach. It reflects an approach to privacy protection based on the technical minutiae of positive law. However, that is the only approach possible in the absence of any theoretical underpinnings of principle, such as Germany's 'informational self-determination' doctrine, strongly upheld in that country's courts, yet conspicuously lacking any equivalent in Australian law.

## ROLE OF PUBLIC OPINION

Privacy is usually an elite concern in Australia as a public issue, but is capable of quickly grabbing public attention and widespread media coverage. This ensures that policymakers do not ignore privacy issues, but instead devote resources to managing them.

### **Public and Organisational Attitudes to Privacy Protection**

Public concern in Australia for privacy and data protection interests is generally high, at least in the abstract, according to survey data. There would also appear to be widespread public support in Australia for legal safeguards of these interests (Morgan 2004 referring also to 1995 and 2001 surveys). However, community knowledge of existing safeguards appears to be poor. Although knowledge that federal privacy laws exist has risen to 60 per cent of

respondents, only 34 per cent were aware that the Federal Privacy Commissioner existed (Morgan 2004).

Australian organisations in both the public sector (Morgan 2001) and private sectors (Morgan 2001a) seem generally to regard public concern about privacy issues as legitimate and as an important factor to take into account when dealing with information about their customers and clients. They seem to be generally supportive of existing privacy laws, though there are some gaps in knowledge of how these laws work, particularly with respect to the business community.

### **Elite Involvement in Privacy Issues**

Elite participants interested in privacy issues are well served in Australia, in the sense that it is possible for individuals to have an impact on policy development, and there are NGO structures to facilitate their doing so. Although it is a big country, Australia has a relatively small civil society and most significant meetings are held in Canberra or Sydney. Attendance is often possible for the policy elites residing in those cities. Ministers, Opposition spokesmen, Privacy Commissioners and other policymakers are relatively accessible in comparison with the policy makers of Washington or Whitehall.

Consumer groups, including specialist telecommunications, credit and medical consumer groups, as well as the broad-based Australian Consumers Association, take a continuing interest in privacy issues. Some general civil liberties organisations also do. Of these, Electronic Frontiers Australia (EFA) has been the most prominent (EFA 2004), providing continuous detailed input into privacy debates and lobbying.

Since 1987 the Australian Privacy Foundation (APF 2007), formed to oppose the Australia Card, together with its members wearing other hats, have been the most consistent and effective privacy advocates in Australia, though still rarely gaining the policy changes they seek. 'Ex officials' including two former deputy Privacy Commissioners have been key APF board members or Chairs since its inception. The APF's key achievements since the defeat of the Australia Card include leading the opposition to 'positive reporting' which resulted in the credit reporting legislation (1990), leading the boycott against self-regulation discussions (1997), and its role in opposing the 'Access Card' (2007). The APF also influenced the content of the NPPs (1998), obtained Opposition support for successful improvements to the Federal private sector legislation (2000), obtained upper house support to stop the NSW government abolishing its Privacy Commissioner in 2004, and derailed Federal plans to convert the census into an identified longitudinal database in 2005 (APF 2005). The Australian Privacy Charter launched in 1993 is a restatement of privacy principles in a stronger and simpler form than the Privacy Act's IPPs.

It was developed outside the APF but led and drafted by APF participants. It had a strong influence on the NPPs, and was subsequently adopted by the APF as its 'policy constitution'.

The APF also launched the Australian Big Brother Awards (the 'Orwells') in 2003, influenced by Privacy International. Winners of the premier 'Lifetime Menace Award' for long records of profound disregard for privacy have included a Federal Attorney-General for sponsoring anti-privacy legislation, and the NSW Government for its failure to appoint a new Privacy Commissioner. This irreverent approach to public officials sits well in the Australian psyche, and has obtained good media coverage.

Organisations of professionals have not had a continuing input into the development of privacy laws, with the exception of the Australian Computer Society (ACS), the largest organisation of computing professionals. Since the early 1970s ACS has consistently supported the development and strengthening of information privacy laws. In part this can be explained by an overlap of key activists with the APF, but nevertheless the whole professional body has been willing to appear in the pro-privacy camp.

Business groups are almost always better resourced than NGOs, and key groups have much more ready access to ministers than do NGOs. The Melbourne-based employer group, ACCI, was particularly influential in getting the Federal Liberal Government to first oppose private sector legislation and then, two years later, to adopt it in a 'light handed' version. However, business groups have often not been as adept in using the press on key privacy issues as have NGOs, and they do not uniformly achieve their objectives. A privacy issue is never a hopeless cause in Australia, nor is victory assumed.

A small group of key business representatives, and a core group of privacy advocates have remained relatively stable for at least 15 years, while government representatives have changed far more regularly. This has often facilitated effective communication of positions, with compromises on either side, particularly in relation to legislative developments. For example, in the 2005 review of the Privacy Act, businesses and privacy advocates were able to agree that requiring opt-out notices in all direct marketing communications was a sensible change to existing law, though it did not represent the ideal position of either side (OPC Review 2005).

## **Public Opinion's Influence on Privacy Developments**

By the mid-1970s there was considerable media attention to privacy issues throughout Australia, arising from fear of computers (Australian businesses being relatively 'early adopters'), from notorious abuses of 'Special Branch' police political surveillance, and from widespread fears of the actions of credit bureaux. Although the Australian Law Reform Commission privacy

investigations from 1976 helped keep the issue alive, privacy was less prominent as a public issue throughout the early 1980s. The 'Australia Card' defeat in 1987 gave privacy credibility as a national issue, and it has remained a significant public issue since then, but there has been no equivalent extraordinary issue to galvanise opinion. The result has been (in the view of privacy advocates) that Australians have suffered the fate of the boiling frog: that each incremental increase in surveillance has gone largely unnoticed (the tax file numbers and 'parallel matching', the extensions of financial surveillance, the spread of CCTV etc) and largely unopposed because the cumulative impact is not apparent.

## LOCAL CULTURE AND TRADITIONS VS INTERNATIONAL INFLUENCES

### **National Culture and Traditions**

Australia's self identification as 'The Lucky Country' (Horne 1966) is opposite in relation to privacy. There has been no wartime occupation or an authoritarian regime from which to recover and no terrorist actions as yet within the country to prompt (or justify) major changes in mass surveillance. Australian privacy protection has therefore as yet only needed a story of incremental wins balanced against losses, not a cultural revolution. It is a complex balance sheet, with much scope for disagreement about what type of balance has been reached.

Our legal culture's British inheritance has not served us well in creating foundations for privacy protection. From Britain Australia inherited no common law right of privacy, and no constitutional bill of rights as a basis for privacy protection, and nor does it have major treaty obligations. Whereas Britain has now imported the last two from the Continent, Australia languishes with neither and lacks any underlying principle such as 'informational self-determination' on which privacy protection can be anchored. If the immediate future is one of increasing encroachments on privacy and other civil liberties, where justifications are framed in terms of increasing risks from terrorism, Australia's national culture and legal traditions have few tools with which to resist and shape such encroachments.

### **International Privacy Developments and their Influence**

Despite Australians' minimal obligations under international privacy agreements (discussed earlier), Australia has had a significant role in the development of those standards, and its domestic legislation has in fact been

influenced by those international developments. Three agreements have had key influences in each of the last three decades.

The OECD Privacy Guidelines (1981) were adopted by Australia in 1984. An Australian, Justice Michael Kirby, chaired the expert group that drafted them. There is no method of enforcing the Guidelines, either by OECD members or by individuals, and no external assessment of whether they have ever been implemented (though their terms require implementing legislation). Australia implemented them for its Federal public sector in 1988, but took until 2001 to implement them in the private sector, and has put no pressure on State public sectors to implement them. The OECD Guidelines clearly influenced the IPPs in the ALRC Privacy Report (1983), and via that route the public sector IPPs in the Privacy Act 1988 which mirrored them fairly faithfully. Since then there has been a 'ripple down' influence through all Australian privacy laws, which all probably satisfy the OECD Guidelines' reasonably weak requirements. Australia subsequently became a strong promoter of the OECD Guidelines as the 'only credible international standard' (Ford 2002) in the negotiations over the APEC Privacy Framework.

Throughout the 1990s, the EU Privacy Directive (1995) was a constant feature of elite debates and newspaper reportage in Australia because of the success with which privacy advocates played the 'adequacy card'. The content of the Directive had some influence on the federal Privacy Commissioner's NPPs in relation to 'sensitive' information and inclusion of a data export provision. However, the European Union is not yet satisfied that Australia's private sector privacy legislation is 'adequate' in European terms. Europe's data protection Commissioners are very critical of the Australian legislation (Article 29 Committee 2001), resulting in claims of unfairness and willful misunderstanding by Australia's federal government (as exemplified by Ford 2002). The EU commenced its formal assessment of the 'adequacy' of Australia's privacy laws in 2005 and (depending on the outcome) this may further increase hostility between Australia and Europe over data protection issues.

In the present decade, the international focus of Australian policy has turned to APEC (Asia-Pacific Economic Cooperation) and the development of the most recent international privacy instrument, the APEC Privacy Framework (2004). Australia had a significant influence on the development of the Framework, the first draft of which was by an Australian committee chair (Greenleaf 2003a). The principles in the APEC Privacy Framework are weaker than in Australia's existing laws and are at best an approximation of the OECD Guidelines (Greenleaf 2005). The APEC Framework was only completed in mid-2005 in relation to data export restrictions. Although the Australian government has expressed antipathy to judgments of its privacy laws by any other country (see Ford 2002), APEC did not reject the legitimacy

of data export restrictions and therefore set itself against EU notions of 'adequacy', contrary to the fears of some commentators (Greenleaf 2006). The final framework said virtually nothing on the subject and there is now little chance that APEC will develop into an anti-EU bloc (Greenleaf 2005).

Australia has therefore had 20 years' involvement in developing international privacy standards as an influential non-EU participant. Its chosen role has been to advocate privacy protection as a legitimate and unavoidable issue, but one that can be managed in the interests of business and government, rather than advocacy of privacy as a human right.

## WINNERS AND LOSERS

The broad trajectory of the development of privacy protection in Australia is one of steadily increasing surveillance, but the picture is not uniformly negative. Often these losses to privacy are accompanied by small gains in individual privacy rights and ability to exercise them. Increased surveillance and increased legislative protection have often occurred in tandem, as legislative 'packages'. It may well be that Australians are accepting more surveillance as part of the price of an information-based economy and to achieve an acceptable level of social control, but this is still accompanied by demands for mechanisms to control abuses. 'One step forward, two steps back' is the general trajectory.

Court decisions and complaints to Commissioners have played very little significant role in bringing about systemic changes to practices. Privacy Commissioners have delivered some justice to individual complainants. But even there their record has been very limited and their general failure to use their complaints experience as a method of deterrence and public education makes it questionable whether the expenditure of public monies has been worthwhile.

Australian privacy legislation leaves many consumers and citizens as major losers in many of their most important life roles. Unprincipled exemptions from the Federal Privacy Act are a major cause: as voters, political parties owe them no privacy; as employees, they are left to fragments of protection in industrial laws and varying State laws; as customers of the majority of businesses in the country (so called 'small' businesses) they have no privacy rights unless the business trades in personal information.

The negative privacy protections of inefficiency mean that Australians are still winners in not having a national ID card. 'Like the Australia Card' is still the kiss of death to any identification proposal in Australia, and is flatly asserted and denied by those on either side of an issue, usually with little grasp of what the Australia Card proposal involved.

## Information Flows and Constraints

The main gains in privacy protection in Australia stem from the simple fact that legislation exists. Both government agencies and private sector bodies are generally law abiding even in the absence of any effective sanctions or credible threat of sanctions, at least if the compliance costs are not too high. The potential for embarrassing media publicity is probably more potent than the featherweight sanctions employed by Privacy Commissioners.

In the private sector, observance of the law still keeps personal information by and large segregated into databases which reflect different industry sectors, and all consumers are winners in that. There have also not been radical changes in relation to private sector access to data from public sector registers. Data aggregators seek to break down both these barriers, but for the moment have not succeeded. In 2007, industry efforts re-commenced to remove the restraints found in the credit reporting and private sector legislation.

The flows of personal information from the private sector to the public sectors have expanded to a massive extent over the past 15 years, thanks to the various data matching schemes, and to the financial surveillance requirements. However, within the public sector, and from the private sector to the public sector, recent developments threaten to tear down barriers to information use and merger. All Australians in their capacity as citizens are in danger of losing their privacy. That must be the focus of an assessment of future prospects.

## PROSPECTS FOR THE FUTURE

The future of privacy always looks dangerous because there are always proposals on the horizon, or new systems in place, which look as though they pose great dangers of abuse. In hindsight we see that most proposals fail – with excessive privacy dangers sometimes a cause – and that many new systems are implemented more cautiously than we feared.

### The Political Ascendancy of Surveillance Post-2001

By 2007 the future for privacy in Australia looked more bleak than it had at any time since the Australia Card seemed a *fait accompli* almost two decades earlier. The prospect of a never-ending ‘war on terror’ has made everyone’s privacy a hostage to agendas which have little to do with genuine attempts to defeat terrorism, but which find it a convenient cover. There are many post-2001 developments in Australia which fall within this category. The ease with which such legislation could be passed in Australia is partly explained by the fact that although terrorist attacks have not yet occurred within Australia, there

have been significant terrorist attacks on Australians in Bali, Indonesia in 2002 and 2005. The Labor Federal Opposition during those years, and the Labor governments of most States and Territories, were cowed by the perceived danger of being labeled 'soft on terror', and even promised to pass proposed legislation before they saw the details. Repeatedly the Federal Liberal Party Government refused to release contentious legislation in bill form so as to enable informed public debate and used its majorities to rush it through both houses of Parliament.

The ease of passage of invasive legislation was caused by a drastic change in the political situation described in the opening of this paper, whereby the protection of privacy in Australia has always depended on limitations on political power in Australia. In particular, governments in Australia have rarely controlled the upper house of Parliament, and have therefore been forced to make political compromises to pass legislation. In July 2005 the Howard Liberal Party government obtained a slim majority in the Federal Senate. They then relentlessly pursued a radical agenda of political change in industrial law, education, social security and, not least, national security and surveillance. The political balance that formerly protected privacy was lost.

Telecommunications interception legislation was amended in 2004 to eliminate the requirement of judicial warrants for access to stored communications such as email, SMS and voice mail. This followed earlier amendments allowing security agencies to plant surveillance devices in computers and take other actions which would otherwise breach computer crime legislation.

New passports legislation in 2005 allows the Department of Foreign Affairs and Trade to develop an electronic passport, featuring a facial biometric and possibly other biometrics. The justification offered was mainly the demands of the USA for such passports if countries wished to retain visa-free status for their nationals.

New anti-terrorism laws contain provisions which are not confined to terrorism offences but are part of long-standing government wishes to give agencies extra powers, including federal police powers to give notice to produce information for 'other serious offences', extensions of optical surveillance, changes to the Financial Transaction Reports Act (discussed below), and extended powers of Customs officers (Anti-Terrorism Act (No 2) 2005; see APF 2005a).

Anti-money-laundering and counter-terrorism financing laws now require 63 categories of businesses to identify and monitor transactions and activities of their customers, extending to transactions as minor as phone or public transport smart cards. Critics argued that 'At least under the current scheme, most reporting is by supposedly well trained bank employees, but in future thousands more people, from casual jewellery store clerks to junior real estate managers, will be legally required to pass on judgments about their customers,

that could bring innocent individuals under official suspicion' (Anti Money-laundering and Counter-Terrorism Financing Act 2006; see APF 2005b). The APF identifies the AUSTRAC system as the central new surveillance system emerging in Australia which straddles the public and private sectors (APF 2005c):

[The] existing FTRA/AUSTRAC regime . . . has offended against privacy principles since its inception, and has progressively developed into a wholly disproportionate surveillance system, part of which involves secret files which can have the potential to blight innocent people's lives without any knowledge or recourse. The history of the FTRA . . . has been a classic example of 'function creep', with the original justification of fighting serious and organised crime having long since given way to routine use by agencies for other purposes, culminating last year in the granting of access to [social security and child support agencies].

In addition to developments under the anti-terrorism cloak, there are many public sector developments which involve an unprecedented degree of surveillance for Australia, including in the areas of health and transport systems. However, the development of a national identification system under the guise of a 'Health and Welfare Access Card' posed the greatest long-term threat to privacy interests.

### **'The Access Card' ID System – Another Near Miss**

Liberal Party Prime Minister John Howard put the issue of an ID card back on Australia's political agenda in the wake of the London bombings of July 2005, but it temporarily disappeared when it became clear that ID cards were not seen as related to this issue in the UK. It reappeared in April 2006 with the announcement that his government had rejected the idea of an ID card, but would introduce a 'Health and Welfare Access Card' instead, intended to replace up to 17 government benefit cards and to reduce fraud against the social security and medicare systems. It was proposed as a multi-function smart card, on part of which individuals would be able to store their own medical and other information. It was claimed that, while individuals would be free to use the card for any purpose they chose, no one outside the welfare and health benefits system would be able to demand its production.

Critics argued that the proposal was indistinguishable, other than for its greater technical sophistication, from the Australia Card proposals of 20 years earlier (Greenleaf 2007, 2007a, 2007b). The essential components of the proposal were a Register to contain photographs, signatures, location information and an ID number for each adult, and links to benefit agency systems; and a chip-based card which would contain the photo, signature and ID number on both card and chip, plus a separate number to act as a debit card linked to

the financial system through ATMs. The proposed legislation would have allowed expansion of the content of both register and chip with little legislative control; access to the Register by police and security agencies; and a system of 'infringement notices' when the card was improperly demanded. Supporters and critics disputed what was needed to reduce social security fraud, whether 'function creep' was inevitable (or even intended), and whether 'pseudo-voluntary' production of the card would see it develop into a near-universal ID system.

The Australian Privacy Foundation and civil liberties organisations opposed the proposals to little apparent effect until a Parliamentary upper house Committee with a government majority began what were expected to be routine hearings on the Bill after its passage through the lower house. The Committee agreed with critics that the Bill was unacceptable because it did not contain the whole legislation (it was proposed there would be a later second Bill). However, its report made clear that it was dissatisfied with many substantive aspects. The government withdrew the Bill within 24 hours. Three months later it released a 'consultation draft' of a completed replacement Bill (Greenleaf 2008).

The Howard government did not reintroduce the Bill into Parliament before Australia's federal election in November 2007, partly because of the political risk involved in introducing ID card legislation once an election was imminent. This was the result that the extra-Parliamentary opposition had aimed to achieve. In the week before the election, the Labor Party Opposition finally announced its clear rejection of the Access Card. The Rudd Labor government was elected on 24 November and within a week it had formally announced the scheme was scrapped, had disbanded its administration, and told all contractors to stop work (Greenleaf 2007b). Exactly 20 years after the defeat of the Australia Card, the political process had again rejected a national ID card scheme.

Despite the Howard government's apparently dominant political position from 2005 to 2007 and the expenditure of millions of dollars on technical studies and consultants, it was unable to push this legislation through in the face of determined extra-parliamentary opposition and public skepticism. The scrapping of the Access Card is testimony to the enduring effect of politics in Australian privacy developments.

### **Back to 'Muddling Through'?**

It would be reassuring to be able to conclude that privacy in Australia will again 'muddle through' as a complex balance sheet of incremental gains and losses, a continuation of its past history. In Australia privacy is politics, because the constitutional and other institutional protections of privacy are so

weak. The lack of a history of overturning authoritarian regimes may also make it more difficult for Australia to resist incremental encroachments on privacy. At the end of 2007 the political pendulum has again swung, and democracy has delivered a pro-privacy result. But it is too early to conclude that Australia has a government actively supporting privacy, and that is not expected.

It is more likely that Australia will be back to the usual situation of governments frustrated in pursuing their ambitions of surveillance (in order to achieve their other goals) because of oppositions opportunistically advocating privacy in order to create political damage to their opponents. The new Federal government does not have a majority in the upper house, and it is quite uncertain whether it will ever obtain one, so there are better prospects than in recent years for the extra-parliamentary supporters of privacy to impede surveillance by obtaining support from the opposition parties. However, there is no reason to expect that the recent losses to privacy outlined above will ever be rolled back: both sides of politics seem committed to expanding the surveillance capabilities of the state. Perhaps this government will be more reluctant to use 'national security' to continually erode privacy, but there is no guarantee of that, as it complied with most of the previous government's wishes on that. The post-2001 trajectory of support for increased surveillance has had substantial support from both major parties, and at both levels of government. Privacy has few friends except opportunism.

To conclude on an optimistic note, by mid-2008 the Australian Law Reform Commission (ALRC) will complete the first major review of federal privacy law in 20 years, and the New South Wales Law Reform Commission will do likewise for that State's legislation. The ALRC has indicated its intention to recommend major changes to the Federal Privacy Act, strengthening its principles, unifying them between the public and private sectors, and removing many of the procedural defects such as the lack of rights of appeal (ALRC 2007, Greenleaf 2007c). If these reforms are adopted by the Rudd government and its State counterparts, then information privacy protection will be strengthened, to complement the near certainty of accompanying extensions of surveillance. Whether they will be strengthened enough for a Web 2.0 society and a post-2001 state is a story for the future.

## 6. Hungary

### Ivan Szekely

---

Constitutional democracy had barely triumphed in Hungary when, in January 1990, the scandal called 'Budapest Watergate', better known to Hungarians as 'Duna-gate', broke out. (*Duna* is the Hungarian name for the Danube, widely regarded as the great national river of the country.) What happened was that activists belonging to certain new political parties, who used to be called 'dissenters' during the not-so-distant days of the overthrown regime, now clandestinely entered the offices of the internal security agencies, and filmed what they found there during the night. The footage presented at a press conference proved that the infamous 'III/III Division', which kept the 'internal enemies' of the communist regime under surveillance, had actually survived the symbolic date of the democratic turn (23 October 1989), and continued tapping the phone lines of new party leaders and activists, keeping their private lives under surveillance and preparing reports on the information thus collected.

Although several commentators later suggested that this was nothing but the aimless and dysfunctional reflex of an apparatus left to its own devices after the collapse of the political system that had created and employed it, the scandal was hyped up by the printed and electronic media, which contributed in good measure to the devastating defeat of the successors of the single party in the free elections that took place a few months later. (The surviving reform-communist party received only 10 per cent of the votes, the new democratic parties about 90 per cent.)

Two weeks after the scandal erupted, the sources also revealed the identity of the person who had helped the documentary crew (named 'Black Box') to enter the premises and shoot their film. This was a renegade intelligence officer named Végvári who, after much self-torment, had made contact with the new democratic forces himself, and ended up in front of the television cameras making a public confession.

Duna-gate had more than mere political significance. It triggered a crisis of conscience among rank-and-file agents and their 'recruited' civilian collaborators, who often wrote secret reports on their colleagues, neighbors, and even their own families. By drawing public attention to secret surveillance methods, it also served to heighten public awareness of the vulnerability of privacy in general.



*Figure 6.1 Hungary beyond the Iron Curtain*

Today, Hungary is one of the so-called new European democracies, a member of the European Union, a forerunner of institutionalizing informational rights in its region. The country inherited its central population registration system from the old regime, under which every citizen's basic identification data, such as name, mother's maiden name, or date and place of birth, are registered, and this registry serves as an authentic data source for all sectors of public administration. However, the universal personal identification number has been split into three sectoral ID codes used in public administration. The biggest collectors of personal data are the tax authorities, the social insurance and the central voters' registry of the Ministry of the Interior. Other major centralized data controlling systems include the Central Statistical Office, the central vehicle registry containing both vehicles' and owners' data, and the system of employment offices.

With the introduction of a market economy, new private data monopolies have emerged, including commercial banks, insurance companies and private pension funds. Direct marketing is legal and regulated by law; spamming is unlawful but widespread. Still, more than 15 years after the Duna-gate scandal, accusations and public revelations about collaboration by public figures with the former secret services remain on the agenda.

When totalitarian rule was finally overthrown, the demands and opportunities

for reform were quickly exploited. A tightly-knit system of institutional safeguards for the new informational rights was constructed, including the protection of information privacy and freedom of information. As a result, in the late 1990s Hungary was catapulted into the position of a sort of role model for the fledgling democracies of the region.

The new Constitution includes the right to protection of personal data among the basic rights and freedoms. This provision is expounded by the Constitutional Court, and accordingly reflected in the legal regime, as the right to 'informational self-determination' – that is to say, the fundamental principle is that everybody has the right to control the flow of his or her personal data. The legislation follows the European general Act – sectoral Acts model. The basic law (the general Act in this respect) is the combined Data Protection and Freedom of Information Act of 1992 (DP&FOIA) which encompasses both the public and private sectors, in terms of all data processing operations, whether digital or conventional, paper-based. The sectoral Acts dealing with data protection (more precisely: with the processing of personal data) include the Records Act, the Direct Marketing Act, the Medical Data Act. Further central privacy provisions are to be found for example in the Police Act, the National Security Act, the Banking Act, the Insurance Act and several other Acts. Today, Hungary has nearly 1000 Acts and regulations that contain such provisions, more than 150 of them explicitly citing the DP&FOIA.

The independent supervisory institution of the new informational rights is the Parliamentary Commissioner for Data Protection and Freedom of Information (often referred to as the data protection ombudsman). His tasks involve the monitoring of the implementation and enforcement of the protection of personal data and the disclosure of data of public interest; investigating complaints and making recommendations (with binding force). The Commissioner's office has about 45 staff members, and it has a far-ranging investigative license; most of the employees are legal experts or information specialists. His powers encompass both the public and the private sector and are subject to very few restrictions.

Although the Commissioner's activities have, in practice, little administrative force, most of his positions are issued as non-binding recommendations, the institution is regarded as highly successful, relying on a broad base of professional and public recognition. Most observers feel it has won deference and support for its recommendations among data processors and data subjects alike. At the level of individual organizations the supervision of fair processing of personal data is supported by the system of internal data protection officers and internal data protection regulations, both stipulated by laws affecting a wide range of data processors.

Today, the exigencies and prospects of revolutionary change in guaranteeing personal freedoms and autonomy have lost much of their momentum and



*Figure 6.2 Hungary within EU borders since 2004<sup>1</sup>*

currency. In the first few years of the new millennium, international events and domestic developments such as anti-terrorist measures or merging of business databases created unfavorable conditions for the enforcement of informational rights in Hungary. That said, the country continues to be recognized internationally as being at the forefront of institutionalized privacy protection, which remains a cornerstone of Hungarian democracy. Indeed, Hungary has become something of a testing ground for latter-day democratic states to work out their own privacy concerns.

## KEY DEVELOPMENTS IN PRIVACY PROTECTION – A BRIEF HISTORY

Prior to World War II – and, for different reasons, for a long period after it – Hungary was not in a position to deploy a full catalogue of individual rights, including a modern system of informational rights. However, for the student of legal antecedents, it is important to remember that the authoritative

---

<sup>1</sup> In January 2007 two new member states, Romania and Bulgaria joined the European Union.

Hungarian textbook of civil rights from the period between the two Wars (Szladits 1941) reflects a positively progressive approach compared to similar western European works of the era.

Privacy in those days was conceived of as part of the larger scheme of protecting individual rights under civil legislation, especially the ‘inner image’ of the person, that is the general right to human dignity and personality. Equally remarkable in this regard is Hungary’s Penal Code of 1878, the so-called Csemegi Codex (Act No. V of 1878), which remained in force throughout the first half of the century, and defined a number of punishable felonies. Among these was the ‘prohibited revelation of a secret’, a notion used to prevent the unauthorized release of confidential information about clients by doctors, lawyers, and other professionals.

The first meaningful step along the road toward modern privacy protection in Hungary was a measure incorporated in the Civil Code in 1977; this declared that ‘the processing of data by computerized means shall not violate individual rights’. The enactment of this provision was not preceded by any sort of political debate or social interest, nor by any high-profile case surrounded by public controversy. In all likelihood, it emerged from professional circles familiar with western legislation, disputes, and initiatives.

International documents on data protection framed in the early 1980s – such as the OECD guidelines and the data protection convention of the Council of Europe – did not pass unnoticed in Hungary. They may have contributed to the decision of the president of the John von Neumann Society of Computer Science in 1981 to propose an ‘Information Technology Act’, which was sadly deemed ‘inopportune’ by the political leadership at the time.

### **A New Concept in an Old Setting**

The first really substantial step – and one that remains seminal today – was taken by an informal multidisciplinary group that had grown up under the wing of KSH, the Central Statistical Office, in the 1980s. This was the last decade of the Kádár Era, named after János Kádár, who came to power as leader of the communist party after the suppression of the Revolution of 1956, and ruled the country for over three decades. The KSH group collected and analyzed western debates, publications, laws, and legal practice, notably including international documents and initiatives pertaining to the protection of personal data and freedom of information.

The group fashioned a comprehensive concept for the information regime of the new Hungary to come, at a time when the country was still being run by the single-party state. The basis of this concept was the dichotomy of a transparent, accountable state and the autonomous, self-determining citizen. In fact, the group prepared two versions of a bill that combined elements protecting

both information privacy and freedom of information. One of these two early drafts ultimately became the foundation of Hungary's combined data protection and freedom of information Act (DP&FOIA), the basic information law still in force today.

Thus by the time communist rule was finally overthrown, not only a general legal concept, but also the single most important constitutional draft incorporating it already existed. This gave Hungary a professional and historical edge during the upheaval of the political transformation, allowing for speedy completion of the infrastructure of information law and its reinforcement by the appropriate institutions. Most important among these was the office of the Parliamentary Commissioner for Data Protection and Freedom of Information (DP&FOI) Commissioner.

Beyond its professional input, the KSH group later gave Hungary, among others, the first president of its new Constitutional Court, who also became President of the Republic in July 2005; the first and the current DP&FOI Commissioners; one of the professional leaders of a reformed Ministry of Justice; and the author of this study. Those members of the group who did not take up office in the institutions of the new political arrangement founded a civil organization, InfoFilia, the Hungarian Data Protection and Freedom of Information Foundation. During the period until the election of the first DP&FOI Commissioner, InfoFilia was instrumental in promoting up-to-date awareness by translating and publishing major international documents dealing with informational rights.

### **The Democratic Turn and the Period of Transition**

In October 1989, after long months of demonstrations and tense negotiations, the new democratic forces took over political power, and, on the anniversary of the bloodily suppressed 1956 revolution – the first nationwide uprising against Soviet rule – the Third Hungarian Republic was proclaimed. This act was emblematic of the single decisive development in recent Hungarian history: the basic transformation of the political system. This transformation went hand in hand with the weakening and eventual collapse of Soviet military and political power, the dissolution of the single party state, the overhaul of the legal system and public administration, the rapid rise of a market economy, the emergence of major organizations in the private sector, the appearance of NGOs, and of course the influence of all of these factors on society. These circumstances created a once-in-a-lifetime chance – a window of historic opportunity that remained open for a couple of years – to shape power relations pertaining to information almost at will, draft the new rights and set up the new institutions, as well as to proclaim information principles and situate them on a reshuffled list of priorities.

Thanks to the efforts of the KSH group, Hungary succeeded in exploiting this opportunity efficaciously and in time, putting in place all the major legal and institutional guarantees before the first wave of change subsided. In the domain of informational rights, this wave came in the form of reforms and initiatives launched from above – in hindsight, one might say it was an elitist movement in its origins.

This is not to say that the masses went unheard in this era. In fact, these voices were very strong, if not in the defense of privacy in particular, at least in their demands for rights and liberties in general. The privacy-related topic that received the greatest social and media exposure was the operation and eventual disbanding of the secret intelligence agency – the Hungarian equivalent of the Russian KGB or the East German Stasi. The single-party state maintained this organization throughout its existence under names, including the ‘III/III Division’. It differed little from its counterparts in Hungary’s allies, its main function being to monitor large chunks of its people’s private lives. Although the number of agents and their collaborators and the scope of their activities was never as extensive as in the GDR, everyone was aware of its machinations. This awareness left an indelible stamp on people’s conduct, distorting behavior patterns even in the private sphere – in particular among the dissenters and detractors of the system themselves.

The Duna-gate scandal triggered a broad-based push to unveil the operations of the III/III Division and to enable surveillance victims to access the files it had compiled on them. These demands threw into relief the two poles of classic privacy protection: the omnipotent state and the helpless citizen. Additionally, the institutionalization of privacy protection became inextricably intertwined with the codification of another fundamental informational right, freedom of information – or, as it is often referred to in Hungarian laws, ‘access to data of public interest’.

It also became clear, as soon as the party-state regime was overthrown, that Hungary’s institutional privacy protection would embrace the European approach. Particularly influential was the German model, in which the right to human dignity is one of the most solid cornerstones of constitutional democracy. Another development emerging from the fall of the old systems was the tendency for individual rights to become not only the subject of political debate, but also the subject of political negotiation and infighting. This made the implementation of new rights contingent upon current political realities and, in so doing, eroded the fundamental value of individual rights, including the right to privacy.

## New Rights, New Institutions

Hungary's new Constitution came into force on 23 October 1989. In reality, however, Hungary did not adopt a new Constitution in 1989 and has not done so since then. Instead, it has radically reworked and repeatedly amended the 'communist constitution', also known as Act XX of 1949. By insisting on thorough revision as opposed to all-out abolition, Hungary demonstrated its commitment to legal continuity and the achievements of the 'constitutional revolution', but it also passed up for good the historic chance to enact a brand new Constitution. Once the elation of transforming the political system had subsided, professional concerns and party politics made it impossible to indulge in such a lofty, symbolic gesture.

The new provisions of the Constitution declare that 'everyone in the Republic of Hungary has the right to [. . .] the privacy of his home and the protection of secrecy in private affairs and personal data' and that 'everyone in the Republic of Hungary has the right to [. . .] access and distribute information of public interest'. The Constitution also stipulates that the guarantees for these two rights have to be regulated by an Act of Parliament, passed strictly by a two-thirds majority vote. As another key measure, the Constitution not only established the institution of the Commissioner for Civil Rights as a pillar of constitutional democracy, but also empowered Parliament 'to elect special ombudsmen for the protection of individual [*meaning specific*] constitutional rights'. It was on the grounds of this provision that a Data Protection and Freedom of Information (DP&FOI) Commissioner was later elected.

April 1991 proved to be a milestone for privacy protection in Hungary, in terms of legal foundations and public awareness. This was when the Constitutional Court passed its Resolution 15/1991 (IV. 13.) AB, ruling unconstitutional the universal and standardized personal identification number devised for unrestricted use. With 'the Court banning the ID number', as the man on the street put it, Hungary became part of the group of former dictatorships that considered all-purpose centralized files on citizens irreconcilable with the principles of constitutional democracy. This camp includes Portugal, which enshrined such a ban in its constitution as early as 1976. In Hungary, the old regime had used a universal code to tag citizens from the 1970s onwards. During the period of democratic transition, both the personal ID number and the State Population Registration Office that kept it on file became emblematic of the single-party state.

Social awareness to the ID code affair, and privacy issues in general, owed much to this Constitutional Court ruling, which provoked fierce criticism among the entire government apparatus. Some detractors warned of nothing less than the end of viable state administration, while others took issue with the unreasonable costs of switching to a new, decentralized records scheme. These officials gave

dire warnings of chaos in the offices and impossible budgetary demands. Now it has become evident that these fears and counter-arguments were unfounded.

However, the abolition of the universal ID code was not the only feature of this well-known Resolution. In addition, the Resolution threw out the entire system of population registration, mandated the legislature to enact a law on the protection of personal data and the disclosure of data of public interest, and to concretize its general principles in a series of sector-specific acts. Most influentially of all, the Constitutional Court outlined a thorough theoretical and technical interpretation of the right to protection of personal data, defining it as the individual's right to make active decisions about information that concerns him or her, rather than merely as the passive right to have such information protected, as in the traditional sense. In other words, citizens are no longer defenseless individuals who, if they behave themselves, deserve the benevolent protection of a paternalistic state. Instead, they are autonomous people with free will who are entitled to determine for themselves who can use information about them – and for what purposes, under what circumstances.

### **New Laws, New Regulations**

The key Hungarian privacy law – an act combining elements of both data protection and freedom of information (DP&FOIA) – was passed in the fall of 1992, following lengthy debate in professional and political circles. Thanks to the conscientious groundwork that had preceded it, the Parliament adopted the DP&FOIA without a single contrary vote. The idea of enacting a single act providing for both informational rights was inspired partly by the Canadian model, and partly also by widespread desire to legislate safeguards for both rights simultaneously.

The joint regulation sought to prevent any easy way of pitting the two rights against one another in an effort to play privacy off against freedom of information, or vice versa. Nevertheless, there have been abuses since the DP&FOIA entered into force. Some public officials have sought to withhold documents from applicants on the grounds that these contained their signatures – unquestionably personal data – and as such warranted their own discretion over disclosure. Obviously such twisted arguments run counter to both the letter and the spirit of the law.

In essence, the DP&FOIA defines personal data and the right to their protection – the latter now interpreted by the Constitutional Court as informational self-determination. It then proceeds to define, as a rule of thumb, all information that is not personal in nature as data of public interest, and therefore subject to public access. This simple model sheds clear light on the original intention behind the law – namely to use both informational rights as a means to rein in the excessive informational power of government.

In the area of privacy, the DP&FOIA explicitly prohibits data processing, except with the consent of the data subject, or as required by law, understood narrowly as an Act of Parliament. It spells out the subject's option of legal remedy, and classifies the act of 'unauthorized data processing' as a violation punishable under the Penal Code. The law furthermore establishes the office of the DP&FOI Commissioner, as an independent body in custody of informational rights. Unfortunately, it took Parliament another three years to elect the first DP&FOI Commissioner.

By and large, the law adopted in 1992 was a modern piece of legislation. It inspired a series of legislative efforts in a number of new democracies from the Baltic countries to the successor states of the former Yugoslavia. It rigorously incorporated the major tenets and provisions of European privacy norms. Indeed in some ways it was slightly more stringent than its European counterparts – as in provisions for data transfers abroad. The advocates of stringent and consistent regulation argued – and they continue to insist today – that new rights and liberties needed and warranted stricter protection in former dictatorships than in traditional democracies with true and tried legal and social practice.

The adoption of the DP&FOIA did not mark the end of legislative efforts pertaining to privacy. Starting in the mid-1990s, a series of sector-specific data protection laws saw the light. Some of these merely serve to expound upon the general rules of the DP&FOIA and apply them to specific areas from the health sector to higher education, while the majority stipulates exceptions. In 1996, Parliament passed the Identification Numbers Act, which complied with the Constitutional Court's Resolution discussed above. It abolished the universal code, replacing it with three specialized numbers: the personal identification number (its use far more limited than that of its predecessor), the tax identification number, and the social security number.

Beyond proper Acts of Parliament with their own independent titles and numbers, sectoral legislation has prominently included privacy provisions that have been incorporated as chapters, sections, paragraphs, and appendices in a number of other laws besides the DP&FOIA. These include, among others, the Anti-Discrimination Act, the Higher Education Act, and the Electronic Commerce Act. In addition, privacy provisions are to be found also in several regulations lower down the hierarchy of statutory instruments, which do not provide for processing of personal data in and of themselves, but may provide more detailed interpretations of the details of existing Acts of Parliament. The number of laws and decrees with implications for data processing continues to rise. Overall, the constitutional right to the protection of personal data has been successfully integrated with the system of Hungarian law. Yet in its spirit and effect it does not follow the traditional branches of legal hierarchy such as the areas of public and private law, instead it constitutes a new dimension permeating the entire legal corpus.

## **The Parliamentary Commissioner as Independent Supervisor**

One could have predicted that there would be strong political and business interests against guaranteeing information privacy for the citizens of the Third Republic. Accordingly implementation and enforcement of the new informational rights would require an independent supervisory agency. But who could be the most efficient, legitimate and publicly accepted supervisor in the turbulent situation of a new democracy? A civil organization, a popular front committee, a new government agency, or an honorable individual? In the DP&FOI Act of 1992, legislators envisioned the latter: a one-person office of the parliamentary commissioner, an independent institution to monitor informational rights with a special range of tasks.

In 1993, the Parliament adopted the Act on Parliamentary Commissioners, which defines the functions and procedures of a parliamentary commissioner of the ombudsman type; that is, a state official appointed to provide a check on government activity in the interests of the citizen, and a general deputy, both vested with general powers. This Act upholds the right of Parliament subsequently to elect specialized commissioners to safeguard specific constitutional rights. This latter measure was motivated by the aim of ultimately deploying three commissioners: one with general powers (plus his deputy, actually the fourth commissioner), one for the protection of national and ethnic minority rights, and one for the protection of personal data and freedom of information – whose duties and powers had already been specified by the DP&FOIA.<sup>2</sup>

In the summer of 1995, a year and a half behind schedule, the Parliament finally elected its first commissioners. These included the DP&FOI Commissioner, László Majtényi, a professor of law. The powers attributed to the DP&FOI Commissioner are far more extensive in scope than those of his colleagues – mainly because they had been drawn up separately by the DP&FOIA in 1992, one year before the Act on Parliamentary Commissioners.

Although the office had been practically unknown in Hungarian law, it took only a few years to find a proper niche within Hungarian institutions and public consciousness. Lodging a complaint with the DP&FOI Commissioner – essentially an alternative to filing a suit in court – has been a popular option with plaintiffs from the start. It is only rarely that individual data subjects (or the lobby groups behind them) turn to court, most parties preferring a submission to the Commissioner. The Commissioner's case law in Hungarian data protection has come to cover a wide range, from ovum donation to the

---

<sup>2</sup> In 2007 the Parliament abolished the institution of the Deputy Commissioner and established a new parliamentary commissioner for the protection of environmental rights, called Parliamentary Commissioner for the Future Generations.

administration of anonymous HIV tests, and from revelations about citizens' political pasts to spamming and direct marketing. This body of law has mainly emerged not from courtrooms but from the evolving practice and recommendations of the Commissioner.

## Landmark Cases

Hungary's first high-profile privacy controversy was the 'lottery jackpot affair'. In October 1995, somebody won the biggest prize in the history of the Hungarian lottery, which had been accumulating for a long time. Szerencsejáték Rt., the State Gambling Company, had the television crew of a news program named '*Objektív*' and photographers from *Népszabadság*, one of the largest-circulation dailies, do several 'takes' on the 'discovery' of the winning ticket. Using the footage, the TV crew managed to identify the name and address of the winners from the reverse of the ticket, and called on the family late at night. Despite the wishes of the winners, who requested anonymity, the interview with them was aired the following day. The imperfect distortion of sound and video, along with the airing of their personal data, made their identity publicly known.

The DP&FOI Commissioner investigated, and ended by condemning Szerencsejáték Rt.'s processing of the data and the TV crew's conduct. True, the fine print on the back of lottery tickets read, '*I consent to the use of my name and address in the news media*'. But it was obvious to everyone that the TV crew had physically infringed upon the privacy of a family and – given the huge amount of the prize thus disclosed – had even put their lives at risk by misleading them about the purpose of the interview. Sadly, the TV crew never really admitted their wrongdoing. The case divided the media industry itself, with some journalists arguing that alert TV journalists had all the rights in the world to delve into private events of interest to viewers.

In 1998 a girl of 13 applied for an abortion, with the consent of her mother. Her case, which came to be known as the 'Case of the Girl from Dávod', received wide exposure due to TV coverage and triggered an investigation brought by the Commissioner. This case proved even more divisive, as it forced everyone familiar with it to take a stand on the boundaries of privacy and, by implication, also on questions of ethics and ideology. Having learned of the pregnancy, a family rights advocacy group initiated an official process to stop the abortion, and helped to publicize the case.

The mother lodged a complaint with the Commissioner in order to identify the person guilty of having abused her daughter's sensitive data. The ripples generated by the case reached both the electronic and printed media. A prime-time report by public television featured the names, address and images of the girl and her mother, and even showed footage of their house and living

environment. The abortion which was performed in the meantime rendered the debate between pro-choice activists and their detractors pointless, even as the continued publicity deprived the family of the last vestige of their privacy. Remarkably, the pro-life commentators never acknowledged the subject's right to privacy or the legal provisions governing it as legitimate concerns.

A case known as the 'VIP list scandal' triggered social debate over another area of privacy. It centered on Postabank, one of Hungary's major commercial banks. Postabank offered loans and investment opportunities to certain leading politicians, public officials, and celebrities at much more favorable rates than the prevailing market terms. Having acquired a list of names of parties and the benefits they received, the press assumed that improprieties had occurred. Not only did they hold that the bank had offered preferential treatment in the hope of improving its lobbying positions, they also charged abuse of office by several of the individuals involved.

The Commissioner answered a journalist's submission by asserting that the public release of the personal data in question could not be defended on any legitimate grounds. Nevertheless, he held, there were indeed strong reasons to enact new provisions assigning broader limits of exposure for individuals in public office. In his position statement, the Commissioner cited a number of Resolutions by the Constitutional Court, which established narrower constitutional protections for the privacy of public officials than for that of the ordinary citizen. Ultimately, the Commissioner was unable to prevent the publication of the VIP list, which also featured the data of several individuals without public responsibility, including actors.

After the turn of the millennium, high-profile privacy cases were increasingly filled with political content. In 2001, the so-called 'National Image Center', an agency created during the previous government cycle, illegally obtained from the Ministry of the Interior's central records the data of at least one person in practically every Hungarian household, and proceeded to mail them issues of the magazine entitled *Millenniumi Országjáró* ['*Millennium Country Rambler*']. The aim was to promote the policies of the conservative government in power.

In response to a barrage of complaints, the Commissioner called on the cabinet members in charge to stop the unlawful circulation of the magazine, but to no avail: the government continued to mail the publication to citizens until it lost the next elections in 2002. Attacks on the government's abuse of its citizens' data in a political direct marketing campaign was high on the agenda of the political opposition. Ironically, a year later, the socialist party, which had led the opposition, availed itself of very similar means when it mailed a campaign letter by its candidate for prime minister to addresses processed in violation of the law. (Hungarian laws prohibit political parties from engaging in direct marketing activities. Pursuant to the Election

Procedure Act, political parties may not legally acquire citizens' addresses until 20 days prior to Election Day.) The Commissioner responded by calling on the party to destroy the list in question. Although the Party Chairman insisted that the party had acted within the law, he destroyed the databases publicly, on the record.

Towards the end of his six-year term in office, the Commissioner issued several recommendations, such as the *Millennium Country Rambler* case, directly blocking interests of the prevailing power-holders. In reply, certain populist political circles went so far as to propose abolishing the office of DP&FOI Commissioner altogether. Even the more sober voices within government made it clear they would not support the reelection of the country's first Commissioner for another term, despite his uncontested qualities as an individual and professional.

Though no political formation of any standing had the slightest intention of getting rid of the institution itself, the election of a new Commissioner turned out to be far more difficult than anticipated. The few individuals who met professional eligibility requirements and proved acceptable to both major political coalitions declined the candidacy, while candidates nominated by one side were consistently voted down by the other. Finally, after negotiations lasting almost six months, the Parliament succeeded in electing the country's new DP&FOI Commissioner, Attila Péterfalvi, a lawyer from the first Commissioner's office. During the transition, the General Commissioner – one of the three parliamentary commissioners – filled in for the DP&FOI Commissioner, running the Office and issuing recommendations and position statements on his behalf. This solution is obviously subject to all sorts of criticism on both legal and professional grounds.<sup>3</sup>

The case spurring the greatest debate since the second Commissioner took office broke out around the website *Hálapénz.hu* in 2004. (*Hálapénz* in Hungarian means an informal payment or gratuity given to doctors and health care workers.) Operated by private individuals, the site featured 'a searchable nationwide database of obstetricians' from which the user could access patient evaluations and learn the amount of the informal payment expected by each physician for care supposedly financed in full by social security – hence theoretically free of charge to the patients. Visitors typically accessed the site to learn how much it would cost them to give birth under the supervision of a specific obstetrician, and precisely what services they could expect in return.

---

<sup>3</sup> At the time of writing a similar situation occurred: in December 2007 the Parliament failed to reelect the DP&FOI Commissioner in office, therefore in the interim period the new General Commissioner – a newcomer himself in the office – had to fill in for his fellow commissioner. The three new candidates were subsequently rejected by the Parliament in February, April and May 2008.

It was of course the online posting of this latter information that stirred heated professional and social debate. Most commentators agreed that gratuities in health care were socially detrimental, but the controversy was about more than just the legitimacy of this custom. The advocates of disclosure proposed that the freedom of communication and opinion entitled expectant mothers and their relatives to share their experiences with obstetricians online. They argued that, in conducting childbirths financed by social security, doctors used public funds and fulfilled a public function – and that therefore their data relevant to these activities did not merit protection under privacy regulations. As for patients referred to a ‘private practice’, they typically received care using institutions and equipment financed by public funds as well. By contrast, the proponents of privacy stressed their perception of the doctor-patient relationship as a strictly confidential one, adding that the physicians involved had never abused their office. According to their view individuals who did not offer a gratuity received equally conscientious care, and gratuities were normally expected only for certain extra services, such as the obstetrician personally attending and conducting the childbirth even when off duty. The DP&FOI Commissioner came out in support of this latter opinion. As a result, the operator removed the site from the internet.

### **Underlying Processes and International Influences**

The legal history and the landmark cases do not necessarily reveal those background forces, both internal and external, which ultimately exert a fundamental influence on the direction of progress. As to the internal forces, during the period following the radical transformation of the political system in Hungary, the three changes with the most notable consequences were: the reform of the state’s mechanism for handling information, the emergence of a new data processing monopoly, and the modernization of the relevant technologies.

The first change came together with the establishing of institutions and tools for steering, supervising and balancing state administration that characterize modern constitutional democracies; consequently, there have been changes in the ways these new institutions demanded information and linked their databases. This is not to say that the thirst of government for ever larger doses of information has been quenched. On the contrary: renewed efforts at centralization have signaled a call to link databases more intimately than ever before, and resulted in the elaboration and promotion of a new system of efficiency-based arguments such as the necessity of avoiding parallel data registration.

The second is the emergence of large data processing organizations in the private sector, such as commercial banks, insurance companies, private

pension funds and direct marketing firms, mostly subsidiaries of multinational companies – some of them handling personal data of almost one third of the population of the country – supplanting the government's former monopoly on information. Growing up around the Big Brother, these 'Little Brothers' claimed their share of informational power, and have continued to exercise that power over large masses of data subjects. These organizations, for example – borrowing the techniques from their western parent companies – are secretly monitoring people's buying and surfing habits on the internet and use this information for offering products and services with unfair 'dynamic pricing', in other words, showing a higher price than advertised, to those supposed to accept it.

The third major change involves more than just replacing computers, in both the public and the newly reborn private sector. It also meant introducing qualitatively new methods of keeping and analyzing records, such as the building of 'data warehouses' and performing 'data mining' analyses, as well as the linking of personal data systems that had so far been handled separately. As a result, banks can share with each other data relating to bad debtors, or advertising companies can flood potential customers with unwanted emails based on their consumer profiles.

In this way, the power to collect and analyze information that so deeply influences the life of the individual was not really reduced in the newly democratic Hungary, so much as restructured and rendered more transparent, as well as being made subject to more extensive safeguards designed to protect the individuals.

The OECD Data Protection Guidelines, the Council of Europe Data Protection Convention, and the EU Data Protection Directive had a considerable effect on the development of privacy protection in Hungary. Hungary became a member of the OECD in 1996. Compliance with the Guidelines has not posed any difficulties since the adoption of the DP&FOIA, considering that the concept for the Hungarian legislation had been well harmonized with the Data Protection Principles since the days before the democratic turn.

The Council of Europe granted membership to Hungary in 1990. Although the country had signed the Convention in 1993, somewhat surprisingly it did not ratify or promulgate it until 1997 and 1998, respectively. The Ministry of Justice explained the delay by saying that they did not want to ratify the Convention until the appropriate regulations for the data processing sectors identified by the Council of Europe Recommendation had been implemented. In this way, the Council of Europe norms left an indelible stamp on the development of Hungarian data protection laws. At the same time, forces intent on limiting data protection, such as the police and other law enforcement agencies have also been very active in exploiting international relations. A case in

point was the 2001 Convention on Cybercrime, a legal document containing several provisions overriding national data protection laws, which happened to be opened for signatures in Budapest.

Hungary joined the European Union in May 2004, during the latest wave of EU expansion,<sup>4</sup> when the number of members grew from 15 to 25. Concurrently, of course, Hungary had to fall into line with the direct and indirect regulatory institutions of the EU, including its Directives. This is why the accession had been preceded by a lengthy process of legal harmonization. Meeting the requisites of the Data Protection Directive did not demand any major amendments in Hungarian law, because the competent EU body had already recognized Hungary – at her own request – as a country offering an adequate level of data protection. Hungary had in 2000 become the second non-EU country after Switzerland to secure this recognition. The result was to ensure that it would receive essentially the same treatment as any EU member state regarding the cross-border transfer of personal data, and that Hungarian citizens would be entitled to the same degree of protection of their personal data as any EU citizen. To bring about full legal harmony it was still necessary to broaden the powers of the DP&FOI Commissioner, which the Parliament duly accomplished by amending the DP&FOIA in 2004.

Despite harmonization efforts, the new international relations and commitments have had a rather contradictory impact on the fate of informational rights, not only in Hungary but in other countries of the region as well. On the one hand, the international community expects the new democracies to enact laws guaranteeing individual rights and liberties. On the other hand, various other factors have put pressure on these countries' privacy guarantees. These include their fresh membership in NATO; the demand to join the common European policy on external border controls and sharing of travelers' data, the so-called Schengen Region, and the consequent broadening of their responsibilities in guarding borders and cooperating with Europol and other international investigative agencies; and even their informational dependence on US support in areas of trade, investments, technology transfer, or immigration. External demands for excessive processing personal data, such as the retention of data of mobile telephone calls, for giving freer rein to secrecy legislation – for example, introducing the four-level classification of 'cosmic top secret', 'top secret', 'secret' and 'confidential' types of documents restricted from public access – and collaborating on anti-terrorism measures have had adverse effects and led inevitably to restrictions on informational rights, no matter how recently the latter may have been enacted.

---

<sup>4</sup> See footnote 1.

## PUBLIC OPINION

The first comprehensive public opinion survey on privacy issues in Hungary was conducted in 1989–90 by the Hungarian Institute of Public Opinion Research (MKI). Conducted in the midst of the political transformation, it served to provide a snapshot of views and attitudes in flux. But the results also pointed to several themes in public opinion that are presumably less prone to fluctuation or change (Székely 1991).

Using a representative sample of 1000 individuals, respondents were asked: ‘Would you personally object or not object if the following data about you were made publicly available?’ The survey concluded that the most sensitive personal data in Hungarian population were those pertaining to family, financial status, and health, with every other respondent objecting to the disclosure of such information (Figure 6.3, dark columns). The least sensitive category comprised information related to ethnic background, level of education, and occupation. The universal personal ID code, still in use in those days, ended up in mid-field.

The survey also included questions about examples of invasion of privacy: ‘Is your private life invaded or not invaded if someone taps your phone?’, etc. According to the responses, the most sensitive examples were: letters received open (over 90 per cent of the respondents objected), conversations and telephone calls monitored (Figure 6.4, dark columns).

The survey also showed that although Hungarians had a moderate awareness of the potential uses and abuses of their data, nearly all reported themselves to be obedient suppliers of their own personal information, whether it was sought on a mandatory or voluntary basis. Responding to the question: ‘Does it happen or not happen that at official places you refuse to give certain

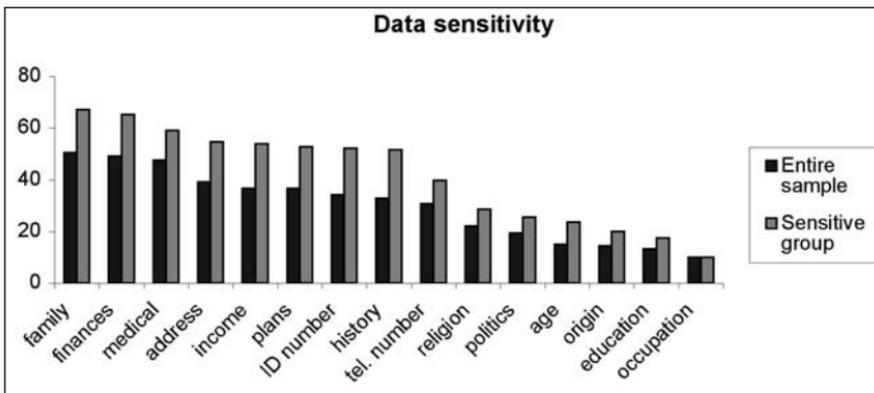


Figure 6.3 Data sensitivity

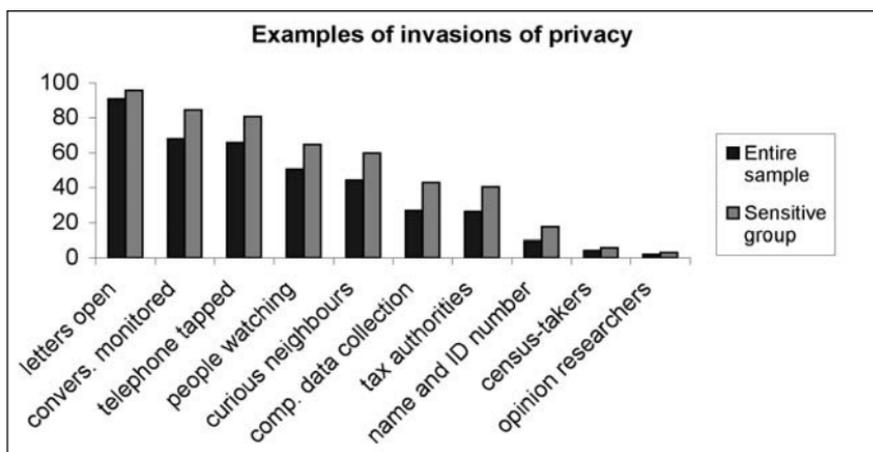


Figure 6.4 Examples of invasions of privacy

data about yourself?', only a very few cases of refusal to disclose personal data were reported. However, the respondents' answers revealed a considerable degree of distrust toward power and control over information, along with its beneficiaries and practitioners.<sup>5</sup> Given that informational privileges in Hungary at the time of the survey were predominantly held by institutions of the single-party state, state-owned corporations, and personnel departments, the most obvious targets of distrust were government agencies in general, and also computerized records as such.

Respondents took the most positive view of data practices at the workplace and those of OTP, the National Savings Bank that was still a monopoly in those days. By contrast, personal data use by the tax authorities and utility bill collectors elicited the strongest dislike among citizens.

Perhaps the most remarkable result of the survey was the discovery of a 'mysterious', privacy-conscious social stratum. Sixteen per cent of the respondents were significantly more sensitive to transgressions of their information-related privacy, in *all aspects* touched upon by the survey, than the rest of the population (Figures 6.3 and 6.4, light columns). Interestingly, however, no difference could be detected between this subset and the entire sample at all in terms of social status – such as age, sex, level of formal education, or place of residence – or political affiliation that could have correlated with the

<sup>5</sup> A comprehensive international survey on the globalization of personal data, conducted in 2006 at Queen's University, Kingston, Canada, showed an increase in acceptance of all major data processing techniques and a decrease in the level of distrust and resistance in Hungarian population (Székely, forthcoming).

discrepancy. This suggests that the demand for informational self-determination does not follow precisely understood social roles but represents a rather special dimension.

Quite noticeably, even without a poll, awareness of the DP&FOI Commissioner's role has been a major factor behind the currency of privacy as a topic in public discourse. In order to ascertain political and public acceptance, in 1998 the three parliamentary commissioners ordered a poll. That survey found the three commissions together to be one of the most popular public institutions, preceded only by the President of the Republic, the Constitutional Court, and the political party preferred by the respondent. According to the representative survey, 43 per cent of Hungarians claimed to have heard about the DP&FOI Commissioner three years after the institution was created.

### **Public Opinion and the Media**

In 1991, MKI conducted another comprehensive survey, entitled 'Aspects of Privacy and Informational Autonomy in the Press', a review of articles from four national dailies from 1987 to 1990. The researchers collected what they hoped was an exhaustive list of publications and analyzed their content, in particular the ways in which they construed privacy-related. The aim was to examine the representation of informational privacy in the leading press organs during the period of democratic transition.

Despite the relatively large number of articles devoted to privacy-related issues, the quantitative and qualitative analyses revealed that the topic *itself* did not get the attention of the press that it deserved. Even though the politicization of informational rights pushed these news and stories briefly into the limelight, later it was the same process of excessive politicization that led both the media and the public to concentrate too much on one, relatively minor, aspect of the problem. The case that provoked the most vocal response in the press of the day was Duna-gate and the associated surveillance scandals that we have already discussed. However, even these articles failed to address the essential fact that the victims were subjected to illegitimate surveillance of their lives, professional and personal relationships, and even their bedroom secrets, as *private individuals*. Instead, the focus was always on their status as *politicians in opposition*.

Since those days, and particularly since the election of the DP&FOI Commissioner, the media has shown much more interest in the topic. And yet, the over-politicized nature of the issue – that is, everything must be evaluated in the light of party politics – has remained with us as one of the most stubborn evils, a sort of *morbus hungaricus*, or Hungarian disease, that keeps haunting not only the media but public affairs in general as well.

## **Professional Reception**

There are several professional groups with vested interests in the broadest possible access to the data of clients, existing or targeted. The representatives of government offices and business ventures are obviously biased in their assessment of privacy concerns by their professional and business interests, for example in selling and buying marketing lists from the central population registry. Ironically, senior public officials and entrepreneurs with a tendency to scorn advocates of privacy often take the opposite view as private individuals. They object to being subjected to the very same methods and techniques by which they themselves seek to encroach on the privacy of others, and for the use of which they seek to win legitimacy by public consensus. An executive director who aggressively propagates the use of consumer profiles, would not be happy if someone built and used his or her own profile. We find, however, two disciplines where any business interest is certainly out of the question: those of law, and of information science. Both of these have a decisive say in assigning limits to the precedence of informational privacy.

In Hungary, civil lawyers, those most engaged in data protection issues, consider the Civil Code as their fundamental source of law, a veritable Bible that guides their views of data protection. Yet Hungarian data protection law derives from a constitutional right, and as such stretches across all the traditional elements of the legal corpus. Many Hungarian lawyers still find it difficult to reconcile the two approaches and the practical consequences they entail. Those lawyers who work in a sector with vested interests in evading privacy typically identify with the standpoint of the company or industry in which they make their living. As a result, the promotion of data protection and informational privacy in professional and public circles has become the privilege of constitutional lawyers, a peculiar elite in the legal sector; indeed data protection itself has become something of an elitist subject as a result.

As for those who work in the IT sector as system designers, programmers or operators, the hostility and lack of comprehension that often manifests itself on the surface is usually underlain by a tendency that is not unique to Hungary but can be found in many countries boasting a highly advanced ICT. This is because, as a rule of thumb, the IT professional is always a natural ally of the more powerful party in the equation (that is, the government agency or the business company rather than the citizen or the customer), which commissions his services, pays him, and presents itself as the underwriter of his professional career. In terms of informational privacy, this stronger party is invariably the data controller, understood as a public or private-sector organization responsible for and interested in processing the data of clients, prospective or existing, as well as of ordinary citizens and those registered to vote. To become a chief information officer of a data handling monopoly such as a big insurance

company is always more appealing for these professionals than working for a grass-root civil organization.

The author's experience, both as a consultant and as a professor teaching future IT professionals, suggests that an average system developed by IT personnel is bound to reflect the perspective of the data controller, with little if any regard for the interests and rights of data subjects. The information technology specialists take 'Big is Beautiful' as their motto. They think in terms of designing, implementing, operating and linking large systems in which personal data are collected, processed and analyzed in ways beyond the control of data subjects and supervising authorities. To be sure, there are also IT professionals in Hungary who dedicate at least part of their talent and efforts to the benefit of the weaker side. This small non-conformist minority, is often ostracized as 'a bunch of hackers'.

Let me mention one last trait that characterizes the IT attitude: many computer professionals are steadfast in equating data protection with data security. This globally familiar misconception no doubt has more widespread and deeper roots in Hungary and other post-communist countries with a history of authoritarian rule. For here, no other interpretation was possible before the democratic transformation: since data protection serves the interests of the individual, while data security mostly serves the interests of the data controller or the informational power, data security proved to be a perfect fit for the ideology of the totalitarian state and its organs.

### **Attitudes of Civic Associations**

NGOs represent special voices on privacy in the public forum – voices that are frail in absolute force but quite radical in their claims. The small number and belated formation of civilian organizations concerned with informational rights seem to reflect an empirical correlation noted in a number of new European democracies: where there is an official custodian in place, the civilian push for informational rights will be weak; conversely, where official supervision is inefficient or nonexistent, NGOs will undertake the missing function of enforcement on their own.

In Hungary, the wide recognition of the DP&FOI Commissioner as the custodian of information privacy and access to public information, along with reforms trickling down from above, has helped to shift the focus of civilian activism to other areas. These include environmental protection, help for the homeless, and the fight against gender discrimination. In other countries of the region, such as Bulgaria, the missing institutional protection of informational rights has triggered grass-roots privacy activism.

Most of the few Hungarian civic organizations focusing on informational rights have emerged since the turn of the millennium. One that had existed

before the foundation of the DP&FOI Commission (and which still exists) is the Hungarian Civil Liberties Union, whose core activity is providing public advocacy and free legal aid in connection with personal data protection. More recently, a new wave of concern has brought us Technology for the People (TEA), and the No Camera Group. All of them are composed of a handful of dedicated professionals and activists who are able to organize public events and attract the attention of the media.

A case in point was a flurry of NGO activity against video surveillance of public areas. This was provoked in no small part by the Commissioner's ambivalent position on the issue, which led him so far as to install CCTV cameras in his own office building. The No Camera Group organized street performances, set up symbolic changing booths in front of public surveillance cameras, and performed strip-teases and changes of clothes amidst the crowds of downtown Budapest. Their formation signals a measure of civil disobedience over the degree to which informational privacy principles are enforced and over the operation of the institution appointed to their protection.

Since 2001, the annual presentation of the Hungarian Big Brother Awards – the local version of the negative prize invented by Privacy International that has been adopted in several countries – has been a popular manifestation of radical civilian censure. TEA organizes this event, and a panel of respected personalities assigns the awards, which are handed out before a small audience – but always with the media in attendance. Ironically, the most intense controversy has surrounded the person of the Commissioner himself. In 2002, he was among those nominated for the Big Brother Award, on account of the cameras installed on his official premises. In 2004, he received another nomination – anyone may anonymously nominate individuals through the internet for the first round – this time for his lenient position on cameras installed in department store fitting rooms. In this case, the Commissioner found himself among the finalists and, after the online votes given to the finalists had been counted, actually ended up receiving the Audience Award. Attila Péterfalvi, the second DP&FOI Commissioner in office, not only appeared at the awards ceremony, but – unlike other recipients to date – accepted the award, although he made a point of voicing his disagreement with the rationale for his own selection.

## NATIONAL CULTURE AND TRADITIONS

Before the fall of the one-party system and the political transformation, there was obviously no real possibility for public debate about privacy and the right to a private life. In other words, these issues had not been properly thematized or made available for systematic study and research. Under the circumstances, one might perceive an element of surprise in the way – always committed and

optimistic but never unrealistic – in which the first DP&FOI Commissioner assessed the situation in his first Report to Parliament, on the years 1995–96, as follows:

The sensitivity of Hungarian society to data protection, and the right to informational self-determination is more advanced than was previously anticipated. Data protection does not represent a luxury demand of people of higher social standing or educational level, and the sensitivity to data protection cannot be closely attributed to social standing: It spreads across Hungarian society from the unemployed homeless to the highest ranking citizens. [ . . . ]

The personal identification number and the problems of shared registrations demanded considerable efforts from the office. Apart from the '*data protection related to the change of the system*' [ . . . ] the other classical fields of data protection are equally apparent in the Office's caseload.

At the same time, the Commissioner found that 'Society's general antipathy towards and distrust of the State is also remarkably strong' and that 'The process of change within the political system does not seem to have come to an end in respect of social or legal values.' (Majtényi 1998, pp. 11–12) These words were formulated a few years after the 'constitutional revolution', the peaceful handover of power to the new democratic forces.

While there was no disputing the benefits of the bloodless collapse of the past political regime and the measured pace of legal and institutional reform, they clearly amounted to passing up more than one cathartic and symbolic moment of opportunity to close the afterlife of communism and to open up the files of the past regime. In vain had the Duna-gate scandal broken out, the perpetuated ban on accessing secret service files left the government vulnerable to blackmail, accusing high ranking officials of being a former agent. On the part of the surveillance victims, the archives became targets of endemic distrust and discontent, being accused of hiding compromising documents in order to protect former agents.

But not all of the political forces active under the new democratic rules embraced informational rights whole-heartedly. The initiative mentioned above, aiming at nothing less than the abolition of the entire data protection apparatus, won influential supporters. One of these figures declared that 'data protection is alien to the Hungarian popular spirit'. (István Csurka, leader of the far-right Hungarian Justice and Life Party, around the turn of the millennium.)

Among the symptoms of a new capitalism springing up without appropriate checks and balances we find notoriously dismal standards of business ethics. These have allowed large multinational companies in Hungary, as in other recent democracies, to subject their clients and employees to treatment, including the use of their personal data, that they would never get away with in their own countries. In a big shopping mall in the neighboring Czech

Republic, for example, the female cashiers were allowed to spend only a limited amount of time in the restroom, just a few minutes each workday. Cashiers who were menstruating were marked with a red ribbon and allowed to spend a few more minutes daily in the restroom. As a result, everybody in the shopping mall, including supervisors, male and female employees and shoppers were visually informed about this sensitive personal data of the cashiers. This practice, which had not been introduced in the company's Hungarian shopping malls, due to adverse publicity, was not only unlawful but humiliating.

The general public concerning privacy matters has been evident not only toward government but also toward the business. There is a widespread and stereotypical belief along the lines of 'You can only get rich if you break the law' or 'The wealthy always have something to hide.' All this goes hand in hand with a hyped-up consumerism relying on a customer base too gullible and inexperienced to see a commercial offer for what it is. This is why the majority of marketing techniques continue to work in Hungary. The average consumer seems willing to go along with any scheme, including requests for his personal data – even while he or she remains skeptical of the honesty of business intentions by and large.

## WINNERS AND LOSERS

The institutionalization of the right to privacy, along with other far-reaching changes restructured informational power relations in Hungary.

During the period characterized by the establishment and consolidation of fundamental rights and their institutions, it was relatively easy to set up typical alliances that exist in other developed countries, with governmental and newly emerged private-sector holders of data on the one side and committed experts and scholars, the media, and the DP&FOI Commissioner himself on the other side. It was the latter coalition that proved victorious in the institutionalization of these rights.

Large private-sector users of personal data, including banks and insurance companies, saw their informational power restricted in the 1990s. But they soon found ways to get round the restrictions by introducing sophisticated data processing technologies such as data warehouses jointly operated by a group of companies – typically financial holdings – and by concealing the true extent and underlying purposes of the processing from both data subjects and auditors. When faced with criticism, these organizations are quick to deploy token solutions and empty rhetoric. As for government organizations, they initially seemed to yield to constitutional demands and partially decentralized their records for a few years directly following the democratic turn, for example,

established independent tax and social security registration systems. But later they improved their lobbying positions in the legislation and redoubled their efforts at re-centralizing information.

Contradictions abound in the situation of employees. On the one hand, they belong to the camp of the winners *in a general sense*, given that data protection law vests them with a variety of means to exercise control over the fate of their personal information. In theory, for example, they can refuse consent to the introduction of new fraud detection systems based on the analysis of their personal transactions, and they have a right to inspect video recordings made of them. In addition, restrictions have been placed on the scope of data processing operations available for the employer (for example, secret workplace surveillance is forbidden, data processing must be based either on law or the informed consent of the employee).

*In practice*, however, employees must be regarded as losers in the transformation, particularly in the private sector. There employers have brought about a situation in which workers fear exercising their rights for fear of losing their jobs or benefits. Moreover, they often do not learn about the violations of those rights until long after the event. Instrumental in perpetuating this sorry state of affairs has been the decline of an already discredited trade union movement and its effective banishment from certain new business sectors. Employees in hypermarkets or department stores owned by multinational companies sometimes have no choice but to deny their trade union membership.

In any event, the workplace has become a prolific source of privacy-related problems, from the monitoring of email correspondence and web surfing habits to tapping phone lines and even resorting to lie detectors purportedly 'based on voluntary consent'. (A comprehensive catalogue of real-world examples can be found in Szabó and Székely 2005.) In a case taken up by the Commissioner's office, a Hungarian company unintentionally replayed in real life an ironic scene from a film, *Egészséges erotika* (Healthy Eroticism), parodying the Communist Little Brothers who were watching the female employees' changing-room through secret video cameras – the real-world company had installed similar cameras in these changing-rooms 'for security reasons'.

There is one group that always sides with the winners: those who design and operate systems for the filing and handling of personal data. They are the natural allies of data controllers. Even an information technologist working in the Commissioner's office said recently during a professional meeting: 'Climbing Rose Hill in Budapest ten times cannot compare with the glory of climbing Mount Everest once' – meaning that creating big data systems is always more attractive for the IT professional than playing with small, interoperable, although more privacy-friendly systems.

On the whole, the media are clearly to be grouped with the winners of the

transformation. But they have had to learn not just how far they may, and indeed must, go in uncovering the secrets of the state, but also where the limits lie to their passion for divulging the private secrets of citizens.

The institution of the DP&FOI Commission in Hungary has been an undoubted success. Indeed, it has proved to be the single most effective tool for protecting constitutional rights. Recently it has received administrative-type powers in compliance with EU norms. But the air of social consensus that surrounded the Commissioner's operations at the outset when almost none of his recommendations had been questioned, now seems to be eroding, as critical remarks are increasingly articulated by the civil sector, the institution's most powerful former ally.

Historians, particularly those who specialize in recent history, believe they have been disadvantaged by the enshrinement of privacy. Many of them regard the subjects of personal data found in various files and documents as some sort of raw material that is free for the taking, arguing that the individual rights of these subjects should be sacrificed on the altar of research and knowledge of the past. By placing restrictions on the availability of such personal data for research and especially publication, privacy laws indeed limit the access of scholars to documents containing them.

A case in point was the Commissioner's widely known investigation and 'Recommendation on the microfilm recording of documents containing personal data relating to the persecution of Jews during the Nazi period, and on their transfer to the Yad Vashem Archives in Jerusalem'. The Commissioner stated that it was both unlawful and unethical to transfer such documents in the absence of bilateral agreements between the parties. The right to protest against the publicity of their data should also be granted to survivors and their family members, the Commissioner held, with respect to documents already transferred. Following this recommendation, bilateral agreements were signed by the respective governments regulating the relations between Holocaust centers in New York and Jerusalem and archives in Hungary, specifying the terms under which copies of documents were to be transferred, as well as detailing the rights and legal remedies available for the data subjects involved and their relatives.

Among the losers of the changes in recent years we find Hungarian travelers, particularly those traveling to the US, who must face data processing practices and treatment often antithetical to European norms. The official Hungarian reactions to the restrictive countermeasures introduced in the US have been a mixed bag. Investigative agencies, the increasingly profitable security companies, and the political forces that have always frowned on privacy and other informational civil rights, have been only too eager to satisfy American demands, indeed actively seeking ways to collaborate with a great new friend they hope will take the place of a lost powerful ally. All the while,

the various institutions safeguarding constitutional values, the DP&FOI Commissioner prominent among them, are defending disclosure of personal data by Hungarian agencies. In their view, such disclosure is based on the 'voluntary, unambiguous and well-informed consent' of the data subject concerned.

The broader social reception of these countermeasures is even more ambivalent. Even though the issue has not generated wide public debate, and Hungarian travelers continue to fill out the forms and submit to fingerprinting, they privately voice their suspicion and discontent at such treatment. On the one hand, this phenomenon seems to corroborate the findings of the detailed survey I mentioned earlier, namely that although people distrust power and control over information, they are obedient suppliers of their personal data. On the other hand, it may well be seen as the protracted survival of reflexes of a 'secondary public sphere' (the underground or informal public sphere under communist regimes in which developments could be sincerely criticized even if in the official public sphere one had to be a loyal follower of the actual system), triggered perhaps by recollections of life under the totalitarian single-party state.

The ranks of losers also include people targeted by advertising and marketing gimmicks, who realize only too late that by volunteering their data they have unwittingly consented to the unlawful and unethical use of their personal information. Those new (and older) internet surfers, for example, who naively supply their personal details for the sake of participating in an online game, often receive nothing but an unstoppable flood of spams. Paradoxically, the conventional direct marketing industry is one of the winners of a process that has created guarantees for the legitimate pursuit of such business, actually in response to the lobbying efforts of leading DM companies in the mid-1990s. True, privacy guarantees assign limits to the options available for direct marketers – mailing lists can be obtained only from legal sources, the source has to be indicated on every direct mail, 'Robinson lists' of individuals who have decided not to receive any direct marketing messages are to be kept etc. But these provisions are lenient enough to allow for profitable operation. Compared to the formerly unregulated situation, the winners include consumers who seek to maintain control of their data and who enforce their right to opt out, guaranteed both by the law and the DP&FOI Commissioner.

## INFORMATION FLOWS AND CONSTRAINTS: SUCCESS AND FAILURE

The single greatest achievement in the struggle for privacy rights was undoubtedly the court decision in the early 1990s ruling the standardized and

universal personal ID code unconstitutional. Following this around the middle of the decade was adoption of sectoral identification numbers instead, entailing the decentralization of government records and databases.

The critical task for the future is not simply to assign limits to the flow of personal information, but also to give data subjects greater control over their own data. The subject should be free to share or withhold personal data at his or her own discretion.

The Commissioner's recommendation and positions provide one index of success and failure. The case of the Holocaust documents, for instance, must be regarded as a success: although the Commissioner ultimately refrained from checking the flow of information, he did uphold the right of victims and their relatives to informational self-determination. By contrast, even the Commissioner himself admitted that his intervention against the drive to centralize and re-centralize data had been much less successful. He quoted a number of negative developments such as the centralizing of large personal data processing systems within the Interior Ministry, the broadening of the rights of investigative authorities to access databases, the establishing of the central debtors' register or the central employment register. All of these developments had legitimate purposes, but all of them significantly exceeded the necessary limitations of people's informational privacy.

By and large, the Commissioner has been rather successful in investigating egregious violations in individual cases, issuing recommendations and positions of general scope, and promoting the newly acquired informational rights. The overwhelming majority of his recommendations have been followed by the organizations at which they are aimed. On the down side, his activities and the way in which he construed his own role as a specialized ombudsperson with 'soft' power have done little to influence the main processes of the democratic transformation in Hungary such as the forming of new systems handling personal information. The Commissioner has often met with frustration in his attempts to deal with violations leading to class-actions violations, the problems of computerized data processing, and the practical implementation of his own registrar functions, that is, keeping record of data processing operations and data processors.

In addition, the Commissioner's attempts to tackle the flow of information concerning the operations of agencies that kept the 'internal enemies' of the regime under surveillance can ultimately be regarded as a failure. True, he was in an almost impossible situation, struggling to satisfy mutually contradictory calls for historic justice, for the respect of the privacy of victims and third-party individuals, for the vetting and removal of former agents from public office, for the retroactive vindication of the right to informational self-determination of everyone involved, and for what has been called the informational compensation of society as a whole. It is hardly surprising that the severally

amended provisions of applicable law and their implementation have failed to unravel the tangle.

To use a metaphor created by the Constitutional Court, the implementation of human rights is a one-way street where you cannot turn back. And yet the space to enforce certain informational rights was narrowed during the period of consolidation that followed the great democratic transformation: the efficiency-minded public administration has increasingly found itself in conflict with demands for privacy protection. Nevertheless, the growth of information processing, as in data mining technologies, should not automatically be interpreted as the failure of the cause of data protection, if the developers, operators and executives of these systems understand that the virtual sum of privacy protection and business targets is not a constant quantity, one of whose constituents will necessarily grow by the same amount if the other one is reduced. In other words, personal data protection is not necessarily an enemy of business or administrative efficiency.

Fighting for its informational rights and liberties, the civic sector has shown progress in recent years, although it is still quite weak. By and large, civic organizations seldom play a decisive role in questions concerning the flow of personal data, but their influence has been commendable for all its indirectness. Through the Big Brother Awards and other highly visible actions, they can be very successful – if only on a provisional basis – in focusing public attention on privacy values.

## PROSPECTS FOR THE FUTURE

Hungary, one of the new democracies of Central and Eastern Europe and a new member of the European Union, has now put the shock of collapse of the Soviet bloc behind it. During the initial phase of the new order, the country led the way in instating and enshrining the new rights and liberties. This is a process rife with blind alleys and labyrinths that we cannot fully discern from our vantage today.

It seems that the harmful and excessive politicization of informational rights, and of public affairs in general – as reflected in a wide range of phenomena from the Duna-gate case through extremist anti-privacy political statements quoted earlier to present-day dominance of party politics in the media – is here to stay. None of the successive, democratically elected parliaments and governments of Hungary have managed to change this so far. Therefore, we must look primarily to the political opposition for a stress on the values of informational privacy.

Dispersion of data protection know-how is now under way, with no sign of stopping. This is a welcome process indeed; a single, central organization of

expertise and advocacy hardly suffices to bring about the awareness of and concern for these rights among the general public. The current level of civic activism will probably be maintained, as will the dissatisfaction of the sector with the performance of the DP&FOI Commissioner as the chief official proponent of privacy. However, in view of the moderate dynamism of civic movements in general, we should not expect to see a significant growth in the number of these organizations or the actions they undertake.

Hungary is still a far cry from boasting a mature, socially responsible business sector. Most companies and entrepreneurs still regard increased market shares and profits as representing the only valid criteria for business decisions; few executives fully embrace fair treatment of customers as legitimate business concerns in their own right. It seems that entrepreneurs still need to experience spectacular breakthroughs and spectacular defeats before they can make room in their value systems for the service of public good and the respect for the rights of customers as individuals and data subjects. (This is what happened for example in the high-tech sector in the US, when, after the 2001 collapse of the market, some of the firms redefined themselves as socially responsible for-profit companies or social enterprises.) Concurrently, we can discern the outlines of another, unfavorable tendency as we witness the controllers of information in the public sector join efforts with their private-sector counterparts vis-à-vis the citizen, whose position in its citizen-type transactions begins to look increasingly like that of the customer as a result. Examples of this tendency can be found in the outsourcing of public functions, including the processing of personal data concerned, or in the cooperation of state registration systems and private insurance companies.

In 2004, Hungary's data protection law made it mandatory for a variety of organizations processing personal data to appoint their own internal privacy officers. Courses have been held to prepare them for this task. Some of these officers continue to fulfill a largely symbolic function, but the strongest among them are successful in raising the level of privacy awareness and know-how in their organizations. This trend is expected to pick up speed in the near future, aided in part by the limited but highly professional practice of voluntary data protection audits. These audits are conducted by specialists at the request of large banks, insurance companies, direct marketing firms and other data controllers in the public and private sector, including the Government's Portal.

In the business sector, privacy performance is strongest among companies with a mother company headquartered in a foreign country with strong privacy laws. For example, German-based businesses tend to improve the corporate culture of privacy within their Hungarian subsidiaries. German ownership in big telecommunication companies like Magyar Telecom has a similar effect. Specialized training also makes an important contribution. Although information technologists usually side with the data processors, they can be quite

privacy conscious if exposed to the values of privacy in the course of their studies. Any curricular item they have to master in this field, including Privacy Enhancing Technologies (such as anonymous browsers to be used by internet users) and IT solutions to be adopted by data controllers (such as segmented access control to customers' personal data), will indirectly shape their mentality, conceptual framework, and work as developers.

The ways in which personal data are handled in the public sector will undergo significant changes with the realization of the visions of e-government, the rising number of public services available through the internet, and the increasing use of the universal client gate. Such a virtual gate where the citizen enters the sphere of electronic governmental services, without proper rules of handling personal data, can lead to a situation in which government offices interchange and use citizens' data without citizens' awareness and control over the fate of their data. Happily, the agencies currently in charge of developing e-government services have displayed a healthy attitude to privacy concerns. Admittedly, though, the right attitude in itself will not guarantee the acceptable implementation of these systems.

In the international arena, we can expect the US, NATO, Europol and other intergovernmental organizations to step up pressure on Hungary and other new European democracies to appropriate their citizens' data and to place restrictions on their citizens' informational rights. The main areas are mandatory data sharing with foreign law enforcement agencies, data retention as well as monitoring of private communications such as mobile calls or emails, and broadening of the sphere of classified information. We have already seen the signs of policy laundering. This is the process in which measures that would be disqualified by the constitution and legal system of a democracy are first exported to an international organization, then subsequently re-introduced for domestic use. Such an attempt could be experienced in early 2005 at the so-called Salzburg Forum, the gathering for the cooperation of six Central European countries in the area of home affairs. At a Forum session Hungary submitted a proposal in order to remove obstacles to the use by the police of the EURODAC database, which contains the personal data and fingerprints of refugees and illegal migrants. Such a proposal would be surely disqualified under Hungarian law but there is much more chance to introduce it through the EU. This tendency is going to continue in the future.

There are also home-brewed attempts in Hungary at restoring the old, centralized personal information regime. To give one notable example, the Hungarian Academy of Science has set up an ad hoc committee which actively promotes such a restoration. Its members include representatives of government bodies with vested interests in concentrating data processing capabilities (among others, to stimulate more extensive use of their e-government services), as well as private companies steered by information technologists

who used to work for the Ministry of Interior and continue to accept contracts from the government, and finally a few scientists whose field of specialization and ideology have to do with the ‘wiring’ of the planet. The barely disguised ambition of this committee is to bring back the old universal personal ID code, and ultimately to render the data of every citizen free prey to all organizations, public or private. It seems unlikely that these efforts will succeed. But it would be foolish to underestimate the forces the committee has managed to mobilize, or the powerful political and business interests behind them.

In Hungary – as in other countries that overhauled their political systems in the first wave of democratization in the region – the euphoric elation and momentum of metamorphosis is now spent. This marks the end of boom in the respect for individual rights, including informational ones. László Majtényi, the country’s first DP&FOI Commissioner, once bitterly observed that ‘The constitutional revolution in Hungary has failed.’ While I would hesitate to go this far myself, I concede that a new, much more technocratic generation has grown up for whom career, profit, business, and political power all take precedence over respect for individual rights, most notably those concerning the uses of information.

For the years ahead, I predict that new business solutions and e-government strategies based on the latest information and communication technologies will continue to redefine the nature and the scope of the ongoing debate – or should I call it struggle – over the handling of personal data. This is precisely why it would be vital for this new generation to permanently embrace the values of privacy. Only then can we ensure that these values will be reflected back upon us by the data processing systems of the future and the ways in which we will elect to use them.

## 7. Republic of Korea

### Whon-Il Park

---

South Koreans are familiar with the words of a song, 'My RR Card'. In 1997, a Korean rock singer roused sympathy by the following lines:

Korean citizens hold RR cards  
I'm bearing in mind 800216-1068312  
This number is more important than my name  
Engraved in my head  
The number will be alive until I die

Without the resident registration card, South Koreans have trouble getting inside government buildings, or applying for financial transactions and website membership. Sometimes they are asked by policemen to show the identity card on the street.

Transsexuals have more troubles with these cards. While the first group of the resident registration number means the birthday (yy/mm/dd), the following seven digits denote the sex and residential information of the holder. So it is troublesome to hold a card which shows a different sexual identity from his/her appearance. Some transsexuals filed a lawsuit with the court to change the sex digit, but only a few succeeded. Until June 2006, when the Supreme Court approved the change of sex in the family census registry, judges would not have allowed such change.

### HISTORY OF PRIVACY PROTECTION

At first, holding the resident registration card was mandatory for the purpose of national security. But the situation has drastically changed in the past 40 years. With unparalleled economic development and democratization of the Korean society, the resident registration number is no longer indispensable to protect the country. On the contrary, it could be a Big Brother's weapon. The fate of this number illustrates the changing view of privacy in South Korea. Initially introduced for national security, the number is now regarded as a potential threat to privacy.

## **Conflict between Liberty and Security**

With the end of the Japanese occupation (1910–45), South Korea adopted liberal democratic ideas. But the Korean War broke out in 1950 and divided the Korean peninsula. After a brief and tumultuous democratic interlude in the early 1960s, Korea's politics were dominated by a series of military strongmen (Ginsburg 2004, pp. 2–3). This authoritarian period nevertheless had a silver lining of rapid economic development.

From the late 1960s until the 1980s, North Korea staged occasional terrorist attacks against South Korea. In January 1968, North Korean guerrillas infiltrated to the outskirts of the Blue House, the Presidential residence in Seoul. A few days later the *Pueblo*, an intelligence ship of the US Navy, and all its crew, were seized by North Korean patrol ships in international waters. The North Korean regime continued to terrorize their South Korean brethren by hijacking a private airplane in 1969, and directing a Japanese agent to assassinate President Park Chung-Hee and First Lady in 1975. In 1983, they attempted to kill President Chun Doo-Hwan on his state visit to Myanmar. In 1987, North Korean terrorists destroyed a Korean airplane with 115 passengers and crew flying over the Indian Ocean to stymie the Seoul Olympic Games.

Perhaps Korea's threatening geopolitical reality justified some restriction of fundamental rights for the sake of national security. However, the restriction of freedom went too far. Throughout the 1970s, President Park proclaimed a series of Emergency Presidential Decrees to restrict fundamental rights ostensibly to protect the state from the North Korean threat. But, in a real sense, President Park's political action was oriented to continue his dictatorship.

## **Struggle for Democratization**

Mounting demand for privacy protection generated pressure on the Korean government to respect the constitutional rights. In 1987, the democratic movement, known as the 'June Struggle', changed the political landscape. It made the authoritarian regime comply with citizens' constitutional rights. Confronted with student protests against the iron fist rule of President Chun, the general-turned-President allowed a broad liberalization. The international environment was a crucial factor in his decision to democratize the nation (Ginsburg 2004, p. 4).

Meanwhile, military tension between North and South eased in the midst of East–West rapprochement. The 1988 Seoul Olympiad focused the international spotlight on the daily life of ordinary Koreans. Rights of Korean dissidents attracted worldwide attention. In 1996, Korea was admitted to the

Organization for Economic Cooperation and Development (OECD). To secure admission, South Korea promised to observe human rights. At that time, its per capita income exceeded \$10,000. In the wake of the rising prosperity of the late 1980s, human rights issues came to the foreground of public opinion.

The advent of the Information Age has opened a new dimension of privacy issues. The information highway has made it possible for the government to implement far-reaching e-Government projects. For example, the government planned to consolidate relevant information in the public sector, and to provide on-line administrative services to citizens. At the same time, popular curiosity has found all sort of new outlets, including celebrity scandals now detailed over the internet.

### **Full Bloom toward a Ubiquitous Society**

Since the early 1990s, 'ubiquitous computing' has become one of the most frequently-used words. The government took an initiative to establish the nationwide computer and communications network in such areas as government administration, banking and finance, education, R&D and national defense.

According to a survey by the Ministry of Information and Communication (the 'Communication Ministry'), 31.6 million people over six years of age use the internet. This means that virtually all Koreans have access to cyberspace. Korea boasts the highest distribution rate of internet broadband networks in the world (*JoongAng* 2005). Over 70 per cent of Korean households subscribe to high-speed internet services. The Information Age has brought to Korea significant improvements in the efficiency and convenience of living. The 'nationwide internet breakdown' on 23 January 2003, when the Sapphire/SQL Slammer worm computer virus paralyzed nationwide administrative and banking operations through national key networks for half a day, illustrated how dependent Korea has become on the internet.

Information processing equipment and facilities are distributed and used everywhere including homes, work places, schools, transportation, communications, finance, sports and games, just like the nerve center of a body. Ordinary Koreans enjoy the benefits of high-speed internet services, but they also demand that the government be concerned about privacy issues involved in the use of this new technology. As for the ubiquitous computing, government officials and specialists are eager to develop some useful guidelines to prevent the abuse and misuse of such sophisticated technology.

### **Overview of Privacy Protection Laws**

South Korea's privacy protection legislation has been established by sector. The public sector, where the resident registration number was generally used,

had urgent need of data protection law while privacy protection in the private sector was implemented on a case-by-case basis.

The Public Agency Data Protection Act of 1995 governs the government's collection of personal information in accordance with the OECD Guidelines on privacy protection. This Act applies to all public institutions, government departments and offices in the Administration, the Legislature and the Judiciary as well as local governments, various schools, government-owned companies, and public sector institutions. Accordingly, in the public sector, privacy protection provisions are found in the Act on Communication Secrets, the Telecommunications Business Act, the Medical Services Act, and the Public Agency Data Protection Act, among others. Because an OECD member state is required to observe OECD rules, the Korean government adopted the OECD Privacy Principles.

In the private sector, the Credit Information Act, the Framework Act on Electronic Commerce and the Electronic Signature Act contain data protection provisions. For example, the Framework Act on Electronic Commerce requires that electronic traders shall not use, nor provide to the third party, personal information collected through electronic commerce beyond the notified purpose for collection without prior consent of the data subject or except as specifically provided in any other law.

Among others, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the 'Data Protection Act' as amended in 2001) generally applies to entities or individuals that process personal data for profit through telecommunication networks and computers. Personal credit information and medical records are protected by other legislation.

### **Public Sector Privacy Legislation**

The Public Agency Data Protection Act sets the norm for the management of computer-based personal information held by government agencies. Under this Act, government agencies are required to limit data collection, ensure the accuracy of data, keep public registers of data files, ensure the security of the information, and limit use of personal data to the purposes for which they are collected. Only computerized data fall within the scope of this Act. Manually collected information may be protected by the Criminal Code and other relevant laws, which require public servants to maintain confidentiality in administrative work.

Personal information maintained by public agencies, whether computerized or not, is also governed by the Act on Disclosure of Information by Public Agencies, South Korea's freedom of information act. But if the information affects another individual's privacy, the public agency must

decline to disclose it. The data subject is also entitled to request necessary modification of defective government-held data (Constitutional Court 1989).

The Public Agency Data Protection Act is enforced by the Ministry of Government Administration and Home Affairs (the 'Administration Ministry') responsible for government administration and police affairs. The Administration Ministry must be informed in advance of what kind of personal information files are maintained in each office by the head of competent agency, and it must publish the list of such personal information files more than once a year in the Official Gazette. The Administration Ministry may request the pertinent public agency to submit the personal information processing report, permit its employees to inspect the actual conditions, and give suggestions or advice on how to protect personal information effectively.

Critics of this Act say that there are few provisions to prevent excessive collection of information by public agencies. In addition, there are overall exceptions to the application of this Act with regard to agencies like the National Intelligence Service (NIS) and other law enforcement bodies. And there is no guarantee of independence of the oversight body in the Administration Ministry and the Personal Information Protection Deliberation Committee under the Prime Minister.

Surprisingly, it was disclosed in early 2005 that NIS, a Korean CIA, had collected personal information without court permission. According to news reports, NIS secretly eavesdropped on conversations of 1800 politicians, journalists, government officials and businessmen in a 24-hour-a-day operation during the period from 1998 to 2003. Public opinion demanded a special prosecutor to investigate the case. As a result, the former heads of the nation's intelligence agency were arrested in November 2005, and sentenced for illegal wiretapping (*JoongAng* 2005b).

## INCREMENTAL INFLUENCE OF PUBLIC OPINION

Over the past two decades, public opinion has played a leading role in democratization of South Korea. Government disregard for citizens' privacy has been the target of criticism by the press as well as civic organizations. The internet and cellular phones play an effective role in mobilizing public opinion. The power of public opinion comes from the keyboards of netizens or the thumbs of mobile phone users based upon Constitutional rights. In the same way as they gathered to support the Korean football team in the 2002 FIFA World Cup, Korean people often gather in front of Seoul City Hall at night to declare or protest something important with candle lights.

## **Constitutional Ground for Privacy Disputes**

The Korean Constitution provides for the general protection of privacy (Art. 17), and specifically for the protection of privacy of home (Art. 16) and in communications (Art. 18). The Constitution also affirms that freedoms and rights of citizens shall not be neglected on the grounds that they are not enumerated in the Constitution (Art. 37(1)). These protections can be abridged in exceptional circumstances: freedoms and rights of citizens may be restricted by the law only when necessary for national security, law and order, or public welfare. Even when such restriction is imposed, essential aspects of the freedom or right shall not be violated (Art. 37(2)). It means that the utmost need to enhance the administrative efficiency cannot justify the infringement upon the privacy of ordinary citizens.

In 2003, the Constitutional Court made a noteworthy interpretation of these provisions:

The right to privacy is a fundamental right which prevents the state from looking into the private life of citizens, and provides for the protection from the state's intervention or prohibition of free conduct of private living. Concretely, the privacy protection is defined as protecting and maintaining the confidential secrecy of an individual; ensuring the inviolability of one's own private life; keeping from other's intervention of such sensitive areas as one's conscience or sexual life; holding in esteem one's own personality and emotional life; and preserving one's mental inner world. (Constitutional Court 2003)

The data protection rule is to protect the data subject from inappropriate access to, and abuse or misuse of, its personal information. Personal information is understood to mean the data of a living person comprising sign, character, voice, sound and image, and so on, which may be used solely, or together with other easily combined data, to identify the data subject by means of a name, resident registration number, and so on. With the advancement of information technology, the scope of such information increasingly expands to include email addresses, credit card numbers, log files, cookies, GPS location data, DNA data, etc. In this connection, individual belief, conscience, medical records, sexual orientation, race, trade union activities and criminal records are regarded as sensitive data.

## **NEIS Controversy Defeating e-Government Project**

The biggest recent privacy struggle between the government and the public was regarding the National Education Information System (NEIS), a scheme proposed in 2003. This plan ostensibly aimed at enhancing the efficiency of educational administration and improving teachers' working conditions. The

Ministry of Education and Human Resources Development (the 'Education Ministry') asserted that NEIS would be an efficient, technologically advanced and transparent system.

NEIS sought to centralize personal data of about eight million students from 12,000 primary and secondary schools across the country in a national broadband network. Twenty-seven categories of personal information were to be consolidated in NEIS servers maintained by local education agencies. NEIS was supposed to include data on students' academic records, medical history, counseling notes, and family background. Even data on teachers' trade union activities were to be held by the Education Ministry.

The National Teachers' Union (NTU) opposed the system. It and other civic organizations conducted protest rallies and threatened a general strike. Disappointed by the lukewarm response of the government, they brought an action with the National Human Rights Commission. The enhanced efficiency in information sharing offered by NEIS was depicted as a potential risk to privacy. The Commission recommended that three of 27 categories of personal data be excluded from the NEIS databases.

Accordingly the Education Ministry excluded these three categories of data, keeping other 24 categories of school affairs intact. While NTU threatened to stage an all-out protest against the implementation of NEIS in November 2003, the Seoul District Court approved a motion to block the use of NEIS data-contained CDs of three high school students. As a result, the Education Ministry was prohibited from distributing useful student data from the NEIS necessary for the application for the college entrance exam. Because NEIS data-contained CDs regarding applicants were indispensable to the processing of the on-line college entrance applications, such a negative court order could paralyze the whole college entrance exam procedure. In December 2003, the government decided to separate the sensitive data from the NEIS databases and to operate them in different computer systems.

In July 2005, the Constitutional Court held that such personal information as the graduate's name, birthday and graduation date, contained in the NEIS databases, are necessary for the administrative purposes of the Education Ministry. Consequently, pertinent schools and institutions are able to issue certificates of graduation at any time by accessing the NEIS database. So the current NEIS databases were found to comply with the Constitution and the relevant laws on data protection, and could be maintained (Constitutional Court 2005).

### **Changing Concept of Privacy**

In South Korea, the right to privacy is a developing and unfinished concept. For one thing, the right to privacy and the freedom of expression are both

fundamental rights; and there is no priority between them. So we have to compare and analyze the competing legal interests when they are infringed upon. The Korean Supreme Court held:

In a democratic state, it is common to form a majority opinion by means of free making and exchange of one's expression, thereby maintaining the democratic political order. So the freedom of expression on a public issue shall be protected as a constitutional right, but the right to privacy or the individual reputation and secrecy shall be ensured as much. The conflict between the right to privacy and the freedom of expression should be settled and adjusted in a concrete case after comparing the interests in a social environment protected by the respective right or freedom, and the extent and method of regulation should be determined accordingly (Supreme Court 1998).

Secondly, once privacy is violated, the damage can be difficult to repair. When celebrities' privacy is violated in a scandalous news story, their loss of privacy becomes a *fait accompli* regardless of the truth. Because a forced apology to cancel the former privacy invasion or the publication of the opposite opinion could exacerbate the infringement upon privacy, injunctive remedies are more generally granted than in the case of defamation (Sung 2003, p. 88).

## NATIONAL CULTURE AND TRADITIONS

Traditionally Korean citizens have been accustomed to authoritarian rule. More recently, they have grown aware of their fundamental rights. Though they are required to use the resident registration number in daily life, they have come to understand the negative aspects of information society, that is, abuse or misuse of personal information. As South Korea has become more democratic, civic groups have been very active in demanding privacy protection from the government and IT businesses. In response to such demands, the Korean government has implemented a unique remedy system that provides pecuniary compensation to alleged privacy victims.

### **Pros and Cons of General Identifier**

Although 'Asian Values' allegedly contributed to economic growth, they functioned as a stumbling block to democratic developments. Since the Korean War in the early 1950s, Korean rulers favored national security and economic growth over human rights. But democratization changed the situation dramatically. A good example is the ID system.

As mentioned before, in South Korea, every citizen is given an ID number at birth – the resident registration number. This number contains 13 digits

conveying information about the holder. This ID system was generally implemented just after the armed guerrilla attack in January 1968. Now the ID number is used for administrative purposes, from applying for various government services to proving that one is a real person with a real name. As a result, someone with access to administrative databases associated with use of the card can gain detailed information about where its holder is living, how much he earns and pays in tax, and what kind of business he is engaged in. It is because the residence, tax and other government databases are constructed based on this general identifier.

The resident registration number functions as a link to government-maintained databases. This number makes it possible for government officials to compile personal information and to do profiling and data matching of extensive information about Korean citizens. The 13-digit number is like 'Aladdin's sesame' to open government databases. Because it is easy to centralize and profile citizens' data, privacy-conscious South Koreans seek assurances that the ID number is not used for purposes of surveillance (Sung 2003, p. 94). Several civic groups have acted as watchdogs against government plans to establish and consolidate databases for administrative efficiency.

In the private sector, on-line information service providers usually demand users' resident registration numbers. To protest this practice, some users submit made-up numbers instead of real ones; others steal someone else's ID number. For example in 2005, 53.9 per cent of those who filed claims with the Personal Data Protection Center in Seoul reported their ID numbers had been illegally used or stolen (PIDMC 2006, p. 50). Against this backdrop, some critics suggested that information service providers should not be allowed to collect individual users' ID numbers (Chung and Kim 2004).

### **Real Name Required for Financial Surveillance**

Throughout the 1990s, the Korean government took the initiative in protecting citizens' privacy both by law and in practice. But civic organizations were not satisfied with these measures. They demanded reinforced security measures for individual privacy including credit information.

Take an example of the Real Name Financial Transaction System, which sought to ensure that financial transactions are conducted under real names. It meant that no one could open bank accounts without disclosing his or her name and resident registration number. Until the early 1990s financial transactions of large amounts between private parties had usually been conducted under false names or pseudonyms to protect the confidentiality of such transactions and to evade tax as well.

In 1993, President Kim Young-Sam suddenly proclaimed his Emergency Presidential Order on Real Name Financial Transactions and Protection of

Confidentiality. The newly-elected President Kim sought a clean image by enforcing the conduct of all financial transactions under real names. It was believed that former Presidents Chun Doo-Hwan and Roh Tae-Woo had concealed their slush funds under false names or pseudonyms. If concealed financial transactions could be exposed by means of the real name transaction system, a remarkable increase of tax revenues should result. This regulation aimed at keeping the underground economy under tight control by making all transactions subject to taxation. The Presidential Order was transformed into the Act of the same name in December 1997.

The real name financial transaction system required everyone to submit such certificates as the resident registration card, driver license or passport evidencing his or her real name before completing transactions with financial institutions. The subsequent surveillance effect was bigger than expected. In November 1995, ex-Presidents Chun and Roh were convicted and jailed for accumulating and concealing huge slush funds while in office and violating the Presidential Order.

The Act prevented banks and other financial institutions from informing third parties (for example, creditors, tax collectors, investigators, and so on) of any financial transaction involving banks, savings, securities companies and insurance companies without a request or the consent of the data subject. There are some exceptions where personal information is required under subpoena or warrant, or required by law for a tax inquiry under tax laws, etc. In July 2001, three large credit card companies were fined under the law. The companies were found to have disclosed personal information on their customers (including bank account numbers, salary, credit card transaction records, customer names, addresses, phone numbers and resident registration numbers) to insurance companies without telling their customers or obtaining their consents in advance (*Korea Herald* 2001). Those credit companies were affiliated with the insurance companies under the same business group.

### **Crimes Abusing and Misusing Personal Identity**

The identity card or NEIS systems are loaded with personal information, opening the possibility of many crimes and abuses. After the financial crises in 1997, a wave of identity crimes broke out. Criminals found ways to use affluent people's personal data to commit fraud or burglary. The original NEIS was dangerous because it disclosed students' family wealth and other information which could be used illegally by criminals.

In the 2000s, some burglars were reportedly tracking foreign-made luxury cars with certain motor vehicle registration plates. Initially the plate number showed the registration place of the garage. Once, robbers threatened a female driver when she parked her car at an isolated parking lot at night. In 2004, the

government hurried to change the format of private car plates to omit information on the owner's place of residence.

### **Privacy Agency Providing Pecuniary Remedies**

In Korea, financial penalties pay for the protection of privacy. The Korean Personal Information Dispute Mediation Committee (PIDMC) provides financial compensation to individuals whose statutory privacy rights are found to have been infringed upon by merchants. In 22 cases reported by PIDMC during 2003–04, the committee awarded compensatory damages in 17 cases where a breach of privacy rules was found. Damages ranged from US\$100 to US\$10,000 (see PIDMC 2005). A mere misuse of personal information case, for example, reckless disclosure of personal data, usually results in compensation of around US\$100. The more serious the privacy invasion is, the more compensation is required. In only a few cases of breach did PIDMC recommend corrections or other remedies without any payment of compensation.

A woman specifically requested her mobile phone company not to disclose details of her telephone calls to anyone else. Then she found that a branch of the telephone company had nevertheless disclosed them to her ex-husband, who had produced a copy of her ID card when applying for the details. The mobile phone company was held responsible for professional negligence, and she was awarded 10 million won (equivalent to US\$10,000) in compensation for the economic and mental damages.

In another case, a plastic surgeon displayed a movie of a patient's operation on his clinic's website. He was required to pay 4 million won (around US\$4000). The award would have been increased if she had objected to it during the filming. A translation service company posted a woman's resume on its website without her consent, as if she was an interpreter employed by them; the company was required to pay 200 thousand won (around US\$200) compensation. An insurance company that provided a person's personal information to another company so that they could solicit business from him was required to pay 200 thousand won (around US\$200). Taking into consideration monetary compensation, Korea's privacy authorities regard privacy violations more seriously than any other data protection agency in the world. We will see later how this unusual privacy agency is doing its work.

Recently pecuniary remedies have seen a different dimension of incidents as Korean-made on-line games are getting popular cross the border. In April 2006, the Seoul Central District Court held that NC Soft of Lineage II should pay 500 thousand won (around US\$500) each to the plaintiffs. The court said that game site operators obtaining commercial profits from many users have a duty of special care to protect the personal information of customers. Though actual damage could not be identified, the defendant should pay damages on

account of a gross negligence or fault that it did not preserve users' personal ID and password by encryption and caused the personal data to be stolen by other customers (Park 2006b, p. 12).

### **Lackluster Self-regulation of the Private Sector**

Self-regulation does not work well in South Korea. Take the example of the Half Price Plaza, an on-line shopping mall. The internet shop owner ran aggressive on-line advertisements, promising its members half price on a number of items. In the end, the owner ran away with customers' deposits. This case rang an alarm bell that on-line shopping malls are not always safe and credible.

One semi-official form of self-regulation was established under the Data Protection Act. The Korea Association of Information and Telecommunication (KAIT, [www.kait.or.kr](http://www.kait.or.kr)), a private entity supported and supervised by the government, started its operation in 2000. KAIT regularly awards the Privacy Mark to internet sites and on-line businesses voluntarily engaged in data protection on an appropriate level. KAIT established an association composed of chief privacy officers (CPOs) in charge of personal information of customers. The organization is to enhance work ethics and awareness of privacy protection, to provide educational and training programs to member companies, and to formulate self-regulatory guidelines by industry.

Although the Data Protection Act does not otherwise stipulate industry-wide self-regulation, it is possible for any entity to implement self-regulatory measures (see Yi and Ok 2003). For example, the Association for the Improvement of E-Mail Environment was established in 2002 by direct marketing merchants as its members to cope with increasing citizens' dissatisfaction with spam and direct marketing mails, as well as improving the internet-based business culture and coordinating the interests of its member businesses.

## **WINNERS AND LOSERS**

The privacy issue on the internet has produced apparent winners and losers. The Korean government has successfully implemented e-Government services via high-speed internet. Today ordinary citizens can process administrative applications at home by using their own home computers. However, the government had to admit some side effects of e-Government when the civic organizations successfully protested against the NEIS.

Privacy concerns have consistently helped swell the numbers of supporters of activist civic organizations. As a result of slush fund investigation, financial

information of the individual is more often than not disclosed because of bribery investigation, tax examination or health insurance fraud, while credit information is firmly protected by a special law.

### **Increasing Activism of NGOs**

In the 1990s, politicians who had earlier been persecuted by military rulers gained power through democratic elections. Civic organizations friendly to such politicians as Kim Young-Sam and Kim Dae-Jung received handsome government support. Since the mid-1990s, these organizations have helped liberalize public policy making in South Korea by participating in various government committees and by shaping public opinion. The Korean political pendulum has made a full swing from the authoritarianism of past decades to today's free society. Civic groups have usually rated privacy issues very high – in contrast to the authoritarian rulers who deemed national security and economic growth as superior to human rights. They provide advice on privacy issues to individuals as well as businessmen, and conduct monitoring of market practices.

One of these groups is the Citizens' Action Network (CAN, [action.or.kr](http://action.or.kr)) – a non-profit NGO which encourages citizen action to reinforce the rights of ordinary taxpayers and consumers by the voluntary contributions of its members. CAN focuses on information-related rights maintaining an internet bulletin board regarding privacy invasion. Anybody can report to it such incidents as spam mails, unauthorized use of resident registration numbers and location information, closed circuit televisions (CCTVs) installation for monitoring, and so on. CAN advocates a comprehensive data protection law applying to both the public and private sectors.

People's Solidarity for Participatory Democracy (PSPD, [www.people-power21.org](http://www.people-power21.org)) is also dedicated to justice and human rights and to legal and policy reforms. Since its establishment in 1994, PSPD, with 13,000 members as of 2005, has been serving as a watchdog against the abuse of power. It has staged public awareness campaigns, particularly in the area of privacy. PSPD has kept an eye on possible violations of privacy protection provisions by major industries. In 2003, PSPD claimed violations of the Data Protection Act by cellular phone companies, and filed suit for the deletion of such data and damages on behalf of over 4000 of their former customers.

The Korea Progressive Network Jinbonet (KPN, [center.jinbo.net](http://center.jinbo.net)) is an activist network seeking enhanced human rights, anti-censorship and free use of copyright in cyberspace. Occasionally it staged a campaign 'e-Government hand-in-hand with Information Human Rights!' which addressed the problems of the resident registration number and NEIS. They demanded that installation of such systems as CCTV, software for monitoring emails or internet usage,

biometrics devices, smart cards and location detectors should be subject to the prior consent of the laborers or trade unions.

These civic organizations all support a campaign to replace the resident registration number with alternative IDs. They held various 'Be-Aware-of Big Brother' events around 25 June 2004 which marked the centennial anniversary of the birth of George Orwell. At one meeting of the centennial event, they debated on how to preserve human rights in a digital environment. In 2003, they succeeded in delaying the nationwide implementation of a real name check on the internet bulletin board, in which the government wanted to prevent users with a false name or non-existent resident registration numbers from posting any message or idea.

### **Protection of Credit Information and Slush Funds Scandal**

In a privacy-friendly world, personal account information should be held confidential from others including the government. However, demand is growing for surveillance of transactions in the private sector as a means of reducing tax fraud and health insurance cheating. Government-maintained data matching is often called for to detect tax fraud.

Initially, individual credit information had no privacy protection. In the 1990s, the partially disclosed slush money of former presidents changed the course of data flow. Investigators found the hidden transactions of ex-President Chun exploiting the underground economy. In order to avoid a run on the bank by ordinary people in fear of all-out tax examination, the government had to promise banking secrecy to individual depositors.

Consumer credit information has been protected separately by the Credit Information Act since 1995. Individual credit information, positive or negative, including bank accounts and transaction details may be used to decide to create or maintain financial transactions with the data subject. There are exceptions where credit information might be provided for other purposes with written consent of the data subject; under subpoena or warrant; for an inquiry under the tax law; or in accordance with other laws.

Consumers who feel their credit information has been misused by distrustful employers and landlords may claim damages against the credit information processor or users. In proceedings, credit information processors or users are required to prove the absence of intention or negligence. The Korean Financial Supervisory Service, a half governmental credit information watchdog, is empowered to supervise the operations of credit information companies. At present, credit information is protected separately from ordinary personal information, but in a manner consistent with core OECD privacy principles.

## **KISA's Activities as Privacy Guardian**

Under the Data Protection Act, data subjects can demand access to their personal information, insist on correction of false information and challenge wrongful information. Collection of personal information should be minimized within the scope of purpose, and the collection and processing of data must be subject to privacy-related laws and regulations.

The Data Protection Act creates a guardian for privacy protection and security, the Korea Information Security Agency (KISA). KISA was established in 1996 to ensure information security and safety. It seeks to develop information security technology and policy research on information security. KISA has conducted surveys of compliance with privacy protection provisions in such areas as mobile communications, on-line shopping malls, banking and financing, department stores, accommodation, traveling, etc. It also monitors whether websites provide for the presence of a chief privacy officer, clarification to users of the purpose of collection and use of personal information, permission for access to the collected data and necessary modifications, the duration of maintenance of such information, and so on.

During 2005, KISA documented 3982 violations of privacy rules in a survey of 27 thousand businesses. Among these were unauthorized use of personal data and collection of children's data without parents' consent. Though the overall compliance ratio in 2005 was slightly over 80 per cent, KISA encouraged the information and communication businesses to implement technological and managerial safeguards of privacy including the adoption of Privacy Enhancing Technologies (PETs). It strongly recommended new guidelines on RFID privacy protection (Korean Briefing 2006), which came into effect in 2006.

## **Resolution of Privacy Complaints**

South Korea has developed a unique method for resolving privacy complaints in the private sector, including a combination of government agency (KISA) investigation and alternative dispute resolution (ADR) with a possibility of litigation.

Under the Data Protection Act, anyone aggrieved in data protection matters may file his or her case with the Personal Data Protection Center (PDPC) within KISA. KISA has operated a secretariat of PDPC since April 2000. The purpose of the Center is to handle complaints regarding data protection, to monitor market practices, and to provide advice on various queries. The Center investigates complaints and provides advisory corrective measures in case of minor violations. It also assists complainants in more serious cases to petition the Personal Information Dispute Mediation Committee (PIDMC). In

more serious cases, the Center notifies the Communication Ministry, police and prosecutors' office of violations or incidents.

Many observers hold that the legal status of both the data protection oversight body (PDPC) and the dispute settlement body (PIDMC) should be more independent. Lawmakers and civic groups also demand that the Data Protection Act be modified so as to secure the extended applicability of the Act into the public sector, which has been regulated by the different law and governmental entity, and the institutional independence of the oversight body.

### **Functions of the Dispute Mediation Committee**

Recently, an increasing number of plaintiffs in Korea have been resorting to alternative dispute resolution (ADR) – arbitration or mediation. Regarding the privacy issue, a separate dispute settlement body has been established under the 2001 amendment to the Data Protection Act, because disputes related with privacy could not be settled by the same procedures as e-commerce or consumer protection disputes.

If a privacy complaint cannot be readily resolved by the Personal Data Protection Center (PDPC), the injured party may file a petition with the Personal Information Dispute Mediation Committee (PIDMC). PIDMC is intended to facilitate the prompt, convenient and appropriate settlement of disputes arising out of personal data or privacy infringement. The Committee is composed of up to 15 members, appointed or commissioned by the Minister of Information and Communication from among well-qualified lawyers, IT engineers, professors, representatives of consumer organizations and IT businesses, whose term, integrity and professionalism are ensured by the Data Protection Act.

Dispute mediation proceedings may be initiated by either an injured subject or the on/off-line information service providers, and are settled free of charge. When a petition for mediation is filed with PIDMC, the Committee opens factual investigation in an informal way and proposes a settlement for agreement by the parties prior to formal mediation. If the parties fail to agree upon a settlement, PIDMC starts the mediation proceedings. After fact finding efforts through hearings, discoveries and experts' examinations, the Committee suggests a mediation proposal for an agreement by the parties within 60 days from the filing of petition. When both parties say 'yes' to the draft mediation with moderate compensation to the applicant within 15 days from the proposal, and execute the mediation record, the mediation becomes legally enforceable like an out-of-court settlement. Otherwise, each party may file a civil suit with a competent court, and the Committee may support the data subject to conduct the court proceedings with reliable evidence and its own findings. In other cases, the parties may go directly to court.

PIDMC is supported by the Secretariat within KISA, which receives petitions for dispute mediation, conducts the factual investigations, prepares the agenda for the Committee meetings and keeps its minutes. PIDMC plays an important role in protecting individual privacy in the cyberspace. As an alternative dispute settlement body, it is swift and efficient in rendering pecuniary compensation to privacy victims subject to the agreement of parties concerned.

## INFORMATION FLOWS AND CONSTRAINTS

Recently celebrities have generated more than their share of privacy controversies. Ironically public appetites for sex scandals and gossip about entertainers has contributed to the popularization of high-speed internet services. The resulting incidents have contributed to the improvement of privacy legislation in the private sector.

### **Extreme Cases of Internet Exposures**

In 1999 and 2000, the high-speed internet networks circulated pornographic videos of Ms Oh, an actress, and Ms Baik, a Korean pop singer, apparently without the entertainers' consent. Such incidents have sparked debates in South Korea. Which is the first and foremost between the individual right to privacy and the freedom of expression or citizens' right to know? Most journalists, NGO activists and academics preferred privacy to freedom of expression, and demanded effective countermeasures.

An unprecedented sensational case culminated when the so-called 'Entertainers' X-File' prepared by a research group was disseminated through an internet messenger program like MSN to the public in January 2005. The file, initially prepared for an advertisement agency, contained unconfirmed rumors and personal details of 99 entertainment celebrities. Some of these celebrities considered lawsuits against the agency, seeking damages over unauthorized release of such sensitive data.. At that time, a standing committee of the National Assembly held public hearings on how to ensure the effectiveness of a newly proposed amendment to the Data Protection Act. The participants agreed on the entertainers' right to privacy. They considered such issues as the need for consolidated data protection legislation of both the public sector and the private sector, the absence of an independent oversight body and the permissible extent of collection of personal information by private companies.

In another case, the tale of the 'Dog-Shit Girl' showed the extraordinary power of netizens. When a young lady refused to clean up after her dog in a

subway train, this scene was captured by another passenger with a digital phone camera. These photos were posted on internet bulletin boards. The homepages showing the 'Dog-Shit Girl' were bombarded with hits from netizens criticizing her action. It was like a kangaroo court, and nobody seemed disturbed about the violation of the young woman's privacy.

In January 2006, the Seoul Prosecutors' Office signaled its impatience against such netizens. This time their victim was not an entertainer. Ms Lim Su-Kyung, a former student activist who visited North Korea without government approval in 1989, lost her son in an accident. At that point, 20 or so netizens including college professors and bank officers attacked her, denouncing her as a 'red' and ridiculed her son's death. The prosecutor brought them to the court by summary indictment without formal proceedings with fine up to one million won (around US\$1,000) each, on the count of defamation of Ms Lim.

Thanks to the explosive advancement of information technology, Korean citizens usually enjoy brand-new services like internet blogs, mini-homepages, on-line shopping, on-line games and chatting and so forth. But there is a dark side of abuse or misuse of personal information involved in these services, on-line defamation or personal assault among them. So far we have failed to find effective remedies or deterrents.

### **Private Sector Privacy Laws under Total Reshaping**

The division of data protection between the public and private sectors is not unique to Korea. The United States and Japan have similar set of rules (EPIC 2001, p. 4). In South Korea, the logic of these two sets of laws is quite different. State and local governments and public enterprises are seen as using personal information in the public interest, whereas the private sector is ruled by market forces and pursuit of private interest.

Since the mid-1980s, the Korean government has been building up information infrastructure in both the public and private sectors. The Act on the Expansion of Computer Networks and the Promotion of Its Utilization of 1986 was changed to incorporate the protection of privacy in a new chapter in 2001, and thus obtained the new name 'Data Protection Act'. This newly revised act sets out principles of data protection of notice and consent on the basis of informational self-determination (Schwartz and Reidenberg 1996, p. 36), the right of data subjects, the responsibility of information service providers, the possible remedies following the infringement on the personal data, etc. All these principles follow the OECD Privacy Guidelines (EPIC 2001, p. 202).

Initially these data protection provisions are applicable to on-line information service providers that use computer systems and communication networks. So this Act has yet to extend its scope of application to certain specific manual data processors that collect or use clients' data. These include

travel agencies and hotels, department stores, airlines, private schools or educational institutes; and other service providers which deal off-line with their customers' personal information.

In response to mounting pressure from civic groups, the Korean government made amendments to the substantive protections in the Data Protection Act in 2004 (Park 2006a, pp. 20–21). The data subject's consent is required for automatic data collection devices which extract email addresses from websites for the purpose of spamming, and data subjects have rights to know how their information was used or provided to third parties. The Communication Ministry may establish data security guidelines for information service providers. 'Spam breaker' software should be distributed by information service providers. The on-line information service providers are required to undergo an annual security diagnosis and audit by specified data protection consultants. The government can set standards for mandatory notices to affected data subjects, for example, in the event of security breaches. Information service providers are also required to obtain the consent of data subjects before they transfer personal information to foreign countries.

### **KISA and Other Authorities for Privacy Protection**

KISA plays various roles under the law, including performing the Secretariat of PIDMC; devising and developing technology and countermeasures to hacking and virus-related problems; operating a peak digital signature authentication agency to safeguard electronic commerce; evaluating a diverse range of information security systems; promoting information security industry; conducting R&D on cryptographic technology; developing system and network security technology; standardizing information security technology; and staging public awareness campaigns on information security.

KISA formulates mandatory guidelines for private businesses requiring them to take precise measures for privacy and security protection. KISA is unusual among world data protection bodies, in that it combines a significant role in privacy complaint resolution with high-tech functions in relation to computer security. In 2004, KISA was admitted as a member of the International Conference of Data Protection and Privacy Commissioners.

In legal terms, the responsibility to protect personal information is taken by the Communication Ministry and the law enforcement agencies. The Ministry is in charge of formulating data protection policy and implementing the Data Protection Act. The Ministry may issue corrective orders or impose penalties on identified violators.

Police and prosecutors are also involved in privacy protection. If the violation of data protection provisions is subject to the criminal punishment, then the police investigate, and court hearings and decisions follow with appropriate

penalties. In the Supreme Public Prosecutors' Office, the Internet Crime Investigation Center devotes itself to hacking and other computer incidents, internet-based fraud, and personal data protection violations. The Cyber Terror Response Center in the National Police Agency attempts to prevent any wrongdoing or misuse of personal data and internet-based criminal activities. A victim of privacy violations may have on-line or off-line access to the above-mentioned institutions, that is, KISA, prosecutors' office or police station.

### **Effectiveness of Law Enforcement in the Private Sector**

As the internet population surpassed 30 million in Korea in 2004 – over 70 per cent of the total population – conventional cyber-crimes including frauds in communications and on-line games decreased in numbers. But new types of cyber-crimes such as defamation on the internet or privacy invasion are on the increase.

For example, in March 2005, the lists of two million customers of CJ Home Shopping Co., a leading telemarketing company in Korea were leaked. According to police, a representative of a call center service company obtained the customer lists from a home shopping-related logistic company during several months of 2004. The lists contained customers' names, addresses, and telephone numbers.

KISA reported that internet users' complaints of privacy infringement in the private sector in 2005 amounted to 18,200, a 3.6 per cent increase over the previous year. Complaints against information service providers included failure to respond to users' withdrawal of consent; lack of any procedure for exit; unauthorized use of another's name, resident registration number or ID cards in cyberspace, and so on (PIDMC 2006, p. 50).

How is it that these privacy protection violations continue to take place even though the Data Protection Act prohibits such activities? Is it because the sanction or punishment is so light? Is it because such privacy invasion is an everyday occurrence in this Information Society? Perhaps it is because cyberspace has become an important part of our daily life. In the Information Age, personal information is not only an intangible asset but also a valuable item to be protected from outside attacks.

## **CONCLUSIONS AND PROSPECTS**

Though Koreans are using the high-speed internet, mobile phones and other digital devices every day, no one believes that users' ethics, usually called 'netiquette' in Korea, are satisfactory. Koreans have a long way to go to

improve their cyber-culture. As an information highway is completed, there must be appropriate traffic regulation.

### **Alternative ID System Wanted**

Nowadays, Koreans are eager to set standard practices for newly adopted information technology. Korean practices and experiences are being closely watched by other countries because Korea is regarded as a testing ground for technological change. For example, an alternative ID system to the current resident registration number is being sought. Another suggestion is that users' real names should be used on the internet on a limited basis to prevent cyber-defamation or malicious replies on the internet bulletin board (Jeong 2005).

However, proponents of freedom of speech object to such an idea. While critics suggested several measures to prevent the unauthorized use of others' ID numbers, the government proposed an alternative ID for use in electronic commerce. In 2005, the government devised a new identification system for the internet. In a few years, on-line businesses will be required to adopt such new PIN systems instead of the controversial resident registration numbers (Chosun 2005).

### **Legislative Proposal of New Comprehensive Law**

Notwithstanding the 2004 amendments to the existing Data Protection Act, there are campaigns to enact a comprehensive law on privacy protection from scratch. The government and legislators, in consultation with civic groups, made such proposals to the National Assembly in 2004 and 2005. The 2004 proposal was automatically repealed because of the closing of the plenary session of the National Assembly.

The three draft bills, proposed by the ruling party and two opposition parties, showed government policy and the intentions of interested groups. They are almost identical in such aspects as the classification and scope of personal information, but they differ in the nature of oversight body and applicable remedies.

All political camps agree the new act should be a comprehensive one governing both the public and private sectors. But they disagree on many points. At issue is the independence of the supervisory body. Until now two government departments conduct the overall supervision of data protection regulation: the Administration Ministry in the public sector and the Communication Ministry in the private sector. Civic groups are critical of this supervisory system because it cannot ensure the independence of the oversight body or the efficiency of privacy protection. They contend that government departments are unable to regulate themselves to protect citizens' privacy

while they are actively carrying out e-Government or digitalization projects. One of the draft bills made the supervisory body independent of all three branches of government, while others have proposed to organize it within the office of the Prime Minister. How this issue is resolved is bound to have a major influence on the future of privacy protection in Korea.

The government and the ruling party were against the reinforced punishment of privacy invasion, and the adoption of class actions other than the current ADR or litigation system. The government does not want to see an avalanche of law suits stimulated by such a new proposal, which might prevent efficient data flow. On the other hand, the civic groups are critical of the master plan of e-Government which facilitates unrestricted data flow in the public sector.

While lawmakers hesitated to deliberate the proposed data protection legislation, there took place the presidential election at the end of 2007 (Park 2007, p. 10). President-elect Lee Myung-Bak proposed a slimline government reorganization based upon the landslide victory, and the Communication Ministry will be dismantled into the Broadcasting and Communications Commission. Consequently data protection in both the public and private sector will be taken over by the Ministry of Administration and Security, and the data protection functions of KISA will be directed by the new ministry. Therefore, data protection legislation would certainly be reconsidered from the beginning on account of the reshaping of governmental functions. It remains to be seen whether the privacy protection in Korea will be reinforced or not in the near future.

## **Future Prospects**

South Korea has achieved both economic growth and political democratization in a short period of time. Its digitization progress in technology and practices such as sophisticated home networking, e-Government projects and u-health practices well deserve worldwide attention. The Korean government and people agree on the idea that the law and practices regarding privacy protection should be in conformity with global standards.

South Korea has significant data protection legislation and, at least in the private sector, novel methods of enforcing privacy rights. Together with the Data Protection Act's coverage of information service providers, sensitive data including credit information and medical data are regulated under separate laws like the Credit Information Act and the Medical Services Act.

As Korea develops a society based upon ubiquitous sensor networks, the awareness and level of privacy protection among individuals and IT businesses are increasingly high. Take an example of RFID, an indispensable material in a ubiquitous sensor network. This burgeoning RFID industry is

being regulated by the RFID Privacy Guidelines 2005 (as amended in 2007), which requires RFID providers to notify users of the presence and functions of RFID tags attached to, or built into, goods. As a result, the concerted efforts of the government and businesses as a whole are necessary lest the new technology should invade privacy of consumers.

When regulatory measures are properly implemented, the existing data protection regime in Korea seems to reach the level of privacy protection in advanced countries. However, some practices remain below the global standards. There is a room for improvement in areas such as procedural transparency with respect to wiretapping; possible data conveyance to third parties without notice to data subjects; helpless individuals' position against spam mails, and unnoticed computer matching in the public sector.

On the other hand, different efforts on the internet real name system have been made to realize a more transparent society. For example, the Act on the Public Election and the Prevention of Election Corruption allows only the person with a real name with his/her resident registration number to list his/her opinion on the bulletin board of the internet press. Thus one cannot express one's political opinion under a pseudonym on the internet. Certainly Korea's privacy legislation will be upgraded in the midst of the tension between mounting privacy awareness and rapid technological advancement.

## 8. Hong Kong

### Robin McLeish and Graham Greenleaf

---

#### INTRODUCTION

##### **Data Spills on the Hong Kong Internet**

In March 2006 personal data, including names, addresses, Hong Kong ID card numbers and in some cases details of criminal convictions, of an estimated 20,000 people who had made formal complaints against the Hong Kong police since 1996 were found on an unprotected web site in Hong Kong. The more serious complaints against the police included allegations of sexual assault, fraud and corruption, and seven complaints were still under investigation. People named in the list have described the disclosure as ‘a nightmare . . .’. The *South China Morning Post* (SCMP) claimed ‘thousands of people are living in fear’ as a result. Legislators claim that the disclosures, particularly of the HK ID card numbers which are widely used as an identity credential, are a ‘big threat’ to the financial interests of the persons concerned. This is the most dramatic privacy issue in Hong Kong’s history, in its combination of the number of people affected and the sensitivity of the data involved.

The scandal erupted when a corporate governance activist accidentally found the data when searching the internet for a person’s address. Hong Kong’s Independent Police Complaints Council (IPCC) admitted it was the source of the data, apparently uploaded to a server of a Hong Kong company by a contractor to the IPCC who was transferring data from one IPCC computer to another. The data had been accessible on the web for three years. Two days after its exposure by the SCMP it was still available in the Google archive even though it had been removed from the original site, and was circulating on file sharing networks.

It was a bad week for the Security Principle in Hong Kong’s Personal Data (Privacy) Ordinance. In the wake of the IPCC disclosures, two prominent companies were also found to have leaked unprotected customer data onto the internet. SCMP reported that ‘telecommunications company CSL apologised for having leaked the personal data of some of its customers’, also found in Google’s cache, and blamed on a ‘manual mishandling’ by their service provider. More significant was the discovery of a database freely accessible in

the Google cache containing details of about 600 policyholders of the ING life insurance company. According to SCMP, it contained 'type and amount of coverage bought, and beneficiaries' names, phone numbers, dates of birth and addresses'. ING claimed that the computer of one of its insurance agents had been hacked.

This is the downside of modern public administration and business, in Hong Kong as elsewhere. In this chapter we will see what Hong Kong's law and practices do to prevent, punish and compensate privacy dangers such as those revealed so dramatically in one week.

## **Key Personal Data Systems and their Impact**

The information systems built around the Hong Kong ID card have the most pervasive effect on the residents of Hong Kong. The laminated paper ID cards which originated at the end of World War II and include a photo are currently being replaced by a multi-purpose 'smart' (that is, chip-based) ID card which will also replace drivers' licences, library cards and other identifiers. A person must provide his ID card number 'in all dealings with government' where required. Extensive use of the card by the private sector for identity verification is also allowed despite the Personal Data (Privacy) Ordinance. Data matching between government agencies based on the number is extensive but controlled by the Ordinance. Hong Kong residents normally carry their ID cards and are accustomed to disclosing their ID number.

In the private sector, Hong Kong did not have a comprehensive consumer credit reporting system until the late 1990s, when the Hong Kong Monetary Authority, in the wake of the Asian financial crash, put pressure on all financial institutions to join the existing credit reporting system. Since 2003 credit reporting has been allowed not only on credit defaults but also on the regularity of payments and level of indebtedness of all consumer creditors, so details of the credit transactions of all Hong Kong consumers and small businesses are now much more readily available. However, use of personal information about credit practices is still largely confined within the credit industry and is not accessible to employers, insurers and those outside.

Hong Kong has taken a relaxed view of anonymity in transport systems. The Octopus Card is a pervasive, anonymous, stored-value card which can be used on most forms of public transport, and users are increasingly able to use them to purchase goods from vending machines, supermarkets etc, as well as pay for parking. It stores details of the last 20 transactions. Cards may be purchased and topped-up for cash anywhere in Hong Kong. It is now possible to obtain an identified card which can be topped-up automatically from your bank account whenever the balance on the card falls below a certain limit.

Identified cards are also being used by employees who seek reimbursement for fares, but the option of using another anonymous card for other transport remains. Cash can be paid on all tollways and tunnels in Hong Kong, allowing anonymous travel. This is important because it is impossible to travel by car from the island to the New Territories without using such facilities. A road transport system without anonymity options would be a very effective surveillance mechanism in Hong Kong. There is no pervasive surveillance of people's movement in Hong Kong.

Anonymous cash purchases of SIM cards for mobile phones (cards containing a microprocessor chip which enables a telephone number) can be made at convenience stores, and they can then be used without further identification to the network, so it seems that anonymous telecommunications are possible in HK. This contrasts with countries such as Australia where SIM cards can only be put into use once the network identifies the owner.

Workplace surveillance is extensive in Hong Kong. A survey by the Privacy Commissioner found 48 per cent of employer respondents engaged in at least one of five forms of workplace surveillance (CCTV, telephone, email, web browsing and computer use) and 27 per cent made use of two or more types (HKPCO 2005). About a third of all employees surveyed knew they were subject to some form of workplace surveillance, but only 20 per cent of them had been notified of this by their employers (HKPCO, 2004).

In summary, Hong Kong residents do not experience life as omnipresent or oppressive surveillance, and their day-to-day experiences are not the same as people living across the border in the rest of the People's Republic of China. Their experience is probably most similar to citizens of a European state where government agencies have a relatively high degree of basic information about all citizens though a centralised ID system, but where both public and private sector bodies keep personal information collected for different purposes segregated because of privacy laws.

### **Major Privacy Measures and Institutions**

Hong Kong was a British colony until 1997, when sovereign control was resumed by the People's Republic of China (PRC), and since then has been a Special Administrative Region (SAR) of the PRC. Its relatively short history of privacy protection is shaped by the conditions of that 'handover' of sovereignty. The colonial administration's desire to legislate on pre-handover 'unfinished business', particularly in relation to protection of civil rights, gave Hong Kong a data protection law, the Privacy (Personal Data) Ordinance of 1995. Hong Kong is still the only Asian jurisdiction that has a 'European' style Privacy Commissioner.

The continuation of United Kingdom-influenced common law means that, as in the UK, there is no common law right of privacy. However, the constitutional settlement between the UK and the PRC resulted in Hong Kong's 'mini-constitution', the Basic Law (1990) which established constitutional privacy rights. In 2005 the Courts upheld these constitutional rights of privacy for the first time and privacy activists forced the government to introduce legislation controlling telecommunications interception.

## KEY DEVELOPMENTS IN PRIVACY PROTECTION

### **The Constitutional and Political Context**

Hong Kong's privacy protection has a unique constitutional context. Hong Kong is a Special Administrative Region (SAR) of the People's Republic of China (PRC), established under the PRC Constitution. The 'system' instituted in Hong Kong is prescribed in the Basic Law as allowing the exercise of a 'high degree of autonomy'. This is as promised in the Sino-British Declaration (1985), the constitutional settlement by which the UK agreed to 'restore' sovereignty to the Mainland in 1997, in order to realise Deng Xiaoping's concept of 'one country, two systems' for Hong Kong (Ghai, 1999, p. 56). The system involves only limited democracy. The Chief Executive is appointed by the Central People's Government. The members of his 'cabinet', the Executive Council, are all appointed by him. Legislation is made by a 60-member Legislative Council (LegCo), of which half are elected by direct elections from geographical constituencies and the other half from specified occupational groups and industries.

The Basic Law gives Hong Kong independent judicial powers, with the judicial power of 'final adjudication' vested in Hong Kong's Court of Final Appeal. However, this is subject to an overarching power of interpretation of the Basic Law vested in the Standing Committee of the National Peoples Congress of the PRC, which is a political rather than a judicial body. So, although Hong Kong's common law legal system is preserved by the Basic Law, it is ultimately subordinated to the very different legal system of the PRC insofar as interpretation of the Basic Law is concerned. The Standing Committee of the NPC has exercised its power of interpretation on three occasions to date, two of which have been controversial. The constitutional protection of privacy in HK is, like all the other protections of the Basic Law, subject to this uncertain process of final interpretation by a political body.

## **Constitutional Protection of Privacy and the Crisis over Surveillance Laws**

Constitutional protection of privacy occurs in three different ways in Hong Kong. First, the Basic Law (1990) provides for the continued application of the International Covenant on Civil and Political Rights (ICCPR, 1966), the broadest international convention protecting human rights. These rights in the ICCPR and the Basic Law include both a general right of privacy and the right to protection of the law against 'unlawful interference with . . . privacy, family, home or correspondence'. Because Hong Kong is not a party to the First Optional Protocol to the ICCPR, and China has not ratified it on behalf of Hong Kong, its residents do not have any direct right of appeal ('communication') concerning breaches of the ICCPR to the UN Human Rights Committee.

Second, the ICCPR provisions have been replicated in local legislation in Hong Kong's Bill of Rights Ordinance (BORO, 1991), but its provisions are subject to amendment or repeal by the Legislative Council (LegCo), unlike those of the Basic Law. The BORO is binding only on government authorities and can not be used by individuals to seek protection against actions by businesses or other private bodies. There are as yet no significant privacy cases under the BORO.

Third, the Basic Law specifically provides in relation to privacy that 'The homes and other premises of Hong Kong residents shall be inviolable' and that 'arbitrary or unlawful search of, or intrusion into [such homes and premises] shall be prohibited'; that 'The freedom and privacy of communication of Hong Kong residents shall be protected by law'; and that 'No department or individual may . . . infringe upon the freedom and privacy of communications of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences'. These Basic Law protections cannot be amended by the local legislature, but can be 'interpreted' by the Standing Committee of the National People's Congress (NPC) of the People's Republic of China.

This third constitutional protection finally became a major public issue in 2005, to the great discomfort of Hong Kong's administration. The Telecommunications Ordinance prohibits unauthorised interception of telecommunications, but also empowered the Chief Executive to authorise such interception ('wiretaps') if he considered that the public interest so requires. The Administration refused to reveal how often the Chief Executive used these powers, but in 1999, an unofficial report estimated interception of more than 100 conversations per day (EPIC HK 2005). There were warnings even before the handover that these practices were unconstitutional (HKLRC 1996), and LegCo passed a Bill restricting them in 1996. But the

Administration had since then refused to bring it into force on the grounds that it would 'severely hinder' law enforcement (SCMP 13/8/05). So matters rested for nearly a decade.

Police surveillance by means other than telecommunications interception did not require any legal authorisation. This resulted in a court ruling in April 2005 that the use of covert surveillance devices by a law enforcement body (ICAC, the Independent Commission Against Corruption) was a breach of the 'privacy of communications' protection of the Basic Law because its requirement for 'legal procedures' to sanction their use had not been met (HK District Court 2005). The government's response was to issue an 'Executive Order' made by the Hong Kong Chief Executive (Executive Order 2005) that provided for 'authorisation' of covert surveillance for law enforcement purposes by senior officers designated by any government department head. This resulted in a constitutional crisis when two democratic activists, one a legislator known popularly as 'Longhair', fought and won a court action through all levels of Hong Kong's judicial system to establish that both the 2005 Executive Order and the Telecommunications Ordinance provision were constitutionally invalid. The Courts, in a controversial decision, suspended the invalidation for six months until September 2006 to allow the Administration opportunity to pass new and valid legislation. But Longhair's claims of constitutional invalidity were upheld all the way to the Court of Final Appeal.

In August 2006 LegCo enacted a government-proposed Communications and Surveillance Ordinance, thus ending the crisis. The Ordinance requires judicial authorisation of both interception of communications, and the more intrusive types of other covert surveillance by law enforcement bodies, but allows the executive to authorise less intrusive forms. A Court of Appeal Judge has been appointed as Commissioner on Interception of Communications and Surveillance, required to submit an annual report to LegCo including statistics of surveillance activities. Where he discovers unauthorised surveillance activities, the individuals subjected to such surveillance will have to be notified. Many of the recommendations of the Law Reform Commission, both in 1996 and in its final 2006 Report (HKLRC 2006) were included in the Bill. As a result, Hong Kong has moved from being a jurisdiction with only nominal controls over surveillance, to one with a high degree of accountability and transparency. An activist in the Courts achieved what a decade of law reform had not.

The surveillance crisis has also shown that constitutional litigation is possible as a means of privacy protection. In June 2006 two of the 20,000 people in the 'data spill' of complainants against police commenced actions in the High Court claiming that the Independent Police Complaints Council (IPCC) has breached their privacy rights under both the Basic Law and ICCPR. One of the litigants stated that she fears for her life.

## Judicial Protection of Privacy – the Common Law Vacuum

The Basic Law guarantees that Hong Kong remains a common law jurisdiction, and so its Courts are free to adopt principles developed in Courts of other legal systems of British origin. If the common law protected privacy, constitutional provisions and legislation would not be so important. Hong Kong courts have not made any significant decisions on this, but it is likely that they would follow the United Kingdom approach in rejecting any general common law right of privacy (*Wainwright v. Home Office* 2003). At the same time it is possible that Hong Kong's courts may give greater protection to privacy in future by expanding the law of breach of confidence, again in line with the recent UK approach (*Campbell v. MGN Ltd* 2004).

In August 2006 pictures of 'Twins' pop star Gillian Chung Yan-tung, half-naked while changing her costume, were taken by a hidden camera and published in *Easy Finder* magazine. The Hong Kong Law Reform Commission had recommended legislation for new privacy rights of civil actions for public disclosure of private facts and intrusions into privacy (HKLRC 2004a), but the government had ignored the proposals. In the media furore resulting from the 'Twins' photographs, Chief Executive Donald Tsang promised that the government would use these proposals as the basis for exploring new measures to guard against press intrusion into privacy (SCMP 30/8/06).

## ID Cards, Dumb and Smart

ID cards and uses of personal data associated with them have been essential parts of Hong Kong life since the end of World War Two. The public appears to accept them as necessary to deal with illegal immigration and border security. Required of all residents over the age of 11, the ID card includes a unique identification number which must be provided if requested 'in all dealings with government' (Registration of Persons Ordinance (ROPO)). Before the 1995 privacy Ordinance, many private sector organisations had already established practices of requiring the card or number, because no law prevented this. This method of identification was convenient for individuals and business as well as government, though only government authorities had the means to check the authenticity of cards or numbers.

In 1997 the Privacy Commissioner issued a Code of Practice on the ID number (HKPCO 1997), as required by the new privacy Ordinance. The Code specifies how the Ordinance applies to the ID number, provided it does not contradict the Ordinance. This one-off opportunity to control the ID card and number was lost when the Commissioner took the view that 'roll-back' was not a viable option, even in the private sector, in the absence of specific

statutory direction or strong public demand. In his view, the most that the Code could achieve was to contain its use to existing uses. The Code does not limit the collection of ID numbers by government agencies, due to the ROPO requirement to produce. In the public sector, the ID number makes data matching between agencies technically easy because they share a common identifier for their clients. In the private sector, the Code allows routine collection of ID numbers wherever reliable identification is necessary to avoid non-trivial losses. ID numbers may be shared between private sector organisations where collected for a common purpose, but disclosures for purposes of 'data matching' have to satisfy additional rules. Any organisation may use the ID number as a multi-purpose internal identifier. At present the main limit on expansion of use of the ID number is the difficulty of collecting them by automated means whenever a person presents an ID card.

Although the Code is permissive, it is still possible to breach it and the six Data Protection Principles (referred to below as 'Principle 1' etc) underlying it. The Commissioner receives more complaints about the ID card than anything else. Unauthorised disclosures (Principle 3), the most common complaint, were held to occur where a newspaper published a witness statement by a police undercover agent which included his ID number and name; and when a finance company disclosed to its debt collector a copy of a debtor's ID card, and the debt collector put a copy on an envelope sent to the debtor. Breaches of the security principle (Principle 4) have been found where a mobile phone service company used the first six digits of its customers' ID numbers as their default password; where a radio station let prize-winners see a list of ID numbers of other prize-winners as evidence that prizes had been paid; and (not surprisingly) when a bank staffer left a briefcase in a public bus containing the credit card applications and copies of ID cards of applicants. Excessive collection (Principle 1) is rarely a source of ID complaints due to the Code's liberal acceptance of collection of ID numbers. One excess was to require ID numbers on a membership card for a gift redemption scheme. These are the unspectacular events that people complain about.

The 'roll-out' of chip-based 'smart' ID cards to replace the existing laminated cards will not be complete until at least 2007, so its effects are yet to be felt. The core problem of the Hong Kong ID system is that its purpose has never been defined with precision even for the public sector and not at all for the private sector. It has therefore always been susceptible to expansion of uses beyond its main purpose of controlling immigration. The smart ID card capitalises on this weakness by being multi-functional from the start, but with expansion of functions intended but undefined. Uses under consideration have included e-voting, health records and an electronic purse (a facility to store credit on the card's chip, for later use with parking meters, vending machines and so on). One agency with a key role in developing the smart ID card stated

bluntly that ‘potential use of the chip is large and new possible functions are emerging all the time’ (ITBB 2001). It has four non-immigration functions from inception, as it will also constitute the driver’s licence, central library card, a token to carry a digital signature, and a means of making online change of address. These four uses are ‘voluntary’ in the limited sense that Hong Kong residents will still have alternative ways of doing these things. However in each case the extent of ‘voluntariness’ is significantly qualified because those ostensibly opting out of these functions will be likely to face disadvantages (Greenleaf 2002). It is a multi-function smart card from birth.

There are few political safeguards on further expansion of functions. The chip on the card is technically capable of carrying many more applications and data. The Legislative Council (LegCo), when it authorised the smart ID card did not impose significant limits on future expansion of uses. The card (and chip) can have new data and functions added merely by government regulations which LegCo can disallow but does not have to approve. Most additional new government uses will not require changes to the card or chip, and can therefore proceed without any LegCo scrutiny (Greenleaf 2002). If past experience is a guide, the Privacy Commissioner is unlikely to use the ID Code to impose significant restrictions on what applications can be included on the chip or how data can be collected from the chip. Hong Kong is likely over time to develop an ID system with many different functions.

### **Origins of the Privacy Ordinance**

The most important legislation concerns information privacy. The Personal Data (Privacy) Ordinance (PDPO, 1995) covers both the public and private sectors. Its enactment was not prompted by any significant public demands or major controversy but was led by the then colonial administration, influenced by local elite opinion. It was a positive and not a reactive process, in contrast with the anti-discrimination legislation enacted at around the same time which was seen as the government’s response to an alternative Private Member’s Bill providing for much more far-reaching legislation.

Significant interest in data protection grew from concerns in the late 1970s about the potential privacy dangers from emerging computer technologies. The government established a Working Group in 1983 and by 1988 published voluntary OECD-inspired ‘Guidelines’ and accepted the necessity for legislation (Government of Hong Kong 1988). This acceptance was prompted primarily by trade concerns that Hong Kong’s position as a financial and commercial centre could be jeopardised by limits on personal data flows from Europe following the European privacy Convention (1981) (Government of Hong Kong 1988, pp. 4–5). From 1989 the Hong Kong Law Reform Commission (HKLRC), was given a very broad reference on privacy protection, and following public consultations

published recommendations for data protection legislation (HKLRC 1994), the majority of which were embodied in the 1995 Ordinance (PDPO 1995). The government continued to stress safeguarding the free-flow of personal data to Hong Kong in justifying the Ordinance (Suen 1995).

In the last years of the British Administration the Hong Kong government had a mixed record on initiatives to protect human rights. On the one hand there was the enactment of the Bill of Rights Ordinance (BORO) in 1991 followed by repeal of repressive laws inconsistent with it. On the other hand, the government rejected calls for the establishment of a Human Rights Commission, enacted narrow anti-discrimination legislation, and, stalled enactment of interception of communications legislation. During these years it was balancing carefully which human rights-related measures it felt able to adopt, in light of relations with the Mainland government. The PDPO had an economic selling point, safeguarding the free-flow of personal information to Hong Kong. But it was also a human rights-related initiative difficult to characterise as part of a British plot to destabilise Hong Kong in advance of the 'handover'. This may help explain why the colonial government embraced it so readily.

### **Who is Bound by the Ordinance?**

The Ordinance is comprehensive, covering 'data users' in both public and private sectors, with very few exceptions compared with data protection legislation in many jurisdictions. There are exemptions from the principles of use limitation, and of subject access, where this is necessary to protect various public and social interests such as security, defence, international relations, the prevention and detection of crime, and the remedying of unlawful conduct. But these only apply where complying with a Principle would prejudice the interests concerned.

The media are exempt from most aspects of the Ordinance where personal data is held for a news activity, until after publication. A person cannot request access or correction until after a story is published. The Ordinance has had little enforcement against the media.

The scope of the Ordinance also depends on the meaning of 'personal data', 'data', and 'document'. 'Personal data' must relate to a living individual (so the dead have no privacy) who can be identified from the data, and must be in a form allowing access or processing. An important restrictive judicial interpretation of 'personal data' has not yet been followed in other jurisdictions. In the *Eastweek Case* (2001) a majority of the Court of Appeal held that where a person collects data of an unidentified individual with no intention to identify that individual, this is not collection of personal data and falls outside the Ordinance. So in that case a newspaper's photo of a woman to illustrate the

bad dress sense of Hong Kong women was not collection of 'personal data' because the newspaper was not interested in the woman's identity, even though her friends and colleagues could identify her.

Information only counts as 'data' if it has been held in a document by the data user at some point, and not merely held in someone's mind. For example, where a woman disclosed her personal information to a housing estate office, and this information was passed on to others, her complaint failed because the information about her was never written down. The same result is reached in privacy laws of most other jurisdictions.

### **Content of the Data Protection Principles**

Hong Kong's six Data Protection Principles are broadly consistent with the OECD privacy Guidelines (see Chapter 1), as the HK Law Reform Commission recommended (HKLRC 1994, para 6.2), but are stronger in some important respects.

**Principle 1** limits the collection of personal data to that necessary for a lawful purpose directly related to a function of the collector. Collection must be by lawful and fair means. When personal data is collected directly from the individual concerned, notice must be given of the purpose of collection, consequences of non-provision, the usual recipients of disclosures of the data, and access and correction rights and procedures. Notice is not required where personal data is collected from third parties (as it is in some other parts of the world), or collected by observation of the person.

**Principle 2** requires that all practicable steps be taken to ensure accuracy in relation to personal data, and to erase or not use inaccurate data. It also requires that it shall not be kept for longer than necessary to fulfil the purpose for which it is used. This deletion obligation goes beyond the OECD requirements.

**Principle 3** limits the use or disclosure of personal data to the purposes for which the data were to be used when they were collected, or a directly related purpose, unless the subject voluntarily gives express consent to other uses. Hong Kong therefore takes a narrow view of allowable secondary uses, by only allowing those that are directly related (narrower than the OECD requirement) or with express consent (Australia explicitly allows express or implied consent). This apparent strictness is mitigated by the Commissioner's willingness to take a broad view of the primary purpose of collection. For example, a social worker's purpose of collection of client data was considered to implicitly include compliance with any legal obligation to provide information to a Court. This use and disclosure limitation accounts for more than half of all complaints, and almost half of the contraventions found (HKPCO 2005, figures 5 and 9).

**Principle 4** on security of personal data requires that all practicable steps be taken to protect personal data against unauthorised or accidental access, processing, erasure or other use. Security flaws in online billing systems are a frequent source of complaint, one where the Commissioner seems to have succeeded in obtaining systemic changes by telephone companies, such as more secure password requirements.

**Principle 5** requires openness by data users in relation to their policies and practices with respect to personal data. It could be used by the media and others to investigate the operation of personal data systems but has not been so used as yet.

**Principle 6** provides a right of access to and correction of personal data. Individuals can also insist that ‘their version’ of events be put on file even if the data user does not agree to change a record. Hong Kong does not have freedom of information legislation in the public sector, so the Ordinance provides the only legal rights of access to information. A significant addition to the usual OECD rights is that, where data is corrected, the data user normally has to advise anyone who has received a copy within the past 12 months of the correction and reasons for it.

Data export limitations are missing. The text of s. 33 of the Ordinance restricts the transfer of personal data outside Hong Kong unless conditions are fulfilled that help ensure privacy protection by the data recipient. However, this is the only section that the government has not yet brought into force, so it has no effect as yet. There are a number of likely reasons for this reluctance. The Hong Kong Privacy Commissioner would be understandably reluctant to use powers to specify a ‘whitelist’ of countries with legislative protections substantially similar to those in Hong Kong when the European Union has been so slow to do so through ‘adequacy’ determinations (Chapter 1 in this volume), and where choice of countries may have significant consequences for Hong Kong’s trade. Secondly, s. 33 applies to data exports to ‘a place outside Hong Kong’ which includes all other places in mainland China, where there is (as yet) no similar law. Thirdly, s. 33 is unusually extensive in scope because where a data user’s principal place of business is Hong Kong, the restrictions apply even if Hong Kong is not the place from where the data are transferred. The government’s failure to bring s. 33 into force has allowed offshore processing of Hong Kong personal data by both foreign and HK-based companies to continue uncontrolled. Such processing is believed to be extensive but its full extent is unknown. In 2004 the Commissioner announced a project to measure offshore processing, but nothing further has been heard of it (HKPCO 2005). The demands of trade have trumped the protection of privacy to date.

Given the prominence that the government has given to the need to safeguard the free flow of personal data into Hong Kong, it is ironic that this is the

only section that is not yet in force. This omission significantly compromises Hong Kong's claim to 'adequacy' of personal data protection in order to avoid restrictions being imposed by the European Union on the transfer of personal data from Europe to Hong Kong.

But Hong Kong's law can apply overseas. Mr X was convicted by a Court in the People's Republic of China (PRC) of violating PRC criminal law by disclosing State secrets, sent via his email account while he was in Hunan Province China. He was sentenced to ten years' gaol. Evidence in the case showed that details of Mr X's email transactions were disclosed to PRC investigative authorities by Yahoo! China, a business owned by a foreign company registered in the PRC but which was owned by a Hong Kong company, Yahoo! Hong Kong (YHHK). Even though all the information flows and entities were situated entirely within the PRC, the Hong Kong Ordinance appeared to apply simply because YHHK was legally able to control the data processing from Hong Kong. However, the Privacy Commissioner concluded that YHHK, in relation to this disclosure, lost the control that it was normally able to exert because Yahoo! China were obliged under PRC to disclose the information concerned (HKPCO 2007). Nevertheless, the Hong Kong law has the potential to apply to many transactions occurring outside Hong Kong.

### **Privacy Commissioner's Independence and Pro-active Powers**

The Privacy Commissioner for Personal Data is an independent statutory authority appointed by Hong Kong's Chief Executive for an initial five years and eligible for re-appointment for five more. There have been three Commissioners to date. Stephen Lau, a senior private sector computing executive who was previously the Government's Data Processing Manager, served one term (1996–2001). Lawyer Raymond Tang, served to 2005 before being appointed to another public sector post mid-term and was succeeded by Roderick Woo, another lawyer and former Law Society Chairman. The Commissioner's budget is around HK\$40 million per year for 39 staff (HKPCO 2005). His functions are to supervise and promote compliance with the Ordinance, examine proposed legislation that may affect privacy, carry out inspections of personal data systems, and undertake research into technological developments such as new methods by which data may be collected or distributed via the internet.

The Hong Kong Commissioner's Office is known internationally for its extensive education programmes in privacy rights and responsibilities, using privacy-themed activities such as plays in primary schools, poster and photo competitions, seminars and workshops and an online training tool. They have also advertised extensively on television and on transport ads, though budget cuts are forcing scaling-back (HKPCO 2005). Effectiveness of these

activities is difficult to measure in terms of the extent of compliance or willingness to exercise rights, but should not be discounted. Effectiveness may be indicated by the relatively high level of awareness of the Privacy Commissioner's office shown in user surveys (discussed later). Active engagement in the international development of privacy policies has also given his office a more significant role than the size of Hong Kong would otherwise justify.

The Hong Kong Privacy Commissioner has an abundance of powers which enable him to influence the level of compliance by means other than complaint investigations. He uses some of them effectively and others not at all. He has never exercised his powers to carry out formal inspection of personal data systems. He can require classes of data users to submit 'data user returns' but has not, so Hong Kong has no register of data users. Instead, his office carries out what he calls 'compliance checks', which involve requesting specific data users to improve or remedy practices that have come to his notice as potentially contrary to the Ordinance. In 2004–05 his office carried out 95 compliance checks, 87 involving private sector organisations. He has no power to require 'privacy impact assessments' (PIAs) of potentially privacy-invasive systems before they are built (or authorised by legislation), and the only ones he is known to have done concerned the 'smart' ID card.

### **The Commissioner's Enforcement Powers**

A telecommunications company was convicted in September 2006 in the Kowloon City Magistrates' Court of breaching the direct marketing 'opt-out' provisions of the PDPO, and was fined HK\$4000. Data users are required to cease further contact with a person who chooses to opt-out from such contact, and contraventions are an offence. The complainant had received a telephone call from the telco promoting its IDD service, had immediately requested the Company not to contact him again, but received subsequent calls promoting their broadband service. He complained to the Commissioner and after investigation, the Company was charged. Such prosecutions, or any financial penalties for breaching privacy, have been very rare events under the Ordinance, although a financial institution was convicted of a similar offence in 2005. We will see why they are so rare.

The Commissioner can investigate suspected breaches of Data Protection Principles, or breaches of other provisions, either on complaint from an individual, or on his own initiative. He can enter onto premises and require information and documents, but reported complaints show he rarely does so. If he concludes that a data user has contravened a requirement of the Ordinance and that the contravention is likely to continue or be repeated, he may serve an enforcement notice on the data user directing it to take remedial steps.

He also provides advice on compliance, where no specific complaint is made, in response to enquiries. In 1998–99, his office received nearly 20,000 enquiries, but by 2004–05 enquiries had decreased steadily to 14,862 (HKPCO 2005a). In contrast, the number of formal complaints per year has quadrupled from 253 in 1997–98 to 953 in 2004–05, but the current rate of increase is slight. So enquiries still outweigh complaints 15:1. About 70 per cent of these complaints are against businesses, 12 per cent against government departments and other public bodies and the other 18 per cent against individuals, with the percentage against the public sector declining slightly in recent years (based on the 2004–05 figures). These percentages have been consistent over time. Within the private sector, the most complaints were made against the finance, telecommunications, property management, insurance, retail and media industries, in that order. The hard-sell marketing of both apartments and mobile phone services in Hong Kong helps explain the high number of finance and telecommunications complaints.

Almost 50 per cent of the 953 complaints in 2004–05 concerned the use or disclosure of personal data without consent (Principle 3) followed by complaints about collection (Principle 1), security (Principle 4), direct marketing, access or correction (Principle 6) and finally lack of ‘openness’ (Principle 5) which received only six complaints. A third of all complaints were rejected without investigation because no breach was apparent. Of the two-thirds investigated, about 80 per cent were resolved within a year, 35 per cent were found unsubstantiated after initial enquiries, 30 per cent were dealt with through mediation, 24 per cent withdrawn by the complainant and 6 per cent dealt with by other authorities.

In the 87 cases resolved by mediation the Privacy Commissioner made recommendations to the respondents, which we can only assume were accepted, but we do not know whether the complainants were satisfied. There is no evidence that apologies, financial compensation or any other remedial actions were offered by the respondents. The Privacy Commissioner has no express powers to require or even recommend such remedies.

Only 27 cases or 5 per cent were resolved after formal investigation. Contraventions of the Principles were found in 18 of these cases, almost half of which involved use or disclosure without consent and the rest concerned other Principles in much the same proportions as for the total number of complaints received. Warning notices were issued in 12 cases (and written undertakings of compliance given wherever required). Enforcement notices were issued in the other six to direct them to take remedial actions to prevent their continued or repeated contraventions. Breach of undertakings or enforcement notices can lead to criminal penalties. So enforcement notices result from only 0.6 per cent of all complaints received.

‘Naming and shaming’ data users has at least until the most recent

Commissioner very rarely been used as a sanction. The Commissioner has powers to issue a public report (under s. 48), in which he can identify the data user but not the complainant or other individuals. Until 2005, only one such formal 's. 48 report' had ever been issued, concerning covert video-taping of a female university student by a male co-student in the early days of the Ordinance. In 2005, Hongkong Post installed pinhole cameras in the working areas of the Cheung Sha Wan Post Office, supposedly to detect the theft of stamps by employees. A local newspaper reported what Hongkong Post was doing, and the Privacy Commissioner responded with an 'own motion' investigation and issued a formal public report finding that Hongkong Post had breached the Principles in numerous ways. The potential loss of stamp revenue was out of proportion to the extent of the surveillance, and thus excessive in relation to its functions, breaching Principle 1. It was carried out in an unfair manner since the need for covert surveillance (particularly of unlimited duration) was not demonstrated, breaching Principle 1. In addition, Hongkong Post had no privacy policy in place, breaching Principle 5. The Commissioner issued an enforcement notice to Hongkong Post directing it to immediately cease the practice, destroy the records, formulate a general privacy policy on video monitoring activities, and communicate it regularly to staff. The formal report was accompanied by a press release condemning the practice (HKPCO 2005b, 2005c). Since then the Commissioner has issued two further detailed 's. 48 reports', one concerning the 'data spill' by the Independent Policy Complaints Council, and another concerning Yahoo!'s disclosures on the Chinese mainland (HKPCO 2006, 2007b). These reports are detailed analyses of the practices of the organisations involved, and of the application of the Ordinance. But in all cases so far the identity of the organisation the complaints was against was already notorious due to press publicity. It remains to be seen if the Commissioner will use s. 48 to 'name and shame' organisations whose alleged misdeeds were previously unknown.

In contrast with these public reports, the practice of previous Commissioners was to only publish an average of nine very brief summaries of complaints with no 'naming and shaming', in his Annual Reports and on his website (HKPCO 2007, website). They are a useful store of examples, and comparable in their number and detail to those published by other Commissioners in the region (see Privacy Law Library 2002–), but inadequate to give a clear idea of his practices.

These questions of publication practice are important because the interpretation of the Ordinance by the Privacy Commissioner's office is the *de facto* law in Hong Kong. Few appeals go to a relatively little-known Administrative Appeals Board. There is no appeal to the Courts from the Commissioner or the Board. Few cases go to the Courts as a result of applications for judicial review of administrative action. As a result, there is little judicial interpretation of the

Ordinance as yet, and likely to be little in the future. The Commissioner's lore is the law, so whatever he publishes about his practices takes on more importance than might be expected. The Commissioner's office has published a detailed statement of its views on the interpretation of the Ordinance after ten years of its operation (HKPCO 2006).

### **How Effective are the Remedies?**

A breach of one of the Principles is not by itself a criminal offence, but a breach of any other requirement in the Ordinance, such as contravention of an enforcement notice, is an offence. So the Commissioner can enforce the Principles by the threat of criminal sanction implied in an enforcement notice. The notice may specify steps needed to remedy the contravention. A major limitation on the effectiveness of enforcement notices is that they may only be served where the contravention is likely to be continued or repeated by the data user. So, while valuable to protect other data subjects against continuing or future contraventions, such notices will not necessarily provide a sufficient remedy to the complainant. This is particularly so in situations where a breach is not due to any systematic deficiency in the practices of the data user but has nevertheless already resulted in damage to the complainant's reputation, injury to feelings or financial loss. The police complaints 'data spill' illustrates this weakness: it is not likely that the Independent Police Complaints Council will repeat anything resembling the security breach that disclosed 20,000 people's data. Enforcement notices are an inadequate remedy.

In Hong Kong's mercantile society, money talks – but not in privacy cases. The Commissioner has no powers to require payment of compensatory damages or the giving of apologies by the data user, nor any specific function of mediating between the parties to reach a mutually satisfactory outcome. The Commissioner's office states that it does not mediate but merely leaves negotiations to the parties (Lam 2005). Consistent with this there is almost no mention of apologies and none of compensation in the Commissioner's complaint summaries. Compared with other jurisdictions where Commissioners have actively sought negotiated compensation (eg Victoria, Australia) this leaves complainants in a weak position.

Complainants do have a statutory right under the Ordinance to compensation for damage, including injury to feelings, for a breach of a Data Protection Principle or other provision of the Ordinance. Complainants are left to their own resources to start a civil action for compensation in a Hong Kong court. Such compensation actions have not been pursued by complainants, possibly because such an action involves many risks. The litigation costs of both parties may be awarded against them if their claim fails, since the usual rule in Hong Kong Courts is that 'the loser pays'. There is no guarantee of anonymity of the

proceedings. The data user has a full defence if it can show it has taken reasonable care to avoid the contravention, or if the contravention was because of inaccurate data received from a third party. Legal aid is difficult to obtain. The Privacy Commissioner has no power to award damages, nor to assist complaints in any such litigation in the Courts.

The lack of any compensation paid for breaches of Hong Kong's data protection law in nearly ten years of its operation is in stark contrast with Korea, where compensation is routine when a breach is established. It also places Hong Kong at odds with the practices in Australia, New Zealand and Canada, where compensation payments do occur though still as exceptions rather than the norm. The Privacy Commissioner cannot be blamed for the lack of compensation cases brought under the Ordinance, nor for his lack of powers to intervene in such cases. Neither can he be blamed for the lack of any provision in the Ordinance that gives him or the Administrative Appeals Board powers to award damages. Nevertheless, equivalent bodies in Australian and New Zealand jurisdictions have such powers. The Hong Kong system has failed to deliver protection which is normally found in Asia-Pacific jurisdictions.

A failure to comply with an enforcement notice, or other provision of the Ordinance, is an offence, but there have been only a handful of successful prosecutions for breaches. Until the recent telemarketing prosecutions, it appears that Commissioners have chosen to shy away from this power of enforcement.

### **Legitimizing and Expanding Credit Reporting**

As in other countries, a key source of erosion in privacy protection in the private sector has to do with credit reporting. But in Hong Kong it is a strange tale of a government pushing reluctant participants into an expanding credit reporting regime with the assistance of the Privacy Commissioner. Prior to 1998, consumer reporting in Hong Kong was relatively undeveloped compared to, say, the USA or the UK.

It did not have the participation of all the major credit providers, including the largest retail bank. It was also limited to 'negative' credit data and credit reporting, involving only the reporting of credit defaults and lost credit cards, and so only affecting those people who have had 'credit problems'. In contrast, 'positive' credit reporting refers to the continuing periodic exchange of 'payment performance' information (details of periodic payments due and when paid and balances outstanding on accounts) about all credit-holders, whether or not they have ever been in default.

In 1998 Privacy Commissioner Lau issued a Code of Practice on Consumer Credit Data (HKPCO 1998) which restricted the credit data that could be

shared via a consumer credit reference agency to 'negative' credit data, with an exception in relation to 'positive' data on leasing and hire-purchase transactions. This reflected the general practice of Hong Kong's major credit reporting bureau (CIS, an industry-owned cooperative) at the time. But the Hong Kong Monetary Authority (HKMA) considered the lack of a 'fully-fledged' credit reference agency with full participation by all 'Authorised Institutions' (that is banks, restricted licence banks and deposit-taking companies) as a weakness in Hong Kong's financial infrastructure (HKMA 1998). HKMA used the existence of the Code to counter objections from non-participating institutions based on confidentiality concerns, and issued a recommendation encouraging them to participate in a credit reference agency under the Code (HKMA 1998). Within a year of the Code, one of the big three American consumer credit reference companies, Transunion, acquired a majority shareholding in CIS in a move that was welcomed by the HKMA (Carse 1999), and is now Hong Kong's sole provider of consumer credit reports. HKMA's pressure on Authorised Institutions to participate in the sharing of credit data later became a requirement under statutory guidelines that they participate in both a consumer credit reference agency and one covering small and medium-sized enterprises (HKMA 2005, IC-6 and IC-7).

The Code was then amended by Privacy Commissioner Tang in 2002 and 2003, with HKMA support (2004), so that it permitted general sharing of 'positive' credit data that had not previously been allowed (HKPCO 2003, Schedule 2). This was a quantum leap in the scope of data shared, and will over time result in information relating to nearly every adult in Hong Kong being shared through CIS, instead of the relatively small minority monitored by CIS under 'negative' reporting. Instead of achieving its original 1998 objective of limiting and regulating the sharing of credit data relating to individuals between lending institutions, the Code of Practice has perversely resulted in far more pervasive and privacy-intrusive sharing of such data. This has resulted from the Code being leveraged by the HKMA, initially to achieve industry-wide participation, and then to facilitate the introduction of a 'positive data' consumer credit reference service. The Privacy Commissioner's role in the first development seems to have been unwitting, his role in the second intentional.

### **Effectiveness of the Office of Privacy Commissioner**

In 2005, the Privacy Commissioner responded to a criticism often made of such Commissioners that he was a 'toothless tiger' with a lengthy defence (HKPCO 2005a), concluding that he 'does not play the role of a tiger and does not want to be regarded as a tiger. On the contrary, the PCO intends to establish a better social culture through complaint handling, provision of information, issuance

of codes of practice, and conduct of public education and promotional activities.' The Hong Kong Privacy Commissioner has invested more serious resources than most others in encouraging compliance, but the overall effectiveness of his Office is still open to question.

On the negative side, the Privacy Commissioner's lack of remedial powers to benefit complainants – or to refer cases to another body for such remedies – leave him bereft of administrative tools found elsewhere, and leaves individual complainants uncompensated. Respondents breaching the Ordinance have been let off from even the sanction of 'name and shame' by the Privacy Commissioner's failure to use formal public reports about complaints until recently. Evidence of Privacy Commissioners' having a major effect on public policy in favour of privacy is hard to find. The office contributed little of substance to the latter stages of the debate on the 'smart' ID card, though the first Commissioner did push successfully for the Privacy Impact Assessments of that scheme. The Commissioner's role in developing Codes of Conduct on the ID card number and other personal identifiers and credit reporting has been to legitimate or expand questionable privacy practices, more than to protect privacy.

On the positive side, there is no doubt that the Commissioner's educational and other compliance-inducing activities have meshed well with the administrative and business cultures of Hong Kong, and that most organisations now observe basic privacy rules far more than a decade ago. The office is also effective in convincing respondents to comply with the Ordinance once complaints come to it. We should also remember that the Privacy Commissioner has had to battle largely alone to establish privacy as a public value. There have been few civil liberties NGOs on the Commissioner's side, balanced against well-established business organisations and government agencies pursuing vested interests in surveillance. It is a reasonable record, but one that could be improved.

## ROLE OF PUBLIC OPINION

### **Public Protest**

Hong Kong has lacked any major public confrontations over privacy issues. More minor public confrontations do occasionally erupt, such as over proposed introduction of electronic road pricing in the early 1980s. Another occurred in Lan Kwai Fong, one of the most crowded areas of downtown Hong Kong, a dense mix of bars, restaurants and shops. In 2002 the Police announced plans for blanket CCTV surveillance to assist in crowd management and crime prevention. 'The cameras would be linked to a police station

and footage would be held for three months. The plan was supported by the local business association, but not by many local businesses who felt the surveillance might affect people's willingness to come to the area. Lawmakers and human rights groups also opposed the plan, as an invasion of privacy' (EPIC HK 2004). This opposition, plus public comment in newspapers and criticisms by legislators resulted in abandonment of the proposal. At issue was 'the apparent lack of regulation of the use of CCTV cameras, the retention and use of videotaped records and the potential intrusion upon privacy in places to which the public have largely unrestricted access' (HKPCO 2004).

On issues such as the privacy impact of the 'smart' ID card and the introduction of 'positive' credit reporting, where strong public opposition would be expected in many other countries, there has been little public challenge to the approach advocated by government and business elites. When the smart ID card was being debated in 2001–02, there was no domestic NGO opposition, no press analysis or even letters to the editor, no significant critical input from the Privacy Commissioner, and no serious LegCo opposition. In submissions to the Legislative Council, the only opposition to the multi-function nature of the card and its expansion came from a visiting academic (Greenleaf 2002), plus a critique of other aspects of the bill from one local academic (Lee 2002). The new multi-purpose 'smart' ID card and information system is arguably more privacy-invasive than systems which caused massive protest and ultimate rejection in Australia and South Korea, and similar in many respects to the proposals which are causing great controversy in the UK and again in Australia. Residents of Hong Kong have become inured to a multi-use ID card system and appear wholly de-sensitised to concerns about the privacy impact of ID cards. These would be major privacy issues elsewhere.

But Hong Kongers are not inherently acquiescent when they perceive infringements of civil liberties. In June 2003, only a couple of months after the ID legislation was passed, an estimated half a million people from a population of 6 million took to the streets to protest against attempts by the government to introduce a 'security' law. The government claimed that Hong Kong's Basic Law required it to introduce this law, which many saw as threatening freedom of speech and association. The government was forced to abandon the law. No such dramatic events have yet been triggered by privacy concerns.

## Public Opinion

While it is clear that public *activism* in relation to privacy has usually been low, the assessment of public *attitudes* toward privacy as a value is a different question. Hong Kong residents have continued over seven years to rate privacy as one of the three social issues of most concern to them. Nearly 70

per cent of respondents were aware of the Privacy Commissioner from media sources, with over 40 per cent aware through the PCO's publicity program (HKPCO 2004b).

Data users also have a generally positive attitude toward privacy protection. These surveys show that 97 per cent of government organisations had the legislatively required written Privacy Policy Statements and Personal Information Collection Statements, but only 46 per cent did in the private sector. Between 80 per cent and 90 per cent of respondents considered that compliance was beneficial to their organisation in various ways, from public image to improved record keeping. Compliance was least likely from small organisations.

### **Elite Opinions and Activism**

A contributing factor toward the lack of public engagement in privacy issues – and perhaps also a reflection of it – has been the absence until 2006 of an *organised* civil libertarian constituency interested in privacy issues in Hong Kong. While Hong Kong has some NGOs involved in promoting human rights, privacy has had virtually no voice. This is paradoxical, because Hong Kong has had for the last decade as high a concentration of experts on privacy law and policy as could be found in any comparably sized jurisdiction in the world. Professors of law and sociology at the University of Hong Kong, members of the bar (including former senior staffers of the Privacy Commissioner's office), judges, and professional staff of the Law Reform Commission comprise this body of expertise. They have created a wealth of erudition and experience which has resulted in the Law Reform Commission's series of reports on privacy issues which is the equal of any in the world (HKLRC 1994, 1996, 2004, 2004a, 2006), and a high quality body of academic and professional literature (Berthold and Wacks 1997, 2002; Wacks 1980, 1989, 2000; McLeish 2000).

But other than providing the impetus for the enactment of the Ordinance, and maintaining high standards in the Law Reform Commission's recommendations, this concentration of expertise has had little effect on legislative change or on creating an activist privacy culture. This is changing. In 2006 steps were taken to form a privacy NGO in Hong Kong, with leading roles taken by ex-members of the Law Reform Commission's Privacy Committee, and it is now taking an active role in public debate on privacy.

Assessment of elite attitudes and activism must now include the extraordinary role of the maverick legislator 'Long Hair' (Leung Kwok-hung) and his activist colleague Koo Sze Liu who have together, with support from the legal profession, successfully challenged the whole police and security apparatus, government and constitutional structure of the SAR in the 2005–06 surveillance

cases. They are a stellar example of the difference that individuals can make in privacy activism.

## LOCAL CULTURE AND TRADITIONS VS. INTERNATIONAL INFLUENCES

### **International Influences**

It is pointless to argue whether the impetus on the colonial administration to enact the PDPO prior to the handover was domestic in origin, or reflected concerns derived from abroad. It was *sui generis*. The content of the Ordinance clearly reflected both the OECD Guidelines and the EU Directive, but not as any direct pressure from abroad. Instead it reflected a government aim for long-term protection of the trading position of Hong Kong, the desire of the departing colonial administration to leave Hong Kong with civil rights protected by law, and an elite concern to be in keeping with international best practice. The constitutional protections found in the Basic Law (and the BORO) are of course a direct reflection of the International Covenant on Civil and Political Rights. Some judges in the wiretapping cases have used the privacy jurisprudence of the European Court of Human Rights.

Post-handover, there have been no significant external influences on the shape of Hong Kong's privacy laws. The Privacy Commissioner's Office was a significant participant in the development of the APEC Privacy Framework (APEC 2004), the non-binding set of principles developed by the Asia-Pacific Economic Cooperation (Greenleaf 2006) but there is no reason to expect that the Framework will have any effect on Hong Kong laws. The next significant test of outside influences on Hong Kong's privacy laws will come when the European Commission assesses the 'adequacy' of Hong Kong's privacy laws for the purpose of authorising personal data exports from Europe to Hong Kong. It is likely that Hong Kong's laws (constitutional, common law and the Ordinance) will be regarded as 'adequate' in most respects, but areas of doubt remain. The EU investigation, when it occurs, may prompt the Hong Kong government to bring the data export restriction into force. This would be a significant decision, given Hong Kong's steadily increasing rate of outsourcing of personal data processing (HKPCO 2004), both to mainland China and to other Asian countries.

### **Local Cultures and Traditions**

The formal structure of Hong Kong's law relevant to privacy has little that is distinctive of Chinese culture: the common law and the drafting of the

Ordinance are little different from what they would be in the UK. The effect of PRC 'interpretation', coming from the very different legal tradition of the People's Republic, is yet to be felt on any privacy issues.

The administration of the Ordinance may be another matter. Neither the first nor the second Privacy Commissioner (Lau and Tang) showed a willingness to take up public causes that would have placed them in direct conflict with the government or private sector interests. The third Commissioner (Woo) has come into more conflict with government authorities over data leaks revealed by the media. It might be tempting to say that the avoidance of public confrontation is consistent with a Chinese cultural emphasis on maintaining 'face', but Privacy Commissioners in many jurisdictions have taken much the same approach and have gone out of their way to avoid identifying or otherwise embarrassing agencies and companies found to have breached privacy laws.

The British civil service tradition is often considered to be compatible with Chinese Confucian traditions of administration, which is not surprising since it is partly based on them. Hong Kong is the jurisdiction more than any other where these two traditions merge. The relatively high quality and non-corrupt administration in Hong Kong reflects this merger. Hong Kong agencies generally attempt to observe any legal protections of privacy, at least provided that they are spelled out in ways which can be implemented and do not require too much interpretation of the 'spirit' of the legislation. As a result, educational campaigns aimed at agencies are likely to fall on receptive ears, and their effectiveness should not be discounted even if difficult to measure. While Hong Kong companies operate in one of the world's more *laissez faire* economies, it is an economy very strongly influenced by notions of the rule of law, observance of contracts, and impartial administration of legislative regulations, even though they are often minimal. There is also a strong cultural imperative not to suffer the embarrassment of being caught in breach of the law. Hong Kong businesses are therefore also likely to be relatively observant of privacy legislation and receptive to educational campaigns concerning its implementation.

Some practices pass unnoticed in Hong Kong which would cause opposition elsewhere. The long history of using an ID card to control immigration has resulted in an acceptance of practices which would be controversial elsewhere, such as the requirement to carry the card and random checking of some classes of people. Lurid media photos and stories of non-celebrity 'domestic' troubles and misfortunes are commonplace in the lower end of the local press, whereas in some other societies these are restricted to celebrities and other public figures (HKLRC 2004).

Some aspects of the Hong Kong experience in protecting privacy do therefore reflect local cultures and traditions, both British and Chinese. But these

appear more as influences on implementation (often positive), and seem less important than Hong Kong's adoption of global standards of privacy protection.

## WINNERS AND LOSERS

Over the last decade the people of Hong Kong have benefited from some privacy victories. They received a handover 'gift' of a mini-constitution in the form of the Basic Law that offers significant openings for authentic privacy protection. Its obligations on the government to protect privacy were the main cause of the 2006 Ordinance regulating surveillance. Another handover present was a data protection Ordinance which is of a similar standard to many overseas laws though like them it has many limitations. A generally law-abiding administration and private sector, coupled with a relatively well-resourced Privacy Commissioner's Office has resulted in a society which observes minimum privacy standards far more than would have been the case a decade ago. This all adds up to a modest set of wins for citizens and consumers.

As far as anyone can tell in the absence of published statistics, there has not been a drastic expansion of surveillance in the government sector, either before or after the 1997 handover. But data matching between government agencies has expanded very significantly, with little critical input from the public or (as far as is known) the Privacy Commissioner. The failure of the Privacy Commissioner to limit the uses of the ID card in 1997, or of the legislature (LegCo) to prevent its expansion in 2002–03 spells a long-term loss of privacy for everyone in Hong Kong. The Hong Kong government could use the ID card to abuse privacy, if it chose to do so.

In the private sector, consumers have had wins and losses. Extensive reporting on consumers in the fields of credit, insurance, employment, and so on, had not developed in Hong Kong prior to the PDPO in the mid-90s. As a result, the PDPO's restrictions on the use or disclosure of personal information for purposes other than that for which it was collected have been largely effective to keep personal information within industry sectors. This contrasts favourably with practices in other jurisdictions such as the USA and UK. In other domains, the right to opt out of most direct marketing now exists; there is little surveillance of transport systems; and anonymous telecommunications are still allowed.

On the other hand, the Commissioner's successive revisions of the consumer credit reporting Code of Practice will result in the building up of much more extensive record-keeping on all consumers. ID numbers and copies of ID cards are still routinely required in many situations, ranging from

visiting an apartment building to entering a competition at Hong Kong Disneyland. The Commissioner is unlikely to limit such practices.

The media continue to be big winners, with the Ordinance exercising little control over their activities. There is great reluctance on all parties to interfere with the press in the absence of fully democratic political institutions. Vigilant media provide some counter for the democratic deficit. But unjustifiable media intrusion is widespread (HKLRC 2004). The Hong Kong Law Reform Commission's proposal for the establishment of a statutory Press Commission is unlikely to reach the political or legislative agenda, but after the 'Twins' incident the government is at least promising to examine the HKLRC's proposals to limit privacy intrusions by the media.

## PROSPECTS FOR THE FUTURE

In most respects Hong Kong has uncertainties about the future of privacy typical of other economically advanced countries with mature privacy laws. Predominant future influences on privacy are likely to be the international development of government and business practices and the ways in which privacy laws adapt to them.

But there is one big difference. An assessment of the future of privacy in Hong Kong must end with the implications of the relationship between Hong Kong and China. Hong Kong is a liberal society (with a deeply rooted tradition of freedom of speech, freedom of association etc) but it is not a democracy. The extent to which it will develop into a democracy, and the path it will take, are uncertain. It is part of the People's Republic of China (PRC), which is certainly not a democracy but a one-party state, and not a liberal society despite increasing liberalisation in some respects. It is not a country in which there is yet much legal protection for privacy and is one where the surveillance activities of the state are extensive (EPIC 2005, China Country Report).

Hong Kong at present poses the question of whether privacy or its protection can flourish in the long term in a jurisdiction which is at best quasi-democratic. There are no extant examples elsewhere. The future development of Hong Kong democracy within the framework of 'one country, two systems' will be crucial. Will Beijing be drawn into internal issues of privacy protection in Hong Kong through the constitutional role of mainland institutions to 'interpret' the privacy protections in the Basic Law, and if so with what result? This did not occur in relation to the 2006 surveillance Ordinance, and it may be that both governments are keen to avoid this.

Will the PRC develop its own information privacy laws? Will they be influenced by the Hong Kong model as the only jurisdiction with such laws within its borders? China has played an active role in the development of the APEC

Privacy Framework (REF International Chapter), and detailed discussions and drafting are underway within the Chinese government for development of a data protection law. PRC privacy legislation would be beneficial for Hong Kong in reducing its difference from the mainland (as will any changes toward democracy on the mainland). But such legislation may also bring with it some countervailing pressure for consistency with mainland laws.

Much outsourcing of processing of personal information for Hong Kong companies takes place on the Mainland. Will Hong Kong be able to bring into force the data export restrictions which are in the text of the Ordinance without disrupting its cross-border economic relationships? Of course, if the PRC does adopt its own data protection law, particularly for its private sector, this should ease such difficulties. The effect of an 'adequacy' assessment by the EU is also likely to be significant here. Will it take a hard line on this deficiency in Hong Kong's law?

Beijing will always cast a long shadow over Hong Kong's affairs. In an area such as privacy, which is a sensitive one for both state security and the economy, the working out of the relationship is likely to be a difficult and lengthy one. Nevertheless, while the people of Hong Kong are accustomed to a reasonably high degree of bureaucratic and business monitoring of their affairs, the 2003 security law protests and the 2006 surveillance challenges in the courts indicate that they will not surrender their privacy lightly.

# Conclusion

## James B. Rule

---

‘All politics is local’, goes the familiar wisdom among American politicians. The chapters of this book often seem to support this adage where the politics of privacy are concerned. In the seven countries depicted here – as in many others – the emergence and evolution of privacy as a public issue has often been idiosyncratic, to say the least. In some cases, it has turned on events and episodes that one cannot imagine happening anywhere else.

True, one can identify an archetypal state of mind underlying all demands for privacy protection. This is the gut-level indignation that flares on learning that outside interests have gained access to, or use of, what we consider ‘our own’ information. Regardless of whether the outsiders are the police, the tax authorities, credit reporters or direct marketers, this core reaction goes, ‘how did they get *my* information?’ And, ‘*what gives them the right to act on this private data, without my permission?*’

Yet we have seen that very different situations – very different juxtapositions of individual lives and institutional demands – trigger such reactions in different countries. Forms and uses of personal data that would fan the fires of public protest in one country meet with routine acquiescence elsewhere. Institutions whose efforts to acquire and use personal data are accepted without note in one setting spark bitter controversy in other national settings. And these differing ‘flash points’ leave their marks on privacy regimes prevailing in each country, long after the critical moments in public opinion have passed.

Revelation of the exact chemistry triggering privacy demands in any particular country often comes as a surprise, even to privacy-watchers on the scene. The classic case is the virtual tsunami of public indignation in Australia in 1988 over government proposals to introduce ‘the Australia Card’, a mandatory national ID document. As Graham Greenleaf notes in Chapter 5, even Australian privacy advocates at that time (including himself) felt that prospects for resisting this measure were close to nil. But to general astonishment, the activists’ dogged efforts to convey their anxieties about the project to the media sparked a broadly-based protest movement that preoccupied Australian media for months. That astonishing bit of spontaneous combustion rattled the Labor government and paved the way for creation of laws and institutions whose workings are fundamental to Australia’s privacy landscape today.

Other countries, we have seen, have their own versions of Australia's story, typically involving quite different 'triggers'. In the United States, the country's most vivid 'privacy moment' – the point at which public attention and anxiety were most dramatically focused on institutional treatment of personal data – was undoubtedly the Watergate period leading up to the resignation of President Richard Nixon under threat of impeachment. One thing that particularly galvanized public opinion in that heady episode was disclosure of White House efforts to delve into federally-held record systems in order to harass Nixon's political enemies. Coming at a moment of maximum public distrust of government power, that perception fed grass-roots demand that 'something must be done' to protect privacy. One result, as Priscilla Regan notes in Chapter 2, was the Privacy Act of 1974, still the most comprehensive federal privacy legislation in the United States.

Other countries, other triggers. In Germany, as Wolfgang Kilian points out, an unexpected flare-up of public indignation against the 1983 census tapped the same latent privacy instincts. Ordinary Germans facing comprehensive census inquiries simply could not believe that their government really needed (or perhaps, deserved) to know such things as the educational level of household members and their preferred leisure activities. This 'privacy moment' left its mark in a critical decision by the Federal Constitutional Court, as Kilian explains, upholding each citizen's right of 'informational self-determination'. This doctrine has formed the basis for subsequent privacy-friendly court decisions.

In France, the birth of privacy as a public issue dates from an influential feature story in the prestigious *Le Monde*. The account detailed government plans to link personal data from a variety of government agencies, using social security numbers as informational hooks. The acronym for the project was SAFARI, and *Le Monde* titled its account 'The Hunt for the French'. Widespread public anxiety about the plan caused the government to withdraw it, as Andre Vitalis shows, and led directly to legislation in 1978 creating the CNIL – today regarded as one of the world's more successful privacy protection agencies.

In South Korea, as Chapter 7 explains, the political chemistry of the issue has been different still. True, identity cards have been a source of controversy, as in Australia and elsewhere. But the country's most distinctive privacy moment came in the widespread public opposition to NEIS, the scheme to centralize information on pupils' school performance from throughout the country. As Whon-II Park points out, not only teachers but also broad swaths of public opinion objected to the prospect that information on pupils' 'academic records, medical history, counseling notes and family background' might be available to those with access to the systems' servers. These objections ultimately prevailed – at least to the extent that government planners significantly

curtailed the extent of data to be centralized. Stories like this demonstrate that South Koreans do not regard privacy concerns simply as European imports.

Hungary's key privacy moment came with the collapse of the Soviet bloc and the institution of that country's Third Republic in 1989. One immediate manifestation, as Ivan Szekely explains, was 'Duna-gate', the public controversy over domestic spying carried out by that country's security services before, and for a time after, its democratic turn. Another privacy controversy emerging in the same period focused on the national system of ID numbering – seen as a manifestation of police state surveillance, and abolished in a Constitutional Court ruling in 1991. These developments set the stage for the laws and institutions that have since defined Hungary's relatively strong approach to privacy protection.

But not all countries show sequences like these in the emergence of privacy as a public issue. Often privacy codes and institutions come into existence not from the push of popular demand, so much as through quiet action by policy-making elites. At some point, in other words, policy-makers look around at their global counterparts and conclude that such measures are somehow 'the thing to do'.

Among our cases, Hong Kong most closely fits this pattern – though one could make similar observations on adoption of privacy codes in Canada, the UK, Japan and many other countries. In Hong Kong, according to McLeish and Greenleaf, the British colonial authorities went to some lengths to create privacy codes in the last years before reversion of control to Beijing in 1997. Local democracy has continued to support and nurture the resulting laws and institutions since then. Chapter 8 shows how successive privacy commissioners have waged effective behind-the-scenes campaigns on behalf of privacy interests, without relying on anything resembling populist support for their issue.

A major political impetus to elite support of privacy codes – in Hong Kong, as elsewhere – is purely commercial. Frictionless exchange of personal information across international boundaries is clearly profitable in today's global economy – whereas inability to exchange such data can spoke the wheels of many business interests. As Chapter 1 points out, the European Union's relatively strong Privacy Directive of 1995 itself reflected desire to forestall privacy barriers to commerce within Europe. Similarly, the prohibition in that Directive against export of personal data to countries lacking 'adequate' privacy standards of their own has had a bracing effect on privacy protection abroad. One imagines that business and political elites in Hong Kong had no enthusiasm whatsoever for the possibility that their companies might be excluded from profitable data-management contracts with European companies, in the absence of 'adequate' protection.

Other countries also provide bountiful evidence of such sensitivities.

Canada, for example, appears to have fashioned its private-sector privacy law with an eye to achieving 'adequacy' by EU standards – and thereby forestalling trade disputes like the controversy that later nearly triggered a trade war between the USA and the EU over export of Europeans' personal data to America. Even authoritarian Singapore has recently sought to develop non-enforceable privacy standards for industry, with an eye to keeping its commercial ties to Europe unimpeded.

\*

But once adopted, privacy codes must address a predictable array of questions. Regardless of what circuitous route a country takes to membership in the global 'privacy club', that membership focuses policy-makers' attention on certain recurrent points of tension between individuals and institutions seeking their data.

By now, most readers will find these points familiar. Governments, for example, almost always want more information about their people in their efforts to enforce taxation. Social security schemes and other welfare-state programs generate their own demands for personal data on the life-situations and eligibility of would-be recipients of such benefits – demands often made in concert with taxation efforts. Policing, counter-espionage and anti-terror efforts lead to collection and use of vast data stores on those believed involved in such activities – and often non-suspects who might simply be sources of information on those who are. Vehicle registration and driver licensing require extensive record-keeping enterprises in every prosperous country. Data on their people's use of telecommunications, whether via state-owned companies or private ones, tempt every government. And the very movements and identities of citizens and residents are invariably matters of intense state interest – interests that governments increasingly seek to satisfy through reliance on universal, government-issued ID cards.

For private institutions, the foci of institutional demand for personal data are no less predictable. Direct advertising and marketing interests amass vast amounts of personal data, in their efforts to direct their (normally unwelcome) appeals to just the recipients most susceptible to them. Banking, retail trade and medical care access inevitably generate archives of personal data of interest to a variety of public and private institutions. The marketing of credit and insurance are no less intensive in their demands for personal data. Records of the financial affairs of would-be credit users, and of the personal situations and insurance claims histories of those seeking insurance, make the difference between profit and loss in these industries. Similar observations could be made for demands on personal data in employment, rental housing, and medical care delivery.

Any of these occasions for claims on personal data may be highly salient to public opinion in one country, and not at all in the next. But regardless of national context, any and all of these junctures demand coverage in any privacy code that any country may adopt. As policy-makers in any country look around for models, they confront principles that invite application to forms of personal information not necessarily anticipated at the outset.

## THE VISION OF PRIVACY-WATCHERS

Of course, conviction on the need for such codes is not universal. In all the countries covered in this book – indeed, in any democracy with vigorous public debate on the matter – some observers remain nonchalant in the face of rising institutional tracking of private individuals. For these commentators, such developments hold no particularly worrisome portends. Instead, the story goes, such monitoring simply represents an inevitable and ultimately harmless feature of a world where major institutions ‘need’ personal information, if they are to deliver performances and services that nearly everyone ultimately expects. Anyone sincerely determined to resist such changes, in this view, should adopt a way of life that involves no use of government services, no convenient consumer credit, and no use of telephone or internet.

Privacy-watchers, of course, take a less relaxed view. True, they are apt to agree, many of these personal data systems have their origins in the most banal administrative routines of state or private organizations. But the potential effects of such systems, they would insist, are not dictated by the attitudes leading to their creation. Regardless of anyone’s intent in creating systems for tracking and recording individuals’ affairs, those systems change something fundamental about the quality of civic life. They shift the balance of advantage in relations between large institutions and ordinary people, accumulating power in the hands of those gaining access to personal data. Resisting unnecessary concentration of personal data in institutional hands thus represents no more than prudent concern to preserve vital autonomy of private realms of action. Like concern for freedom of expression or limitation of police powers to imprison and interrogate, efforts to protect privacy reflect prudent concern for balance between institutional and individual prerogatives.

To such anxieties, critics often respond with remarks to the effect, ‘Show us the bodies!’. If privacy abuses are really so serious, in other words, where are the examples of specific injuries to specific parties that they promote?

But here privacy-watchers do, in fact, have stories to tell. One of the earliest accounts of personal-data-systems-turned-destructive comes from the Netherlands during the Second World War. The Nazi occupiers found detailed population records compiled by Dutch authorities – records that happened to

cite the religious identifications of each resident. Frantic efforts ensued to keep as much of this material out of Nazi hands as possible; in the words of Frits Hondius, an eye-witness who later became a data-protection specialist,

Attacks by resistance fighters against population record offices were heroic feats to save people, as was the precision air raid carried out on 11 April 1944 by the 63rd RAF Squadron . . . as a result of which 250,000 personal records were destroyed. The author vividly remembers this spectacular act of ‘international data protection’. (Hondius 1975, p. 87)

Obviously the records at issue in this astounding drama were compiled for the most routine bureaucratic purposes; absent the unexpected shift in political winds, they would presumably have remained instruments of enlightened state administration. But for privacy-watchers, the lesson is profound: no one can justly claim to foresee the political directions that will govern the uses of any stored personal information into the indefinite future.

Closer to home for Americans are examples of this country’s well-documented abuses of personal data compiled by government agencies. These include the notorious activities of the FBI in hounding domestic dissenters during its COINTELPRO operations of the 1950s and Richard Nixon’s efforts to use federally-held data to attack his political enemies. The Bush administration’s so-called ‘War on Terror’ could well be fostering further such abuses at the time of this writing.

Collective memory of such repressive uses of personal information seem to go a long way toward solidifying public support for privacy codes. Wolfgang Kilian points to awareness of Nazi-era repression as a potent source of support in German public opinion for that country’s relatively strong privacy codes. Similarly, reaction against repression in the immediate past strengthened popular enthusiasm for privacy measures in both South Korea and Hungary, according to Ivan Szekely and Whon-II Park. The unfortunate corollary here may be that countries without severe experience of government repression – ‘a political context . . . of unbroken “normality”’ as Graham Greenleaf describes Australia – may be more complaisant about the growth of personal monitoring.

Such complaisance, or its absence, may also shape the public definition of the ‘needs’ of institutions for personal data – the catch-all notion invoked by privacy-skeptics to justify virtually any and all privacy-eroding demands. Such ‘needs’ are by no means simply imaginary. Strategists for nearly every institution involved in large-scale collection and use of personal data can plausibly identify points where their organizations could do better by knowing more. Taxation authorities could identify and collect more revenue, with access to more and finer detail of taxpayers’ lives. Credit grantors could extend credit more intelligently – and more profitably – if they had access to

more information about consumers' 'private' financial lives. And certainly law-enforcement and anti-terror organizations are convinced – and not without reason – that knowing more about the lives of populations they deal with would help them identify and track suspects who require their attention.

The question is, will such 'needs' be taken as the last word in the disposition of information on people?

Privacy protection as a public issue begins, one might say, with the willingness of publics and law-makers to distinguish between 'legitimate' institutional needs for personal data, and others. So long as *any* data that *might* be useful to institutions are permissible for them to collect and use, there is no rationale for limits on their activities. But privacy protection begins when policy-makers accept the premise that lines have to be drawn – lines between legitimate claims of organizations, and those of individuals seeking some modicum of control over 'their' data. In short, when it is acknowledged that not all institutional 'needs' for personal data can be satisfied, if privacy is to hold its own.

Thus assessment of the 'needs' of organizations for personal data must never simply be regarded as readings of some objective reality – like the height of Mount Everest or the core capacity of a computer. Instead, definitions of such needs are inevitably social and political phenomena. How much state security agencies 'need' to know about ordinary citizens' telephone or email connections is a matter for determination through some form of collective deliberation – through public soul-searching in which different ideas of the public good are entertained and weighed against one another. 'Privacy moments', as described above, are points in public life where such weighing occurs. By the early twenty-first century, virtually every democracy has experienced such moments, in either their dramatic or their low-key form.

## PRIVACY CODES: THE GLOBAL CONSENSUS

Obviously these national efforts to define the just demands of privacy have not gone ahead in isolation. As Lee Bygrave's chapter demonstrates, a rough but clearly discernible global consensus has emerged over at least four decades that specifies what most privacy-watchers would bracket as privacy-friendly fair information practices. As that consensus has taken shape, both new and old members of the world's 'privacy club' have striven to adjust at least the public face of their privacy codes to accord with its themes.

By now, the essential tenets are familiar to all readers. The consensus principles demand *openness* in personal data systems, such that those depicted in them may see information recorded about themselves and, where warranted, correct those data or challenge their use; they require *legality* in operation of

the systems; they seek to establish *responsibility* of the data-keepers for following legal and procedural guidelines, normally through appointment of a figure specifically charged with such responsibility; they require that data held not be *excessive* in relation to the stated purposes of the systems; they proscribe *release or sharing* of data held in files without the consent of the individual; and they foresee creation of national-level *public offices* charged with monitoring and enforcing individuals' interests in treatment of 'their' data.

Some observers consider this rough global consensus a distinguished and definitive accomplishment. Some even hold that, with it, all serious questions of principle in the institutional treatment of personal data have been resolved.

Readers of this work know better.

For one thing, embrace of these principles is hardly complete, even among the world's 'advanced' democracies. The conspicuous outlier is of course the United States. This country has never developed broad privacy rights applying to data held in the private sector. The result is that medical records, consumer credit information, bank account archives and other categories of personal data are governed by a patchwork of different codes – and many areas of life are subject to private-sector data-gathering with virtually no legal constraint. As Priscilla Regan's chapter shows, anti-privacy interests managed in 1974 to block creation of a national privacy commission or commissioner. This departure from global trends, among others, has led privacy-watchers around the world to bracket America as having the weakest privacy protections of any advanced democracy.

More recently, in the negotiations culminating in the 'Safe Harbor' agreement, the United States stonewalled efforts of the European Union to establish what the Europeans define as 'adequate' levels of protection. With no national office-holder to act as spokesperson for privacy concerns, the United States shows little sign of drawing closer to global consensus practices.

But even where national privacy codes enshrine the global consensus as their guiding inspiration, those principles leave profound questions of practice unanswered.

For one thing, the consensus principles have been widely interpreted not to apply to the state's coercive or investigative institutions – the police, counter-terrorist operations, or similar branches of the state apparatus. Most privacy-watchers would probably agree that such agencies need to operate in a degree of secrecy, in certain of their activities, and for certain periods. But this is hardly to say that *no* restraints should apply to such organizations, in the interests of privacy. Yet privacy codes, as these chapters show, have not made much inroad on the largely free hands of these bodies to collect personal data. Often, as in the United States, such protections as exist derive from constitutional guarantees pre-dating information privacy law as such.

Germany stands as a partial exception here; as Wolfgang Kilian points out in Chapter 3 its courts have extended some of this country's privacy principles even to these activities.

Another question that remains unanswered – unacknowledged, in fact – in consensus fair information practices is more subtle, and perhaps even more profound. This is the matter of when systems of monitoring and recording human affairs ought to exist in the first place. The consensus principles, one might say, provide rules of the road to guide the workings of personal data systems, mediating the claims and interests of data-keepers and individuals. But they do not tell us whether we need to make the trip at all. What institutions or interests should have the right to record and draw upon facts on people's lives? When should people have the right to expect to go about their affairs anonymously? Should any and all personal information that is 'public' – that is, openly disclosed at one point, like the outcomes of court proceedings – be available for incorporation in institutional data systems? Should legal mandate be necessary to create such systems? If so, by what principles should that mandate be allocated? These are hardly unimportant questions; any response to them has sweeping impact on the form and extent of privacy prevailing in everyday life.

Thus for privacy codes, as so often in application of broad principle to practice, the devil flourishes in the details. The consensus principles admit of such vast variation in application as to be compatible with radically different privacy regimes.

Consider the realm of consumer credit information – that is, the data on ordinary citizens' financial status and past history of credit use sought as bases for assessing their desirability as credit customers. In principle, the range of such information is all but unlimited. Banks, retailers and credit card companies would find it advantageous to know virtually all there is to know about prospective customers' financial situation, family and residential status, past dealings with creditors and the like. The privacy interests of consumers, by contrast, lie in leaving it as much as possible in their own discretion as to how much or how little such data to disclose to prospective creditors.

This is why commercial interests predictably seek what Graham Greenleaf refers to in Chapter 5 as 'positive reporting'. This up-beat term was coined by industry to refer to their unlimited access to consumers' accounts with banks and other creditors. Under positive reporting, the consumer can do nothing to stop retailers and financial institutions from routinely funneling details of his or her current accounts to credit reporting agencies. The resulting compilations of personal data, in this privacy-unfriendly system, in turn govern the consumer's access to all sorts of further financial and consumer relationships. In the United States, this system is now so finely tuned that rising levels of debt in one credit account – as reported by credit agencies – trigger rises in the

interest rates charged to the consumer in *other* credit accounts – even in the absence of delinquency in any account. The virtues of ‘positive reporting’ as a means of enhancing profitability in the credit industry are obvious. From a privacy standpoint, the system obviously constitutes a disaster area.

But ‘positive reporting’ is not universal in countries with privacy codes. Australia simply proscribed it in 1990, as Graham Greenleaf points out; as a result, holders of consumer account data may report on delinquent accounts and applications for new accounts, but not data from existing accounts in good standing. Practice in France is even more privacy-friendly: only data on delinquent accounts are centralized. Thus it remains at the discretion of French credit applicants to bring their other credit relationships to the attention of prospective new credit grantors – or to keep such information to themselves.

In the United States, Canada and Britain, by contrast, the informational advantage lies with the credit industry. There any application for credit requires that the consumer give ‘consent’ to reporting on the use of the accounts he or she is seeking to open, into the indefinite future. As Wolfgang Kilian points out in Chapter 3, much the same system prevails in Germany, where applicants for accounts with banks, credit-grantors, and even public utilities must ‘consent’ to have their use of these accounts shared with the SCHUFA, that country’s central credit reporting exchange.

Note that all these countries apply some form of privacy code – based more or less directly on the consensus fair information practices – to credit reporting. In addition, the UK, Germany and France are all part of the European Union; hence their privacy laws supposedly represent ‘transpositions’ of the EU Privacy Directive of 1995.

Thus in all these cases, consumers have rights of access to their files and related due process rights. Yet the level of privacy accorded ordinary consumers in these countries in their dealings with prospective credit grantors varies vastly. The consensus principles simply do not specify how much personal data financial institutions are legally able to appropriate.

This example also points to another far-reaching question left unresolved in the consensus principles – the meaning of ‘consent’. It is of course basic to the consensus fair information practices that consent be required for institutional use of personal information, except where such use is legally mandated. But when do the conditions under which people ‘consent’ to use of their information become so overbearing as to deprive the term of all meaning? Here the consensus principles provide no guidance.

Thus Germany, like other countries with ‘positive’ credit reporting, requires consumers’ ‘consent’ before communicating with the SCHUFA on the applicant’s credit history. But refusal of such consent will inevitably spell denial of a bank account, credit accounts, or even access to public utilities like phone or electrical service. Without a bank account, in Germany, employment is all but

impossible, as employers are required to pay employees electronically via such accounts. The 'consent' forms that one signs for credit in other countries pose the same issues. If failure to consent to sharing of one's data comes at the cost of renouncing what most people would consider trappings of any normal life, what sense can be ascribed to notions of consent?

Or, consider some other basic precepts of the consensus principles – individuals' right to be informed of the existence and uses of information on themselves; to access such information and, if necessary, correct it or challenge uses made of it. The role of such rights as instruments of privacy protection is obvious, and hard to fault. But not all measures ostensibly aimed at achieving these things are equally privacy-friendly. Some seem intended to leave the individual as baffled as possible.

Consider the 'privacy notices' required of organizations holding personal data by recent legislation in the United States. Credit card companies, banks, accountants and other private-sector institutions now have the obligation to inform those whose data they hold of uses likely to be made of such information. The apparent intent of the legislation was to enable consumers to choose to deal with businesses that were more respectful of their privacy. But businesses have responded by composing privacy statements so dense and detailed that no normal consumer can understand them – much less rely on them as bases for deciding which companies are taking best care of their data. The companies' vague acknowledgements that they share personal data with 'affiliates' or 'companies with whom we have joint marketing agreements' give no practical guidance as to what steps any consumer could take to protect himself or herself.

Not many policies for access and awareness are this bad, but many fall far short of providing individuals with meaningful options for altering their actions in the interests of privacy. For one thing, notices of the existence and role of personal data systems often do not seem to be accessible to individuals in any convenient way. In Germany, Wolfgang Kilian notes, consumers do not seem to understand either the workings of two key private-sector repositories of personal data – the SCHUFA, a credit-reporting monopoly, and the 'Bonus System', providing small rebates to consumers for multiple purchases – nor the repercussions of these workings on consumers' interests. Such ignorance obviously makes grass-roots demand for change in their operations unlikely.

In the United States, credit reporting is one form of personal record-keeping that few consumers can ignore. Most Americans probably realize that their reliance on credit is constantly tracked and reflected in their ever-changing, three-digit credit ratings. Accordingly, it is widely understood that one has the right to view one's credit file and to challenge its contents – though credit reporting companies do everything in their power to encourage people to pay

for these services, when in fact the law requires that they be made available free of charge.

But when they spot errors in their files, American consumers find that the law leaves it mostly at the discretion of credit reporting agencies as to whether to act on such complaints. In the absence of any privacy commissioner or other official mediator, the burden of convincing the holders of data that their files are in error lies with the consumer. If the reporting agency does not agree, its only obligation is to allow the aggrieved party to enter his or her own brief statement of extenuating circumstances on the record. The only alternative for the consumer is to file suit against the credit reporting company – a recourse much too costly for most to contemplate.

Countries with privacy commissions and commissioners often seek to forestall such dilemmas for the individual by creating systems of mediation of complaints over use and misuse of personal information. Here, too, the preceding chapters have revealed a broad spectrum of privacy-friendliness in the workings of such mediation. Not all countries have the resources to mediate all the cases brought to them – nor are all mediation programs equally forceful as forces for change in privacy practice.

Australia's privacy commissions, as Graham Greenleaf notes, provide extensive mediation of individual complaints, though in a pattern where satisfaction most often seems to go to the institutional party. A particular cause of concern, in Greenleaf's view, is the fact that the results of mediation typically do not go down on any sort of record – and thus generate no equivalent of a common law tradition of precedent in personal data practice. France's CNIL, as Andre Vitalis shows, does serious mediation in many of the cases brought to its attention, and goes out of its way to publish the results.

Perhaps the strongest mediation institutions among those reported here are South Korea's. As Whon-Il Park reports, that country's Personal Information Dispute Mediation Committee (PIDMC) is supported by financial penalties levied against privacy abuses. The Committee seems to have no difficulty finding in favor of complainants, and the penalties levied as a result can be significant. The contrast to practice in the United States, which leaves those aggrieved with treatment of their data reliant on their own initiative to correct abuses, could hardly be more dramatic.

\*

It would be easy to multiply examples like these. Even among countries officially subscribing to the full range of consensus fair information practices, variation in privacy-friendliness of specific systems is vast. The consensus principles represent the beginnings of national privacy debates, then, rather than their resolution.

Yet in another sense, examples of national variation in privacy-friendliness of everyday practice also warrant a more up-beat conclusion. That is that privacy codes matter – often quite sweepingly. The control available to individuals over their own information stands to be vastly strengthened or undermined by crucial legislation and court decisions. Or to put the matter differently: neither technology nor any other impersonal force solely determines what personal data will be appropriated, and what will remain under individual control. Law and policy can and do intervene at crucial junctures to preclude some crucial forms of personal information use, and to facilitate others.

We have seen what sweeping differences such national codes make in terms of consumer credit information. The privacy that Australians and French can expect in treatment of their credit accounts differs as night and day from that available to Germans, Americans and (of late) Hong Kong residents.

Virtually as far-reaching are differences in what privacy-watchers sometimes call ‘secondary use’ of personal data – that is, commercialization of information on customers and others held in periodicals’ subscription lists, charitable organizations’ data-bases, retailers’ customer files, and the like. In the United States, bastion of the free market in personal data management, virtually any personal information disclosed to any commercial or non-profit entity – even charities – is subject to sale, trade and ultimate exploitation as a basis for direct advertising and other appeals. In Europe, any such release requires permission from the individual. Other countries – including Australia, as Graham Greenleaf points out – impose restrictions more like Europe’s. The resulting difference in background noise of unwanted, but often highly personalized advertising, is dramatic.

Thus we are hardly wasting our time by tracking differences in national practice. Battles gained and lost between privacy advocates and their adversaries set patterns with the most far-reaching implications for national privacy regimes. The battles may be public and flamboyant, or they may be muted and behind-the-scenes. But their outcomes matter profoundly in shaping what things we can keep to ourselves, and what we are bound to disclose.

## TOWARD STRONG PRIVACY

Have these discussions pointed to any single institution or precept as a guarantor of strong results in protection of personal information? Probably any such conclusion would be too sweeping – if only because it is hard to imagine institutions or precepts as having force independent of the climates of political culture and public opinion from which they spring.

Yet it is hard to see how any defense of privacy in the public arena can fail

to benefit from the existence of a privacy commissioner – or some office charged with responsibility for public advocacy of privacy values. Had such an office existed in the United States, as originally contemplated in the legislation that became this country's Privacy Act of 1974, privacy forces would almost certainly have had stronger grounds in many public battles. It would surely have been much harder for the United States to adopt the privacy-unfriendly stance it took in confrontation leading to the Safe Harbor debacle, for example, had there been a serious privacy advocate within the Clinton administration.

Similarly, at the time of this writing, Americans are reacting to rejection by federal courts of a privacy-related lawsuit by the American Civil Liberties Union. The suit sought details of an acknowledged program of government wiretapping of ordinary citizens' telephone communications without court order. Though the White House has acknowledged ordering these sweeps, no rationale has ever been provided as to why established procedures for court orders were bypassed. The ACLU suit has been denied – it may yet be appealed – on the grounds that the complainants were not parties to the dispute. But in another political and institutional world, an independent privacy commissioner would *ipso facto* have legal standing to challenge such apparently illegal use of personal data.

To be sure, not all privacy commissioners around the world enjoy the freedom of action that would make such a challenge to executive power possible. Nearly all privacy-watchers would identify the executive branch as the key source of pressure on privacy in any country. As Whon-II Park shows, South Korea's privacy-protection responsibilities are largely in the hands of the Administration Ministry in the public sector and the Ministry of Information and Communication in the private sector. South Korean privacy activists accordingly complain, he notes, that as part of the governing administration these bodies are not in strong positions to challenge government policy.

France, Hungary and Germany, by contrast, have privacy commissions and commissioners that are relatively independent of short-term executive branch pressures. In Hungary, as Ivan Szekely reports, the privacy commissioner is one of several ombudsmen appointed by and answering to Parliament. The term of his or her office can be renewed by Parliament, but not shortened. In France, the CNIL actually lies outside the normal institutional structure of government, neither part of the legislature, the executive or the judiciary. Its members are elected from a number of legislative, executive and judicial bodies, and are not subject to recall. In Germany, as Wolfgang Kilian notes, the Federal Data Protection Commissioner is a high-level civil servant, elected by two-thirds majority of the federal Parliament, and not subject to removal by the executive.

Yet the chapters have also made it clear that no privacy commission or commissioner is ultimately beyond the reach of public opinion, or of political

forces more generally. Or to put it more positively: every privacy commissioner must remain attuned to the level of public support of the values he or she seeks to defend.

Robin McLeish and Graham Greenleaf report a public spat in Hong Kong that has had many parallels around the world. Critics in 2005 characterized the city-state's Privacy Commissioner as a 'toothless tiger'. The Commissioner diplomatically replied that he 'does not play the role of a tiger and does not wish to be regarded as a tiger', the authors note; instead, he aimed at better public information on privacy and its protection, better handling of privacy complaints and the like. Thus he deftly deflected an issue that virtually all other privacy commissioners are bound to confront. Where pressure to appropriate personal information is rampant, and sensitivities to privacy concerns unevenly distributed at best throughout the public, any privacy commissioner will face demands to join struggles that he or she may consider unwinnable. At best, privacy commissioners must choose their battles with some care.

And they do not always prevail, in the battles that they do choose. Around the world in recent years, privacy commissioners have inveighed against the expansion of government claims for retention of and access to telecommunications data – expansion always sought in the name of pursuing terrorists. A particular concern has been extended retention of 'connection data' showing patterns of telephone and email contact – a cherished source of information not only for terrorism investigations, but also for many other investigative purposes. But privacy commissioners' complaints have not sufficed to prevent rule changes affording longer and longer-term archiving of such telecommunications data, 'just in case' the information might later come to interest investigators.

No privacy commissioner can sail indefinitely against political headwinds. Some of these figures have terms that outlast the terms of those who appoint them. But none of them lasts forever. Forceful decisions made during a given commissioner's term are subject to reversal later on. Privacy codes rarely have the strength of constitutional guarantees. And even privacy guarantees held to exist in constitutional law, as in the United States, are subject to privacy-unfriendly interpretations – always a possibility in authoritarian political climates. At best, strong privacy commissioners can force attention to, and respect for, privacy codes that would otherwise be ignored. But they cannot ultimately prevent changes in those codes – as the struggle over retention of telecommunications data illustrates.

\*

Recall the 'privacy moments' cited at the beginning of this section – periods at which public attention focused sufficiently on treatment of people's personal information that legislators and other policy-makers felt compelled to

act. The moments often proved to be formative points in formulation of each country's privacy code. But none of the preceding chapters has suggested that such salience of privacy concerns is a regular staple of any country's political culture – in the sense, for example, that concern over taxes or foreign policy are apt to be ever-present themes in political life. As Priscilla Regan points out most explicitly in the case of the United States, the privacy issue rises and falls on the radar screen of public attention, often experiencing long periods of latency between moments when political action in its favor is possible.

In most of the national stories told here, the country's key privacy moments came well in the past. A number of the authors have commented on this, usually rather nervously, where it has appeared that privacy concern appears to be waning. Graham Greenleaf notes how Australians, 20 years after their successful revolt against a national ID card, seem to be acquiescing to something very similar under a different name. Andre Vitalis reports that the CNIL has lost the veto power that it once had over privacy-related legislation. Wolfgang Kilian notes with disquiet the willingness of Germans to disseminate their personal data in reality TV shows – a development he seems to attribute to a generational weakening in privacy sensitivities, with the passing of post-war privacy consciousness. Ivan Szekely seems to detect that privacy sentiments in Hungarian public opinion, relatively strong just after the collapse of Soviet influence, seem to be attenuating in response to present-day Hungary's market economy.

To be sure, these observations are selective and anecdotal. But what does seem clear is that none of our authors, with the possible exception of Whon-Il Park in his reports on South Korea, reports 'privacy moments' in public opinion in the immediate past. The implication is that privacy institutions – the privacy commissions, and the laws that they enforce – may be living on the capital of public concern that dates to an increasingly distant past.

In any event, privacy-watchers debate among themselves whether the apparent attenuation of privacy concern in global public opinion represents an enduring, secular trend. An alternate interpretation is that it is mainly the youngest generation of computer users who have grown de-sensitized to providing their data to any and all would-be users – and that those now in their teens, 20s and early 30s will gradually come to regard such demands with more suspicion. The alternative is that the pervasiveness of such demands, and the seductions of succumbing to them, will effect life-long acquiescence to such practices.

This would be bad news for privacy interests. The last decade seems to have generated more than its share of what one might call 'anti-privacy moments' – moods in public opinion characterized by willingness to let more and more personal data slip out of individual control. The shock of mass terrorism in Europe and North America have been one impetus to such moods,

though hardly the only one. What the last ten years do not seem to have yielded is more moments like Watergate in the United States or the revolt against excessive Census demands in Germany – dramas that sharpen the public's immune reactions against privacy invasion, and consolidate the institutions and practices built upon such reactions.

Of course, all this could change. The United States faces at the time of this writing what is likely to be an agonizing national reckoning over the failures of its invasion of Iraq, and the domestic excesses of its so-called War on Terrorism. Public indignation could well rise in this country, as it did during Watergate, with eventual discoveries of privacy abuses almost certainly carried out under the Bush administration. Such sentiments could in turn fuel demands for stronger privacy institutions in this country – perhaps even including creation of a privacy commission and commissioner. Similar revivals of privacy sentiments are imaginable in other countries, as well.

But such possibilities are matters of speculation. In the absence of further privacy moments, privacy concerns are bound to remain a minority phenomenon in public opinion in most democracies. And this will continue to pose problems for defense of the values embodied in privacy codes – all of which ultimately require support in public opinion.

## LOOKING AHEAD

Let us imagine how the dynamics of privacy as a public issue might unfold in future decades. What are the best hopes that privacy advocates can reasonably entertain? And what do we most have to fear?

I want to suggest that any response to these questions must take into consideration two quite different forms of variation in social and political life.

One is variation in the broader climate of public sensitivity and political receptiveness to privacy concerns just discussed. The most we can say for sure is that every country appears subject to fluctuations in national sentiment between authoritarian and liberal poles. Historians of the United States, for example, have long identified the period after the First World War and the anti-communist obsessions of the 1950s as relatively illiberal periods – periods, not incidentally, when government data-gathering powers over individuals were abused. The period from the mid-1960s to the late 1970s, by contrast, appear in American history as relatively anti-authoritarian and supportive of civil liberties – and also favorable to privacy interests. Similar alternations could easily be demonstrated in the lives of many other nations.

Some observers take comfort in the cyclical character of these patterns. Even if liberal values like privacy protection go into eclipse for certain periods, they might observe, such losses are not irreversible. Public support for

protection of individual rights *vis à vis* institutional prerogatives eventually reassert themselves. Thus even if privacy guarantees are bent and bypassed in periods of anxiety over terror, the reasoning goes, public reaction against authoritarian excesses will in the long run redress the losses.

But this soothing interpretation misses something crucial – another trend in the evolving social role of personal information that is not so much fluctuating as uni-directional. This is the secular trend toward ever closer monitoring of individuals' lives – for purposes ranging from the most banal administrative ones to those of political repression. As the chapters of this book have attested, both government and private-sector institutions constantly find new ways to track and record new moments of ordinary people's everyday lives. One impetus to these trends is obviously technological innovation. But no less important is the sheer ingenuity of managers and planners in turning technological possibilities into effective, and profitable, routines for turning personal information into bases for deciding how to treat people. Data-mining, analysis of consumption patterns, tracking of travelers' movements, and countless other routines continue to enhance the grip of government and private institutions on the lives of those they deal with.

To be sure, such innovations take somewhat different forms and move at different rates in different countries. In some countries, at some points, they are blocked by privacy-related concerns – as in the case of consumer credit data in Australia and France. But it appears rare for the trend to go in reverse – that is, for established compilations of personal information to be liquidated. Thus the sheer amount of personal data 'at risk' of misappropriation and abuse seems to grow without limit. And rollbacks in the growth of such systems – that is, cases where effective means for collecting, organizing and using personal information to support major institutional decision-making efforts are actually dismantled, after operating successfully – appear extremely rare. Thus it is hard to believe that the uses of personal data instated in the name of the so-called 'War on Terror' will be dispensed with, even if threats of terrorism actually subside.

The capacities of these systems to shape people's lives – for better, but also for worse – inevitably raise the stakes for privacy concerns. Like the Dutch population records that proved so dangerous when the German occupiers turned them to destructive purposes, their negative potentials may be far from the minds of those who compile them. But privacy-watchers must always ponder the worst-case scenarios in these matters. The more personal information is stored and available, the larger is the scope for destruction, should repressive intent gain the upper hand.

Thus privacy-watchers face a severe challenge, if they view their work in the long historical perspective. The best way of forestalling disastrous misuses of personal data appears to lie not in creating safeguards for its lawful use – so much as in avoiding its accumulation in the first place.

Charting strategy to this end is not easy. Even the most zealous privacy defenders will acknowledge the need for *some* personal data systems – including even some that will hardly be welcome to those tracked by them. Dealing with persons suspected, or convicted of serious crimes or terrorist acts will always require hard-headed surveillance measures. By the same token, consumers judged responsible for systematic refusal to pay legitimate obligations, or those who make insurance claims for identical losses over extended periods, warrant some systematic monitoring. It is impossible to imagine a world worth living in that categorically avoids forceful surveillance.

What privacy advocates *can* do is to urge new ground rules for public consideration of such systems. Too often, as the preceding chapters have shown, the criteria for creating new systems of personal data-management have been purely ones of institutional efficiency. If personal data are available for collection, and if use of such data promises to be cost-effective for an established institution – if these conditions are met, no further justification for extending the coverage of individuals' lives appears necessary.

Privacy advocates should insist that the burden of justification be reversed. Systems for institutional recording and monitoring people's lives should never be undertaken without compelling, positive justification – and not simply in terms of the efficiency of the institutions involved. The steady growth and interlocking of such systems should be regarded as a dangerous thing in itself. The threshold requirement for their creation should be 'opt in', rather than simply 'opting out' from those that appear particularly noxious.

When such systems are held necessary, the same rigorous justification needs to apply to their operations. Without compelling need, no single item of personal information should be retained. The fact that personal data collected for one purpose might someday be useful for another, for example, should never be held to suffice for their indefinite retention. Without meaningful consent from the individual, institutional archiving of *any* personal information has to be regarded as an infringement on the rights of that individual.

Critics will be quick to point out that these ideas are not new; indeed they have been themes of many privacy codes since the earliest debates on these subjects. But the fact that the ideas are familiar can hardly be grounds for discounting them – particularly if they have rarely been conscientiously applied. In fact, there are no principles of privacy protection that promise good results, in the absence of forceful public support. In fact, if these chapters demonstrate anything, it is that there *are* no such principles. Only good practices backed by active public concern can provide hope of countervailing against the endless erosion of privacy.

Let us hope that this work has contributed to such informed concern.

# Bibliography

---

- Abernathy, W. & L.Tien (2002). *National identification system: A solution in search of a problem*. Electronic Frontier Foundation. Available online at: <http://www.eff.org/Privacy/Surveillance/nationalidsystem.html>
- Act No. V of 1878. (Csemegi Codex). *A magyar büntetőtörvénykönyv a buntettekrol és vétségekrol*. [Hungarian penal code of criminal acts and offences]
- Alpert, S.A. (2003). 'Protecting medical privacy: Challenges in the age of genetic information'. *Journal of Social Issues*, 59(2), pp. 301–322.
- ALRC (Australian Law Reform Commission) (2007). *Review of Australian Privacy Laws Discussion Paper*, 72.
- American Civil Liberties Union (ACLU). (2004, May 20). *New documents obtained by the ACLU raise troubling questions about MATRIX program* (ACLU Issue Brief No. 2). Available online at: <http://www.aclufl.org/pdfs/Whitepaper%20on%20new%20MATRIX%20docs%20-FINAL.pdf>
- American Library Association (ALA). (2002, January 19). *Guidelines for librarians on the USA PATRIOT Act: What to do before, during and after a 'knock at the door?'*. Washington DC: ALA. Available online at: <http://www.ala.org/ala/washoff/woissues/civilliberties/theusapatriotact/patstep.pdf>
- Andrews, E.L. (1999, May 27). 'Europe and US are still at odds over privacy' [Electronic version]. *The New York Times*. Available online at: <http://www.nytimes.com/library/tech/99/05/biztech/articles/27europe-us-privacy.html>
- APF (Australian Privacy Foundation) (2007a). *BOPTA: Blame it on the Privacy Act*, available online at <http://www.privacy.org.au/Resources/BOPTA.html>
- Armatte, E. (2001). 'Informatique et libertés: 30 ans de débats'. In *Mémoire de DEA de Sociologie*. Paris: Université Paris V.
- Art. 6 EGBGB. [Introductory Statute for the German Civil Code]
- Article 29 Committee, Data Protection Working Party (2001). *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, available online at: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2001/wp40en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp40en.pdf)
- Article 29 Data Protection Working Party. (1998). *Transfers of personal data to third countries: Applying articles 25 and 26 of the EU Data Protection Directive* (WP 125025/98). Available online at: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/1998/wp12\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf)

- Asia-Pacific Economic Cooperation (APEC). (2004). *APEC privacy framework*. Available online at: <http://www.asianlii.org/apec/other/agrmt/apf209/>
- Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2002) 208 CLR 199. Available online at: <http://www.austlii.edu.au/>
- Australian Law Reform Commission (ALRC). (1983). *Privacy* (ALRC Report 22). Available online at: <http://www.austlii.edu.au/au/other/alrc/publications/reports/22/>
- Australian Privacy Foundation (APF). (2005). *2006 census proposals*. Available online at: <http://www.privacy.org.au/Campaigns/Census/>
- APF (2005a). *Anti-Terrorism Bill (No 2) 2005* (Submission by the APF). Available online at: <http://www.privacy.org.au/Papers/SenLCCTerror-sub165.pdf>
- APF (2005b). Letter to all Australian Privacy Commissioners. Available online at: <http://www.privacy.org.au>
- APF (2005c). *Bigger Brother signals the death of financial privacy* (Media Release). Available online at: <http://www.privacy.org.au/Media/index.html>
- APF (2005d). *Electronic health records*. Available online at: [http://www.privacy.org.au/Campaigns/E\\_Health\\_Record/index.html](http://www.privacy.org.au/Campaigns/E_Health_Record/index.html)
- APF (2007). *Australian privacy foundation*. [Homepage] Available online at: <http://www.privacy.org.au/>
- Barrier, G. (2003). *Cybercontrôles: Veille numérique et surveillance en ligne*. Paris: Editions Apogée.
- Basic Law of the Hong Kong Special Administrative Region*, Seventh National People's Congress of the People's Republic of China, Third Session (1990, April 4).
- Baudry, P., C. Sorbets & A. Vitalis (2002). *La vie privée à l'heure des médias*. Bordeaux, France: Presses Universitaires de Bordeaux.
- Beck, U. (1986). *Risikogesellschaft*. Frankfurt am Main: Suhrkamp.
- Belloeil, A. (2001). *E-privacy. Le marché des données personnelles: protection de la vie privée à l'âge d'internet*. Paris: Dunod.
- Bennett, C.J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca, NY: Cornell University Press.
- Bennett, C.J. & C.D. Raab (2006). *The governance of privacy: Policy instruments in global perspective*. Cambridge, MA: MIT Press, 2nd edn.
- Berlau, J. (2003, November). 'Show us your money: The USA PATRIOT Act lets the feds spy on your finances.' *Reason*, 35(6), pp. 22–30.
- Berthold, M. & R. Wacks (1997). *Data privacy law in Hong Kong*. Hong Kong: Pearson Professional Limited.
- Berthold, M. & R. Wacks (2002). *Hong Kong data privacy law: Territorial regulation in a borderless world*. Hong Kong: Thomson, Sweet & Maxwell Asia.

- Besser, L. & A. Clennell (2007, July 9). 'Take train, smile for the camera.' *Sydney Morning Herald*.
- BGH NJW [Neue Juristische Wochenschrift] 1978, 2151. [Decisions of the German Federal High Court]
- BGH RDV 2005, 62.
- BGHZ 30, 7 (*Caterina Valente*). [Decisions of the Federal High Court in Civil Cases]
- BGHZ 50, 133 (*Mephisto*).
- BGHZ 131, 332 (*Caroline v Monaco II*).
- BGHZ 143, 214 (*Marlene Dietrich*).
- BGHZ 162, 1.
- Big Brother Awards (2007, April 5). *Archiv*. Available online at: <http://www.bigbrotherawards.de/archive>
- Bill of Rights Ordinance* (BORO). Chapter 383, Laws of Hong Kong (1991).
- Birkelbach, W. (1974). *IBM-Nachrichten*, pp. 241 et seq., 333 et seq.
- Bizer, J., B. Luterbeck & J. Rieß (eds) (2002). *Freundesgabe für Alfred Büllersbach*. Stuttgart.
- Braibant, G. (1998). *Données personnelles et société de l'information*. Paris: La Documentation Française.
- Brenton, M. (1964). *The privacy invaders*. New York: Coward-McCann.
- Bromberg, T. (2004, March). 'Investigating employee misconduct in the age of privacy law.' *Journal of Workplace Trends*.
- Buchanan, A.E. (1989, July). 'Assessing the communitarian critique of liberalism.' *Ethics*, 99(4), pp. 852–882.
- Bull, H.P. (2006). 'Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?' *Neue Juristische Wochenschrift*, 1617–1624.
- Bundestags-Drucksache VI/2885; Bundestags-Drucksache VII/1027.
- Burnham, D. (1983). *The rise of the computer state*. New York: Random House.
- Bushkin, J. (2000, April 17). 'Our data, ourselves.' *The Wall Street Journal*, p. R34.
- BVerfG 4. April 2006 1BvR 518/02 NJW 2006, 1939. [Decisions of the German Federal Constitutional Court]
- BVerfG 4.4.2006 1BvR 518/02, NJW 2006, 1939–1951.
- BVerfGE 65,1 – Census Case (Volkszählungsurteil).
- BVerfGE 112, 304 (GPS-Observation).
- BVerfGE 113, 348.
- BVerfG NJW 1999, 55.
- BVerfG NJW 2000, 55 = BVerfGE 109, 279.
- BVerfG NJW 2004, 999.
- BVerfG NJW 2004, 2213 = BVerfGE 110, 33.

- BVerfG NJW 2005, 1338 = BVerfGE 112, 304.
- BVerfG NJW 2005, 1917 = BVerfGE 113, 29.
- BVerfG NJW 2006, 976.
- BVerfG NJW 2006, 1939.
- BVerfG Urt. v 27.7.2005 1 BvR 668/04, MMR 2005, 674.
- BVerwG 22.10.2003 NJW 2004, 1191. [German Federal Administrative Court Decisions]
- BVerwG NJW 2006, 1116.
- Bygrave, L.A. (1998). 'Data protection pursuant to the right to privacy in human rights treaties.' *International Journal of Law and Information Technology*, 6, pp. 247–284.
- Bygrave, L.A. (2000). 'Determining applicable law pursuant to European data protection legislation.' *Computer Law & Security Report*, 16, pp. 252–257.
- Bygrave, L.A. (2002). *Data protection law: Approaching its rationale, logic and limits*. The Hague, London, New York: Kluwer Law International.
- Cadoux, L. (1996). *Voix, images et protection des données personnelles* (Rapport Commission Nationale de L'informatique et des Libertés). Paris: La Documentation Française.
- Campbell, D. (2001). *Surveillance électronique planétaire*. Paris: Allia.
- Campbell v. MGN Ltd* [2004] UKHL 22 (6 May 2004), available at <http://www.bailii.org/uk/cases/UKHL/2004/22/html>
- Cantril, A.H. & S.D. Cantril (1994). *Live and let live: American public opinion at home and at work*. New York: American Civil Liberties Union Foundation.
- Carse, D. (Deputy Chief Executive, Hong Kong Monetary Authority) (1999, January 27). Unpublished speech.
- Center for Media Education (CME). (1998, June 4). *Children's advocates call for national privacy policy to protect children online* (Press release). Available online at: <http://www.cme.org/cme>
- Centre de Coordination pour la Recherche et l'Enseignement en Informatique et Société (CREIS). (2004). *25 ans de critique de l'informatisation*. Paris: Colloque Université Paris 6.
- CREIS. (1991). *Informatique et libertés: nouvelles menaces, nouvelles solutions* (Actes colloque). Nantes: laboratoire LIANA, Université de Nantes.
- Charlesworth, A. (2000). 'Clash of the data titans? US and EU data privacy regulation.' *European Public Law*, 6(2), pp. 253–274.
- Charlesworth, A. (2003). 'Information privacy law in the European Union: E pluribus unum or ex uno plures?' *Hastings Law Journal*, 54, pp. 931–969.
- Chosun-Ilbo* (2005, November 1). 'New Internet identification to protect privacy.' *The Chosun-Ilbo* [English edition].
- Chosun-Ilbo*, 'Juvenile gamers are on the brink of becoming criminals.' (2006, September 15). *The Chosun-Ilbo*.

- Chulov, M. & A. Hodge (2005, July 26). 'All eyes are on you.' *The Australian*, available online at <http://www.theaustralian.news.com.au/story/0,25,97,160457832-28737,00.html>.
- Chung, Y.S. & H.E. Kim (2004). 'Unauthorized use of resident registration numbers and privacy protection.' *Internet Law Journal*, 3(2).
- Clarke, R. (1988, January). 'Just another piece of plastic for your wallet: The "Australia Card" scheme.' *Computers & Society*, 18(1), 7–21.
- Clarke, R. (1988, July), 'Addendum (to 'Just Another Piece of Plastic').' *Computers & Society*, 18(3), 7–21.
- Clarke, R. (2002). *A history of privacy in Australia*. Available online at <http://www.anu.edu.au/people/Roger.Clarke/DV/OzHistory.html>
- Commission Nationale de l'Informatique et des Libertés (CNIL) (1975). *Rapport tricot et annexes*. Paris: La Documentation Française.
- CNIL (1980–2005). *Rapport annuel* (published separately). Paris: La Documentation Française.
- CNIL (1998). *Les libertés et l'informatique. Vingt délibérations commentées*. Paris: La Documentation Française.
- CNIL (2001). *La cybersurveillance des salariés dans l'entreprise* (Rapport d'étude). Paris: CNIL.
- CNIL (2005), *Informatique: servitude on libertés?*, Paris: CNIL.
- Cotts, C. (2003, October 29). 'Wolves in sheep's clothing: The journalists who would be CEOs.' *The Village Voice*. Available online at: <http://www.villagevoice.com/issues/0344/cotts.php>
- Couch v United States*, 409 US 322 (1973).
- Council of Europe (1985, October 1). 'Convention for the protection of individuals.' *European Treaty Series No. 108*.
- Court of the European Union. (2006, October 16). Press Release 14006/06/288.
- Cowen, Z. (1969). 'The private man.' *The Boyer Lectures*. Sydney: Australian Broadcasting Commission.
- Craig, P. and G. de Búrca (2008). *EU Law*, Oxford: Oxford University Press.
- Cripps, A. (2004). *Workplace surveillance*. (Paper submitted to NSW Council for Civil Liberties). Available online at: <http://www.nswccl.org.au/docs/pdf/workplace%20surveillance.pdf>
- Datalag, SFS 1973, 289. [Swedish Code of Statutes]
- Delahaie, H. & F. Paoletti (1987). *Informatique et libertés*. Paris: La Découverte.
- Dempsey, J.X. (2002, Winter). 'Civil liberties in a time of crisis.' *Human Rights Magazine*, 29. Available online at: <http://www.abanet.org/irr/hr/winter02/dempsey.html>
- Deutsche Rentenversicherung (2003, December). [German social security administration]. Available online at [www.deutsche-rentenversicherung.de](http://www.deutsche-rentenversicherung.de)

- Dhont, J., M.V. Pérez Asinari, Y. Pouillet, J.R. Reidenberg & L.A. Bygrave (2004, April 19). *Safe harbour decision implementation study* (Report for the European Commission, Study Contract PRS/2003/AO-7002/E/27). Available online at: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/studies/safe-harbour-2004\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf).
- Dix, A. (1996, September). *Fallstudie: Nordamerika und die Europäische Richtlinie*. Available online at: [www.datenschutz-berlin.de/doc/int/konf/18/bahn\\_de.htm](http://www.datenschutz-berlin.de/doc/int/konf/18/bahn_de.htm)
- Doe v Australian Broadcasting Corporation & Ors* [2007] VCC 281. Available online at: <http://www.austlii.edu.au>
- Doyle, C. (2003, February 26). 'Libraries and the USA PATRIOT Act.' *Congressional Research Service Report for Congress*.
- EFA (1994), Electronics Frontiers Australia website, established 1994, at <http://www.efa.org.au>
- Eberle, E.J. (2002), *Dignity and Liberty: Constitutional Visions in Germany and the United States*, Westport, Connecticut: Praeger.
- Eger, J.M. (1978). 'Emerging restrictions on transborder data flow: Privacy protection or non-tariff trade barriers.' *Law and Policy in International Business*, 10, pp. 1055–1103.
- Eisenstadt v Baird*, 405 US 438 (1972).
- Ellger, R. (1990). *Der Datenschutz im grenzüberschreitende Datenverkehr: eine rechtsvergleichende und kollisionsrechtliche Untersuchung*. Baden-Baden, Germany: Nomos Verlagsgesellschaft.
- Ellger, R. (1991a). 'Datenschutzgesetz und europäischer Binnenmarkt (Teil 1).' *Recht der Datenverarbeitung*, pp. 57–65.
- Ellger, R. (1991b). 'Datenschutzgesetz und europäischer Binnenmarkt (Teil 2).' *Recht der Datenverarbeitung*, pp. 121–135.
- Elmajzoub, M. (2004). *La gestion des données personnelles dans le secteur de la police en Europe*. Thèse de Droit, Université de Montpellier I.
- EPIC and Privacy International. (2001). *Privacy and human rights: An international survey of privacy laws and developments*. Washington, DC: EPIC.
- EPIC (Electronic Privacy Information Centre) (2005). 'Country Report – Hong Kong', *Privacy and Human Rights 2005*, EPIC, Washington.
- EPIC (2002, February). *Your papers, please: From the state drivers license to a national identification system* (Watching the Watchers – Policy Report No. 1). Available online at: [http://www.epic.org/privacy/id\\_cards/yourpapersplease.pdf](http://www.epic.org/privacy/id_cards/yourpapersplease.pdf)
- Etzioni, A. (1999). *The limits of privacy*. New York: Basic Books.
- European Commission (2003, May 15). *Report from the commission: First report on the implementation of the Data Protection Directive (95/46/EC)* (COM(2003) 265 final). Brussels: EC. Available online at: [http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003\\_0265en01.pdf](http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf).

- Farrell, H. (2002). 'Negotiating privacy across arenas: The E.U.–U.S. "safe harbor" discussions'. In A. Héri-tier (ed.), *Common goods: Reinventing European and international governance* (pp. 105–126). Lanham and Oxford, England: Rowman & Littlefield.
- Federal Trade Commission (FTC) (1998). *Privacy online: A report to congress*. Available online at: <http://www.ftc.gov/reports/privacy3/toc.htm>
- Flaherty, D.H. (1989). *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, NC: UNC Press.
- Ford, P. (2003). 'Implementing the EC directive on data protection – an outside perspective.' *Privacy Law & Policy Reporter*, 9, pp. 141–149.
- Frayssinet, J. (1992). *Informatique, fichiers et libertés*. Paris: Litec.
- Fried, C. (1968, January). 'Privacy.' *Yale Law Journal*, 77(3), pp. 475–93.
- Froomkin, A.M. (2000, May). 'The death of privacy'. *Stanford Law Review*, 52(5), pp. 1461–1543.
- Gandy, O.H. (1993). *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview Press.
- Geiger, H. (1989). 'Europäischer Informationsmarkt und Datenschutz.' *Recht der Datenverarbeitung*, 5, pp. 203–210.
- General Accounting Office (GAO) (2004, February). *Aviation security: Computer-assisted passenger prescreening system faces significant implementation challenges* (GAO-04-385). Available online at: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-385>
- Gesetz- und Verordnungsblatt für das Land Hessen, Tiel 1, p. 625 (1970).
- Ghai, Y. (1999). *Hong Kong's new constitutional order: The resumption of Chinese sovereignty and the Basic Law* (2nd edn). Hong Kong: Hong Kong University Press.
- Ginsburg, T. (2004). 'The politics of legal reform in Korea'. In T. Ginsburg (ed.), *Legal reform in Korea*. New York: Routledge Curzon.
- Giro, J.L. (ed). (2005). *Le harcèlement numérique*. Paris: Dalloz.
- Government of Hong Kong, Departments and General Division, Administrative Services and Information Branch. (1988, March). *Data protection principles and guidelines*. Hong Kong: Author.
- Graham, G. (2005a). 'APEC Privacy Framework completed: No threat to privacy standards.' *Privacy Law & Policy Reporter*, 11(8).
- Greenleaf, G. (1987). 'The Australia Card: Towards a national surveillance system.' *Law Society Journal (NSW)*, 25(9), p. 24.
- Greenleaf, G. (1987a). 'Lessons from the Australia Card – deux et machina?', *Computer Law and Security Report*, 3(6).
- Greenleaf, G. (1987b). 'The Australia Card: Towards a National Surveillance System', *Law Society Journal (NSW)*, 25, (9).

- Greenleaf, G. (1988, March/April). 'Lessons from the Australia Card – deux ex machina?' *The Computer Law and Security Report*, 3(6), p. 6.
- Greenleaf, G. (1992). 'The most restrictive credit reference laws in the western world?' *Australian Law Journal*, 66, p. 672.
- Greenleaf, G. (1995). 'European privacy directive and data exports.' *Privacy Law & Policy Reporter*, 2, pp. 105–108.
- Greenleaf, G. (1996). 'Privacy and cyberspace – an ambiguous relationship', *Private Law and Policy Reporter*, 88(3), available online at <http://www.aust/ii.edu.au/au/journals/PLPR/19965/48/html>
- Greenleaf, G. (1998). 'Privacy and consumer organisations withhold endorsement of "National Principles".' *Privacy Law & Policy Reporter*, 5(3), pp. 41–43.
- Greenleaf, G. (1999). 'A new era for public sector privacy in NSW.' *Privacy Law & Policy Reporter*, 5(7), p. 130.
- Greenleaf, G. (2000). 'Private sector bill amendments ignore EU problems.' *Privacy Law & Policy Reporter*, 7(3), p. 30.
- Greenleaf, G. (2000a). 'Reps Committee protects the "privacy-free zone".' *Privacy Law & Policy Reporter*, 7(1), p. 16.
- Greenleaf, G. (2000b). 'Safe harbor's low benchmark for "adequacy": The EU sells out privacy for US\$.' *Privacy Law & Policy Reporter*, 7, pp. 45–47.
- Greenleaf, G. (2000c). 'Victoria's privacy bill still sets the standard.' *Privacy Law & Policy Reporter*, 7(2), p. 24.
- Greenleaf, G. (2001). '“Tabula rasa”: Ten reasons why Australian privacy law does not exist.' *University of New South Wales Law Journal*. 24(1), p. 262.
- Greenleaf, G. (2002, October 28). *Submission on the smart ID Card and the Registration of Persons (Amendment) Bill 2001* (Submission to Bills Committee on Registration of Persons (Amendment) Bill). Hong Kong Legislative Council. Available online at: <http://www2.austlii.edu.au/privacy/articles/hkidcard/>
- Greenleaf, G. (2003). 'Australia's APEC privacy initiative: the pros and cons of "OECD lite".' *Privacy Law & Policy Reporter*, 10, pp. 1–6.
- Greenleaf, G. (2003a). 'Reforming reporting of privacy cases: A proposal for improving accountability of Asia-Pacific Privacy Commissioners.' In P. Roth (ed.), *Privacy law and policy in New Zealand*. Wellington, New Zealand: Butterworths LexisNexis. (forthcoming) Available online at: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=512782](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=512782)
- Greenleaf, G. (2005). 'Implementation of APEC's Privacy Framework.' In D.H.A. Raman Saad (ed.), *Personal data protection in the new millenium*, *LexisNexis Malayan law journal*.
- Greenleaf, G. (2006). 'APEC's privacy framework sets a new low standard for the Asia-Pacific.' In A.T. Kenyon & M. Richardson (eds), *New dimensions*

- in privacy law: International and comparative perspectives*. Cambridge, UK: Cambridge University Press.
- Greenleaf, G. (2006a). 'UNESCO starts Asia-Pacific response to Montreux declaration.' *Privacy Law & Policy Reporter*, 11, p. 219.
- Greenleaf, G. (2007). 'Australia's proposed ID card: Still quacking like a duck.' (UNSWLRS 1, UNSW Law Research Paper No. 2007-1). *Computer Law & Security Report*, 23(4), 332–41.
- Greenleaf, G. (2007a). 'Access all areas: Function creep guaranteed in Australia's ID card bill (No. 1).' *Computer Law & Security Report*, 23, 4, 332–41.
- Greenleaf, G. (2007b). 'Function creep defined but still dangerous in Australia's ID Card Bill', *Computer Law & Security Report*, 24(1), 56–66.
- Greenleaf, G. (2007c). 'Australia's privacy law revolution? – The ALRC proposals, 2007, *Privacy Law and Business International Newsletter*, 89, 19–21.
- Greenleaf, G. (2008). 'Hong Kong's "smart" ID card: Designed to be out of control', in D. Lyon and C. Bennett, *Playing the Identity Card*, Routledge (in publication).
- Greenleaf, G. & J. Nolan (1986). 'The deceptive history of the Australia Card.' *The Australian Quarterly*, 58(4), p. 407.
- Greenleaf, G. & N. Waters (2003). 'NSW to scrap Privacy Commissioner, reduce privacy protection.' *Privacy Law & Policy Reporter*, 10(6), p. 101.
- GRID, R. Laperrière & P. Péladeau (1986). *L'identité piratée*. Montreal: SOQIJ.
- Griswold v Connecticut*, 381 US 479 (1965).
- Grosso v United States*, 390 US 62 (1968).
- Hammit, H. (1997, December 1). 'States to feds: We don't want your legislated privacy.' *Government Technology*. Available online at: <http://www.govtech.com/gt/95513>
- Harris, Louis and Associates & A.F. Westin (1988). 'E-commerce and privacy: What net users want', Hackensack, NJ: Privacy and American Business.
- Hartley, T.C. (1998). *The foundations of European Community law*. Oxford: Clarendon Press.
- Hauser, D. (1998). *Baader and Herold. Beschreibung eines Kampfes*. Frankfurt am Main: Fischer.
- Hayden, T. (1978, February). 'The privacy commission report: A national privacy program.' *Privacy Report*, 5.
- Heimann, E. & A. Vitalis (1996). *Nouvelles technologies, nouvelles régulations* (Rapport de recherche IHESI/CNRS). Strasbourg, France: Rapport Gersulp/Pirvilles/IHESI.
- Heisenberg, D. (2005). *Negotiating privacy: The European Union, The United States, and personal data protection*. Boulder, CO: Lynne Rienner Publishers.

- Henke, F. (1986). *Die Datenschutzkonvention des Europarates*. Frankfurt am Main, Bern and New York: Peter Lang.
- Hessisches Datenschutzgesetz. GVB I, p. 625. (1970, October 7). [The Hesse Data Protection Act]
- HEW (1973). Department of Health, Education and Welfare (1973). Secretary's advisory committee on automated personal data systems. *Records, Computers and the rights of citizens*. Washington, DC: Government Printing Office.
- Hijmans, H. (2006). 'The European data protection supervisor: The institutions of the EC controlled by an independent authority.' *Common Market Law Review*, 43, pp. 1313–1342.
- Hockeimer, Jr., H. E. (2002, April 15). 'USA PATRIOT Act is broader than you imagine; from libraries to universities to trucking companies, sweeping provisions of the act change the status quo.' *New Jersey Law Journal*, 168(3), p. 29.
- Hoffsaes, C. & A. Vitalis (1995). Les hommes-numéros. 'La Recherche'.
- Hondius, F.W. (1975). *Emerging data protection in Europe*. Amsterdam: North Holland Publishing Company.
- Hondius, F.W. (1983). 'A decade of international data protection.' *Netherlands International Law Review*, 30, pp. 103–128.
- Hong Kong Chief Executive, *The Enforcement (Covert Surveillance) Order*, S.S. No. 5 to Gazette No. 31/2005.
- Hong Kong District Court, DCCC 689 of 2004. [Unreported judgment of Judge Sweeney of 22 April 2005]
- Hong Kong Law Reform Commission (HKLRC) (1994). *Reform of the law relating to the protection of personal data*. Available online at: <http://www.hklii.org/hk/other/hklrc/reports/>
- HKLRC (1996) *Privacy: Regulating the interception of communications*. Available online at: <http://www.hklii.org/hk/other/hklrc/reports/>
- HKLRC. (2004). *Privacy and media intrusion*. Available online at: <http://www.hklii.org/hk/other/hklrc/reports/>
- HKLRC. (2004a). *Civil liability for invasion of privacy*. Available online at: <http://www.hklii.org/hk/other/hklrc/reports/>
- HKLRC (2006). *Privacy: The regulation of covert surveillance*. Available online at: <http://www.hklii.org/hk/other/hklrc/reports/>
- HKLRC (2006). *Privacy: The regulation of covert surveillance* [2006] HKLRC 1, March, available at <http://www.hklii.org/hk/other/hklrc/reports/2006/03/>
- Hong Kong Monetary Authority (HKMA) (1998, May). 'Credit reference agency'. *HKMA Quarterly Bulletin*.
- HKMA (2004, April 22). 'Viewpoint' (weekly article by the HKMA Chief Executive). *South China Morning Post*.

- HKMA. (2005). *Supervisory Policy Manuals*. Hong Kong: HKMA.
- Hong Kong Privacy Commissioner's Office (HKPCO). (1997). *Code of Practice on the identity card number and other personal identifiers*. Hong Kong: HKPCO. Available online at: [http://www.pcpd.org.hk/english/ordinance/code\\_id.html](http://www.pcpd.org.hk/english/ordinance/code_id.html)
- HKPCO (1997a). *Transfer of personal data outside Hong Kong: Some common questions (Fact Sheet No. 1)*. Available online at: [http://www.pcpd.org.hk/english/publications/fact1\\_intro\\_1.html](http://www.pcpd.org.hk/english/publications/fact1_intro_1.html)
- HKPCO (1998). *Code of Practice on consumer credit data*. Hong Kong: HKPCO.
- HKPCO (1999). *Annual report of the Privacy Commissioner 1998–99*. Hong Kong: HKPCO.
- HKPCO (2003). *Code of Practice on consumer credit data (Revised)*. Hong Kong: HKPCO. Available online at: [http://www.pcpd.org.hk/english/publications/files/CCDCode\\_eng.pdf](http://www.pcpd.org.hk/english/publications/files/CCDCode_eng.pdf)
- HKPCO (2004). *Annual report of the Privacy Commissioner 2003–04*. Hong Kong: HKPCO. Available online at: <http://www.pcpd.org.hk/english/publications/annualreport2004.html>
- HKPCO (2004b). *2004 opinion survey – Personal Data (Privacy) Ordinance: Attitudes and implementation – key findings*. Hong Kong: HKPCO. Available online at: <http://www.pcpd.org.hk/english/publications/opinionsurvey9.html>
- HKPCO (2005). *Annual report of the Privacy Commissioner 2004–05*. Hong Kong: HKPCO. Available online at: [http://www.pcpd.org.hk/english/publications/annualreport2005\\_flash.html](http://www.pcpd.org.hk/english/publications/annualreport2005_flash.html)
- HKPCO (2005a). *Work of the Office of the Privacy Commissioner for Personal Data*, Press Release, 17 August, Hong Kong: HKPCO, available online at [http://www.pcpd.org.hk/english/infocentre/press\\_20050817.html](http://www.pcpd.org.hk/english/infocentre/press_20050817.html)
- HKPCO (2005b). *The practice of collection of employees' personal data by pinhole camera*, 8 December, Hong Kong: HKPCO, available at [http://www.pcpd.org.hk/english/infocentre/files/RO5-7230\\_e.pdf](http://www.pcpd.org.hk/english/infocentre/files/RO5-7230_e.pdf)
- HKPCO (2005c). *Investigation report on a self-initiated case involving covert monitoring at work*, Press Release, 8 December, Hong Kong: HKPCO, available at [http://www.pcpd.org.hk/english/infocentre/press\\_20051208.html](http://www.pcpd.org.hk/english/infocentre/press_20051208.html)
- HKPCO (2006). *Must take security measures to protect personal data when engaging outsourced contractor (Report Number: R06-2599)*. Hong Kong: HKPCO. Available online at: [http://www.pcpd.org.hk/english/publications/files/IPCC\\_e.pdf](http://www.pcpd.org.hk/english/publications/files/IPCC_e.pdf)
- HKPCO (2006a). *Data protection principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's perspective*. Hong Kong: HKPCO.
- HKPCO (2007). *Complaint case notes and enquiry case notes*. Available online at: <http://www.pcpd.org.hk/english/casenotes/case.html>

- HKPCO (2007b). *The disclosure of email subscriber's personal data by email service provider to PRC Law Enforcement Agency (Report Number: R07-3619)*. Hong Kong: HKPCO. Available online at: [http://www.pcpd.org.hk/english/publications/files/Yahoo\\_e.pdf](http://www.pcpd.org.hk/english/publications/files/Yahoo_e.pdf)
- HKPCO (2007a). *Hong Kong Privacy Commissioner's Office*. [Homepage] Available online at: <http://www.pco.org.hk>
- Horne, D. (1966). *The Lucky Country*. Sydney: Penguin.
- Hosking v Runting* [2004] NZCA 34. [Legal materials from New Zealand] Available online at: <http://www.nzlii.org>
- Huet, J. & H. Maisl (1989). *Droit de l'informatique et des télécommunications*. Paris: Litec.
- Information Technology and Broadcasting Bureau (ITBB) (2001, December 20). *Non-immigration applications for incorporation into the Smart ID Card* (ITBB LegCo Panels briefing). Hong Kong: ITBB.
- ITBB (2002, July 4). *Update on non-immigration applications for incorporation into the smart ID card*. Hong Kong: ITBB.
- Jackson, M. (2001). *Hughes on data protection in Australia*. Pyrmont, NSW: Lawbook Co, 2nd edn.
- Jeong, J.H. (2005, December 10). *Legal issues on the internet real name system*. Paper presented at a seminar hosted by the Korean Internet Law Association.
- Johnston, A. (2004). 'Reviewing the NSW Privacy Act: Expectations and inadequacies'. *Privacy Law & Policy Reporter*, 11(3), p. 61.
- Johnston, A. (2004a). 'Reviewing the NSW Privacy Act: Enforcement'. *Privacy Law & Policy Reporter*, 11(4), p. 112.
- Johnston, A. (2005). 'Reviewing the NSW Privacy Act: Expectations and inadequacies', *Privacy Law & Policy Reporter*, 11.
- Johnston, A. (2005a). 'Reviewing the NSW Privacy Act: Enforcement', *Privacy Law & Policy Reporter*, 11.
- Joint Declaration of the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the People's Republic of China on the Question of Hong Kong* (Sino-British Declaration) (1985, December 19). Available online at: [http://usinfo.state.gov/eap/east\\_asia\\_pacific/china/hong\\_kong\\_joint\\_declaration.htm](http://usinfo.state.gov/eap/east_asia_pacific/china/hong_kong_joint_declaration.htm)
- JoongAng*, (2005, November 17). 'Ex-KCIA heads arrested for eavesdropping 1800 VIPs.' *JoongAng Daily*.
- JoongAng* (2005), (2005a, January 31). 'Korea's highest distribution rate of high-speed internet networks.' *JoongAng Daily*.
- Kant, I. (1903). 'Grundlegung zur Metaphysik der Sitten'. *Kants Werke Bd. IV, I. A. 1781*. Berlin: Akademie – Textausgabe.
- Karanja, S.K. (2006). *Schengen information system and border control co-operation: A transparency and proportionality evaluation*. Unpublished doctoral dissertation, University of Oslo, Norway.

- Karanja, S.K. (2008). *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*, Leiden/Boston: Martinus Nijhoff.
- Katz v United States*, 389 US 347 (1967).
- Katz, J. E. & A.R. Tassone (1990, Spring). 'Public opinion trends: Privacy and information technology.' *Public Opinion Quarterly*, 54 (2), pp. 125–143.
- Kent, S.T. & L.I. Millett (2002). *IDs – Not that easy: Questions about nationwide identity systems* (Report for the National Research Council). Washington, DC: National Academy Press. Available online at: [http://books.nap.edu/html/id\\_questions/](http://books.nap.edu/html/id_questions/)
- Kilian, W., K. Lenk, E. Steinmüller (eds) (1973). *Datenschutz*. Frankfurt am Main: S. Toeche-Mittler.
- Kilian, W. (1982). *Personalinformationssysteme in deutschen Großunternehmen*. Berlin, Heidelberg and New York: Springer-Verlag GmbH, 2nd edn.
- Kilian, W. (2002). 'Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung?' In J. Bizer, B. Luterbeck, J. Rieß (eds), *Freundesgabe für Alfred Büllsbach* (pp. 151–160). Stuttgart.
- Kilian, W., K. Lenk & W. Steinmüller (1973). *Datenschutz*. Frankfurt am Main: Toeche-Mittler.
- Kingdon, J. (1984). *Agendas, alternatives and public policies*. Boston: Little, Brown.
- Kirby, M.D. (1991). 'Legal aspects of transborder data flows.' *International Computer Law Adviser*, 5(5), pp. 4–10.
- Kirchner, J. (1981, December 14). 'Privacy: A history of computer matching in the federal government.' *Computerworld*, 15, pp. 1–16.
- Kirsch, W.J. (1982). 'The protection of privacy and transborder flows of personal data: The work of the Council of Europe, the Organization for Economic Cooperation and Development and the European Economic Community.' *Legal Issues of European Integration*, 2, pp. 21–50.
- Korean Briefing (2006, February 14). 'MIC steps up privacy protection.' Korean Government Briefing. Available online at: <http://news.go.kr>.
- Korea Herald (2001, July 19). 'Stricter privacy protection . . .' *The Korea Herald*.
- Korff, D. (2002). *Comparative summary of national laws*. (EC Study on Implementation of the Data Protection Directive. Study Contract ETD/2001/B5-3001/A/49). Available online at: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf)
- Kuner, C. (2003). *European data privacy law and online business*. Oxford, England: Oxford University Press.
- Kuner, C. (2007). *European Data Protection Law: Corporate Compliance and Regulation*, Oxford: Oxford University Press.

- Lam, T. (Acting Privacy Commissioner, Hong Kong). (2005) *Interview Notes* (Interview conducted by G. Greenleaf).
- Lamont v Postmaster General*, 391 U.S. 301 (1965).
- Langan, K.J. (1979). 'Computer matching programs: A threat to privacy?' *Columbia Journal of Law and Social Problems*, 15(2), pp. 158–159.
- Laudon, K.C. (1986). *Dossier society: Value choices in the design of national information systems*. New York: Columbia University Press.
- Lawson, P. (2007), 'APEC provides second-class privacy protection', *Privacy Laws & Business*, 89, 13–14.
- Lee, M. (2002). Submission to Bills Committee on Registration of Persons (Amendment) Bill, Hong Kong Legislative Council [CB(2)2785/01–02(02)], 11 October.
- Lee, L.T. (2003). 'The USA PATRIOT Act and telecommunication: Privacy under attack.' *Rutgers Computer and Technology Law Journal*, 29, pp. 371–403.
- Lemoine, P. (1981). *Informatisation et société*. Paris: Cours IEP de Paris.
- LG Magdeburg DuD 2006, 375.
- LG München 1.2.2001 12 0 13009/00. [German district court decision]
- Lilly, J.R. (2003). 'National security at what price?: A look into civil liberty concerns in the information age under the USA PATRIOT Act of 2001 and a proposed constitutional test for future legislation.' *Cornell Journal of Law and Public Policy*, 12(2), pp. 447–471.
- Linowes, D. F. (1989). *Privacy in America: Is your private life in the public eye?* New York: Simon and Schuster.
- Long, E. (1967). *The Intruders*. New York: Praeger.
- Lucas, A., J. Deveze & J. Frayssinet (2001). *Droit de l'informatique et de l'internet*. Paris: PUF.
- Lukas, A. (2001, October 30). *Safe harbor or stormy waters? Living with the EU Data Protection Directive* (Trade Policy Analysis Paper no. 16). Washington, DC: Cato Institute.
- Lyon-Caen, G. (1991). *Les libertés publiques et l'emploi* (Rapport au ministre du travail). Paris: Ministre du Travail.
- Maglio, M. (2003). 'An economic analysis of the right to privacy.' *Computer und Recht International*, 4, p. 103.
- Maisl, H. & A. Vitalis (1985). 'Les libertés, enjeu d'une société informatisée.' *Études*, 4.
- Maisl, H. & A. Vitalis (1993). 'Protection de la personne face aux techniques de communication.' *Dictionnaire critique de la communication* (Tome 2). Paris: PUF.
- Majtényi, L. (1998). *The first three years of the Parliamentary Commissioner for Data Protection and Freedom of Information*. Budapest: Office of the Parliamentary Commissioner for Data Protection and Freedom of Information.

- Malanczuk, P. (2001). 'The European Directive on Data Protection and the U. S. "Safe Harbour Principles".' In R. Briner. (et al.) (eds), *Recht der Internationalen Wirtschaft und Streiterledigung im 21.* Köln: Heymanns.
- Martin, K. (2003). 'The USA PATRIOT Act's application to library patron records.' *Journal of Legislation*, 29, pp. 283–306.
- Marx, G. & N. Reichman (1984, March–April). 'Routinizing the discovery of secrets: Computers as informants.' *American Behavioral Scientist* 27(4), pp. 423–452.
- Mayer, T. (2001, January 22). 'Überwachung bei der Fußball-WM 2006.' *Der Grosse Bruder*. Available online at: [www.dergrossebruder.org/miniwahr/20050122173000.html](http://www.dergrossebruder.org/miniwahr/20050122173000.html)
- McDermott, Q. (2005, August 15). 'Your money and your life.' In *Four corners* (Australian Broadcasting Corporation television program). Sydney: Australian Broadcasting Corporation.
- McGuire, R.P. (1979–80). 'The information age: An introduction to transborder data flow.' *Jurimetrics Journal*, 20, pp. 1–7.
- McLeish, R. (2000). 'Hong Kong', In *World encyclopedia of data protection*. The Hague: Kluwer.
- Meller, P. (2007, February 1). 'Europe preps for battle with U.S. over traveler data.' *IDG News Service*. Available online at: [http://www.infoworld.com/article/07/02/01/HNBattleontravelerdata\\_1.html](http://www.infoworld.com/article/07/02/01/HNBattleontravelerdata_1.html)
- Michael, J. (1994). *Privacy and human rights: An international and comparative study, with special reference to developments in information technology*. Paris and Aldershot: UNESCO/Dartmouth Publishing Company.
- Miller, A.R. (1971). *The assault on privacy: Computers, data banks, and dossiers*. Ann Arbor, MI: University of Michigan Press.
- Moore, S. (1997, May 13). *A national identification system* (Testimony before the US House of Representatives, Subcommittee on Immigration and Claims, Judiciary Committee). Available online at: <http://www.cato.org/testimony/ct-sm051397.html>.
- Morgan, Roy (2004). *Community attitudes towards privacy*. Paper prepared for the Office of the Federal Privacy Commissioner, Sydney, Australia. Available online at: <http://www.privacy.gov.au/publications/rcommunity04.pdf>
- Morison, W.L. (1973). *Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys-General* (Report No. 170/1973). Canberra, Australia: AGPS.
- NAACP v Alabama*, 357 US 449 (1958).
- New South Wales Privacy Committee. (1975–1999). *Annual report* (annual from 1975–99). Sydney, Australia: Privacy Committee.
- New York Times Editorial Board. (2004 May 16). 'A national ID.' *The New York Times*, Section A, p. 16.

- Niblett, G.B.F. (1971). *Digital information and the privacy problem* (OECD Informatics Studies No. 2). Paris: OECD.
- NJW 1999, 1777. [Neue Juristische Wochenschrift]
- Nugter, A.C.M. (1990). *Transborder flow of personal data within the EC*. Deventer and Boston: Kluwer Law & Taxation Publishers.
- Office of the Privacy Commissioner (OPC, Australia) (1997). *Information privacy in Australia: A national scheme for fair information practices in the private sector* (Consultation Paper). Sydney: OPC.
- OPC (2004). *Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004*. Sydney: OPC.
- OPC (2005). *Summary of state privacy laws*. Available online at: [http://www.privacy.gov.au/privacy\\_rights/laws/index\\_print.html](http://www.privacy.gov.au/privacy_rights/laws/index_print.html)
- OPC (2005a). *Getting in on the act: The review of the private sector provisions of the Privacy Act 1988*. Sydney: OPC.
- Office of Technology Assessment (OTA) (1986). *Federal government information technology: electronic record systems and individual privacy* (OTA-CIT-296). Washington, DC: Government Printing Office.
- Organization for Economic Cooperation and Development (OECD) (1980). *OECD guidelines on the protection of privacy and transborder flows of personal data*. Available online at: [http://www.oecd.org/document/20/0,3343,en\\_2649\\_201185\\_15589524\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/20/0,3343,en_2649_201185_15589524_1_1_1_1,00.html)
- Osswald, A. (1970). 'Datenschutz – ein hessisches Modell.' In *IBM-Nachrichten*, pp. 379–382.
- Packard, V. (1964). *The naked society*. New York: D. McKay.
- Park, W. (2006a, May). 'South Korea fights spam with new laws.' *Privacy Laws & Business International Newsletter*, 8.
- Park, W. (2006b, December). 'Legal regulation of on-line identification in Korea.' *Privacy Laws & Business International Newsletter*, 85.
- Paul v Davis*, 424 US 693 (1976).
- Pedersen, A. (2003, May/June). 'India plans EU-style data law.' *Privacy Laws & Business*, (68), pp. 1, 3.
- PIDMC (2006). *Korean personal information dispute mediation committee yearbook 2005*.
- Personal Data (Privacy) Ordinance, Hong Kong Ordinances (1995). Available online at: <http://www.hklii.org/hk/legis/en/ord/486/>
- Personal Information Dispute Mediation Committee (PIDMC) (2005). (Cases in WorldLII Database). Available online at: <http://www.worldlii.org/kr/cases/KRPIDMC>.
- Phillips, D. & D. Bilefsky (2006, September). 'EU and U.S. shape a deal on passenger data.' *International Herald Tribune*, p. 3.
- Piatti, M.C. (2001). *Les libertés individuelles à l'épreuve des NTIC*. Lyon, France: Presses Universitaires de Lyon.

- Pike, G.H. (2002, December). 'History repeated with the USA PATRIOT Act: several areas of this legislation have raised important concerns.' *Information Today* 19(11), pp. 19–21.
- Pinegar, K.R. (1984). 'Privacy protection acts: Privacy protectionism or economic protectionism?' *International Business Lawyer*, 12, pp. 183–188.
- Platten, N. (1996). 'Background to and history of the directive.' In D. Bainbridge (ed.), *EC Data Protection Directive* (chap. 2). London: Butterworths.
- Podlech, A. (1984). 'Die Begrenzung staatlicher Informationsverarbeitung durch die Verfassung angesichts der Möglichkeit unbegrenzter Informationsverarbeitung mittels der Technik.' *Leviathan*, 1, pp. 85–98.
- Podlech, A. & M. Pfeifer (1998). *Recht der Datenverarbeitung*, 139(153).
- Pollio, M.C. (2004). 'Note: The inadequacy of HIPPA's privacy rule: The plain language notice of privacy practices and patient understanding.' *New York University Annual Survey of American Law*, 60, pp. 579–620.
- Privacy International. (2004, September 8). *PI's country and organizational database*. Available online at: [www.privacyinternational.org/Countries](http://www.privacyinternational.org/Countries)
- Privacy Law Library (2002–). 'Privacy Law Library' on the World Legal Information (World LII) at <http://www.worldlii.org/int/special/privacy/>
- Privacy Laws & Business (2007). 'Google's Global Privacy Counsel and Chief Executive want global privacy rules', *Privacy Laws & Business*, 89, 12–13.
- Protocol No. 37, Deutscher Bundestag, 7th period, 724-2450, Public Hearing on May 6, 1974. [German parliamentary materials]
- Prosser, W.L. (1960, August). 'Privacy.' *California Law Review* 48(3), pp. 383–423.
- 'La protection de la vie privée.' (1995). *Après-demain*, pp. 376–377.
- Regan, P.M. (1993). 'The globalization of privacy: Implications of recent changes in Europe.' *The American Journal of Economics and Sociology*, 52(3), pp. 257–274.
- Regan, P.M. (1999). 'American business and the European Data Protection Directive: Lobbying strategies and tactics.' In C.J. Bennett & R. Grant (eds), *Visions of privacy: Policy choices for the digital age* (pp. 199–216). Toronto: University of Toronto Press.
- Regan, P.M. (2004). 'Old issues, new context: Privacy, information collection, and homeland security.' *Government Information Quarterly*, 21, pp. 481–497.
- Regan, P.M. (1995), *Legislating privacy: Technology, social values, and public policy*, Chapel Hill/London: University of North Carolina Press.
- Reidenberg, J.R. (1999). 'The globalization of privacy solutions: The movement towards obligatory standards for fair information practices.' In C.J. Bennett & R. Grant (eds), *Visions of privacy: Policy choices for the digital age* (pp. 217–228). Toronto: University of Toronto Press.

- Reidenberg, J.R. (2000). 'Resolving conflicting international data privacy rules in cyberspace.' *Stanford Law Review*, 52, pp. 1315–1371.
- Reidenberg, J.R. (2001). 'E-commerce and trans-Atlantic privacy.' *Houston Law Review*, 38, pp. 717–749.
- Reno v Condon*, 120 S.Ct 666 (2000).
- Roe v Wade*, 410 US 113 (1973).
- Rosenberg, J. (1969). *The death of privacy*. New York: Random House.
- Roßnagel, A., K. Pfitzmann & H. Garstka (2001). *Modernisierung des Datenschutzrechts*. Berlin: Bundesministerium des Innern. Available online at: <http://www.computerundrecht.de/media/gutachten.pdf>
- Rothfeder, J. (1989, September 4). 'Is nothing private?' *Business Week*, pp. 74–82.
- Morgan Roy Research (2001). *Privacy and business*. Paper prepared for the Office of the Federal Privacy Commissioner, Sydney, Australia. Available online at: <http://www.privacy.gov.au/publications/rbusiness.pdf>
- Roy Morgan Research (2001a). *Privacy and government*. Paper prepared for the Office of the Federal Privacy Commissioner, Sydney, Australia. Available online at: <http://www.privacy.gov.au/publications/rgovernment.pdf>
- Rule, J.B. (1973). *Private lives and public surveillance: Social control in the computer age*. London: Allen Lane.
- Rule, J.B. (1974). *Private lives and public surveillance: Social control in the computer age*. New York: Schocken Books.
- Sandoval, G. (2000, June 29). 'Failed dot-coms may be selling your private information.' *CNET News.com*. Available online at: <http://news.cnet.com/news/0-1007-200-2176430.html>
- Scheja, G. (2006). *Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank*. Baden-Baden: Nomos.
- SCHUFA (2005). *Annual report*. Available online at: [www.schufa.de](http://www.schufa.de)
- Schwartz, P.M. (1995). 'European data protection law and restrictions on international data flows.' *Iowa Law Review*, 80, pp. 471–496.
- Schwartz, P.M. & J.R. Reidenberg (1996). *Data privacy law: A study of United States data protection*. Charlottesville, NC: Michie Law Publishers.
- Seip, H. (1995). 'Data protection, privacy and national borders.' In J. Bing & O. Torvund (eds), *25 years anniversary anthology in computers and law* (pp. 67–82). Oslo, Norway: Tano.
- Shaffer, G. (2000). 'Globalization and social protection: The impact of E.U. and international rules in ratcheting up of U.S. privacy standards.' *Yale Journal of International Law*, 25, pp. 1–88.
- Shattuck, J. (1984a, June). 'Computer matching is a serious threat to individual rights.' *Communication of the ACM*, 27(36), pp. 538–541.
- Simitis, S. (1990). 'Datenschutz und Europäischer Gemeinschaft.' *Recht der Datenverarbeitung*, 6, pp. 3–23.

- Simitis, S. (1995). 'From the market to the polis: The EU directive on the protection of personal data.' *Iowa Law Review*, 80, pp. 445–469.
- Simitis, S. (2006). 'Übermittlung der Daten von Flugpassagieren in die USA: Dispens vom Datenschutz?' *Neue Juristische Wochenschrift*, 59(28), pp. 2011–2014.
- South African Law Commission (2005). *Privacy and Data Protection* (Discussion Paper 109). Available online at: <http://www.doj.gov.za/salrc/dpapers.htm>
- South China Morning Post* (SCMP). (2005, August 13). [quoting Hong Kong SAR Secretary of Security].
- Starke, J.G. (1987). 'Current topics.' *Australian Law Journal*, 62, p. 6.
- Steinmüller, W., B. Lutterbeck & C. Mallmann (1972, June 6). 'Grundfragen des Datenschutzes'. *Bundestags-Drucks VI/3826*.
- Stender-Vorwachs, S. (2004, November). 'The decision of the Bundesverfassungsgericht of March 3, 2004 concerning acoustic surveillance of housing space.' *German Law Journal*, 5(11) pp. 1337–1348. Available online at: [http://www.germanlawjournal.com/pdf/Vol05No11/PDF\\_Vol\\_05\\_No\\_11\\_1337-1348\\_Public\\_Vorwachs.pdf](http://www.germanlawjournal.com/pdf/Vol05No11/PDF_Vol_05_No_11_1337-1348_Public_Vorwachs.pdf)
- Suen, M.M.Y. (Secretary for Home Affairs, Hong Kong). (1995, April 19). Speech moving the second reading of the Personal Data (Privacy) Bill at the Hong Kong Legislative Council.
- Sung, S. (2003). *CyberLaw*. Seoul: Gilbert.
- Sweezy v New Hampshire*, 354 US 234 (1957).
- Swire, P.P. (2002). 'The surprising virtues of the new financial privacy law.' *Minnesota Law Review* 86, p. 1263.
- Swire, P.P. & R.E. Litan (1998). *None of your business: World data flows, electronic commerce, and the European Privacy Directive*. Washington, DC: Brookings Institution Press.
- Szabó, M.D. & I. Székely (2005). 'Privacy and data protection at the workplace in Hungary.' In S. Nouwt & B.R. de Vries (eds), *Reasonable expectations of privacy? Eleven country reports on camera surveillance and workplace privacy* (IT & Law Series, pp. 249–284). The Hague: T. M. C. Asser Press.
- Székely, I. (ed.). (1991). *Information privacy in Hungary. Survey report and analysis*. Budapest: Hungarian Institute for Public Opinion Research.
- Szladits, K. (ed.). (1941). *A magyar magánjog* [Hungarian Civil Law]. Budapest: Grill K.
- Tabatoni, P. (ed.) (2000). *La protection de la vie privée dans la société de l'information* (Tome 1). Paris: PUF.
- Talley v California*, 362 US 60 (1960).
- Tang, R. (2003, September). *Personal data privacy: The Asian agenda*. Speech given at 25th International Conference of Data Protection and

- Privacy Commissioners, Sydney, Australia. PowerPoint presentation available online at: <http://www.privacyconference2003.org/program.asp#psa>
- Tenants' Union of Queensland Inc [and other parties] v TICA Default Tenancy Control Pty Ltd* [2004] PrivCmrACD 1, [2004] PrivCmrACD 2, [2004] PrivCmrACD 3, and [2004] PrivCmrACD 4. Available online at: <http://www.worldlii.org>
- Terminal* (2002) 'Fichiers et libertés: le cybercontrôle vingt cinq ans après.' (2002). *Terminal* 88. Paris: L'Harmattan.
- Toonen v Australia* [1994] UNHRC 9. Available online at: <http://www.worldlii.org>
- United States Department of Homeland Security (USDHS). (2003, December 18). *US-VISIT program, increment 1: Privacy impact assessment, executive summary*. Available online at: [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_usvisit\\_inc1.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_inc1.pdf)
- USDHS, Transportation Security Administration (2003, July 22). *Notice of status of system of records; interim final notice; request for further comments* (Docket No. DHS/TSA-2003-1). Available online at: <http://www.cdt.org/security/usapatriot/030731cappsii.pdf>
- USDHS, Privacy Office. (2004, February 20). *Report to the public on events surrounding jetBlue data transfer*. Available online at: [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_rpt\\_jetblue.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_jetblue.pdf)
- US House Committee (1966). *The Computer and Invasion of Privacy: Hearings before the Special Subcommittee on Invasion of Privacy, U.S. House Committee on Government Operations, 89th Cong., 2<sup>d</sup> Ses.* (July 26–28).
- US Senate (1966). *Invasions of Privacy (Government Agencies): Hearings before the Subcommittee on Administrative Practice and Procedure, U.S. Senate Committee on the Judiciary, 89th Cong., 2d Sess.,* (June 7–9, 14, 16).
- US Senate (1971). *Federal Data Banks, Computers and the Bill of Rights: Hearings before the Subcommittee on Constitutional Rights, U.S. Senate Committee on the Judiciary, 92d Cong., 1st Sess.,* (February 23–25, March 2–4, 9–11, 15, 17).
- US Senate and House Committees (1974). *Legislative history of the Privacy Act of 1974*. Washington, DC: Government Printing Office.
- Vadrot, C. & L. Gouverne (1994). *Tous fichés*. Paris: Editions First.
- Velasco, V. (1999). *Les libertés individuelles face aux nouveaux moyens de surveillance* (Thèse de droit public). Paris: Université Paris X.
- Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192. [Australian Legal Decision] Available online at: <http://www.austlii.edu.au/>
- Victoria Park Racing and Recreation Ground v Taylor* (1937) 58 CLR 479. Available online at: <http://www.austlii.edu.au/>

- Vitalis, A. (1980). 'Le détonateur SAFARI.' *Terminal*, (2/3). Paris: L'Harmattan.
- Vitalis, A. (1988). *Informatique, pouvoir et libertés*. Paris: Economica, 2nd edn.
- Vitalis, A. (1993). 'L'apport à la démocratie des autorités de régulation indépendantes.' *Revue Européenne des Sciences Sociales*, 97.
- Vitalis, A. (2000). *Vidéosurveillance, sécurité et libertés* (Conférence introductive à la 22ème conférence internationale des commissaires à la protection des données, Venise), available online at <http://www.terminal.sgdg.org/articles/84/vitalis.html>
- Vitalis, A, F. Paoletti & H. Delahaie (1988). *Dix ans d'informatique et libertés* (CNIL). Paris: Economica.
- Wacks, R. (1980). *The protection of privacy*. London: Sweet & Maxwell.
- Wacks, R. (1989). *Personal information: Privacy and the law*. Oxford, UK: Clarendon Press.
- Wacks, R. (2000). *Law, morality and the private domain*. Hong Kong: Hong Kong University Press.
- Wainwright v Home Office* [2003] 3 WLR 1137. [Australian legal materials] Available online at: <http://www.worldlii.org>
- Warren, S. & L. Brandeis (1890, December). 'The right to privacy.' *Harvard Law Review*, 4, p. 195.
- Waters, N. & G. Greenleaf (2004). 'IPPs examined: The security principle.' *Privacy Law & Policy Reporter*, 11, p. 67.
- Waters, N. & G. Greenleaf (2005). 'IPPs examined: The correction principle.' *Privacy Law & Policy Reporter*, 11, p. 137.
- Waters, N. and A. Paramaguru (2007). 'Enforcement of privacy laws – issues arising from Australian experience', *Interpreting Privacy Principles Project*, University of New South Wales, available online at <http://www.cyberlawcentre.org/ipp/publications.html>
- Waymann, J.L. (1997, December). *Biometric identification standards research (Final report vol I)*. San Jose State University, College of Engineering. Available online at: [http://www.engr.sjsu.edu/biometrics/publications\\_fhwa.html](http://www.engr.sjsu.edu/biometrics/publications_fhwa.html)
- Weichart, T. (2000). 'Datenschutz und Payback', *Datenschutznachrichten*, 4, p. 5.
- Weichert, T. (2003). 'Kundenbindungssysteme – Verbraucherschutz oder der gläserne Konsument?' In *Datensicherheit und Datenschutz*, p. 161.
- Weiss, L.B. (1983, February 26). 'Government steps up use of computer matching to find fraud in programs.' *Congressional Quarterly Weekly Report*, p. 432.
- Westin, A.F. (1967). *Privacy and freedom*. New York: Atheneum.
- Westin, A.F & M.A. Baker (1972). 'Databanks in a free society: Computers, record-keeping, and privacy.' In: *Report of the Project on Computer*

- Databanks of the Computer Science and Engineering Board, National Academy of Sciences*. New York: Quadrangle/New York Times Book Company.
- Whalen v Roe*, 429 US 589 (1977).
- Whitman, J.Q. (2004, April). 'The two western cultures of privacy: Dignity versus liberty.' *The Yale Law Journal*, 113, pp. 1151–1221.
- World Legal Information Institute (WorldLII). (2003). *Privacy Law Project* (commenced 2003 and ongoing). [includes Office of the Privacy Commissioner for Personal Data Hong Kong *Case Notes* and Office of the Privacy Commissioner for Personal Data, Hong Kong *Administrative Appeal Board Case Notes*] Available online at: <http://www.worldlii.org/int/special/privacy/>
- Yeh, B.T. & C. Doyle (2006). *USA PATRIOT Improvement and Reauthorization Act of 2005: A legal analysis* (Congressional Research Service Report).
- Yi, C.B. & K.J. Ok (2003) 'Korea's personal information protection laws.' *Privacy Law & Policy Reporter*, 9(9), 172.



# Index

---

- 1984 (book) 57, 76, 88  
III/III Division (Hungary) 174, 180  
63<sup>rd</sup> Royal Air Force Squadron *see*  
    Royal Air Force, 63<sup>rd</sup> Squadron  
A29 Working Party (2001) 154  
AAMVA *see* American Association of  
    Motor Vehicle Administrators  
Abacus database 74  
Academy of liberties (France) 125  
Access Card (Australia) 142, 171–72  
access principle 112, 117, 132  
ACCI (Melbourne employer group) 165  
ACLU *see* American Civil Liberties  
    Union  
ACS *see* Australian Computer Society  
Act no. 78–17 on Data Processing, Data  
    Files and Individual Liberties  
    (France) 35  
ACT *see* Australian Capital Territory  
Axiom 147  
Administration Ministry (Republic of  
    Korea) 211, 227, 270  
Administrative Appeals Board (Hong  
    Kong) 245  
Administrative Decisions Tribunal  
    (Australia) 159  
Advisory Committee on Automated  
    Personal Data Systems (USA) 55  
Aetna Life Insurance Company 58  
African Charter on Human and People's  
    Rights (OAU Doc. CAB/LEG/67/3  
    rev. 5) 45  
Agreement between the European  
    Community and the United States  
    of America on the processing and  
    transfer of PNR data by Air  
    Carriers to the United States  
    Department of Homeland Security,  
    Bureau of Customs and Border  
    Protection (2004) 40  
Agreement Establishing the World Trade  
    Organization (1994) 40  
Aid to Families with Dependent  
    Children 60  
ALA *see* American Library Association  
Albrecht, Hans-Jörg 100  
Alpert, S.A. 65  
ALRC *see* Australian Law Reform  
    Commission  
*Amann v Switzerland* (2000) 46  
American Association of Motor Vehicle  
    Administrators (AAMVA) 51, 78  
American Bar Association 61  
American Civil Liberties Union (ACLU)  
    70, 270  
American Lawyer, The 79  
American Library Association (ALA) 69  
Andrews, E. L. 15  
ANIS (*Approche nouvelle de*  
    *l'information sociale*) software 120  
anonymity principle 153, 161  
Anti-Money-laundering and Counter-  
    Terrorism Financing Act (2006)  
    (Australia) 171  
Anti-Discrimination Act (Hungary) 183  
anti-terrorism 88, 98–9, 129, 138, 145,  
    170–71, 272–3  
Anti-Terrorism Act (No. 2) 2005  
    (Australia) 170  
APC *see* Privacy Charter (APC) (1992)  
    (Australia)  
APEC *see* Asia-Pacific Economic  
    Cooperation  
APF *see* Australian Privacy Foundation  
APPA *see* Asia-Pacific Privacy  
    Authorities  
archiving of data 3–4, 96, 230, 275  
Argentina 4, 39, 47, 94  
Armatte, E. 121  
Article 29 Committee (EU) 167  
Asia-Pacific Economic Cooperation  
    (APEC) 18, 43, 47–8, 145  
    Privacy Framework 28, 43–5, 49,  
    167–8, 252, 255

- Asia-Pacific Privacy Authorities (APPA) 18
- Aspects of Privacy and Informational Autonomy in the Press (MKI Report, Hungary) 193
- Association for the Improvement of the E-Mail Environment (Republic of Korea) 218
- associational privacy 53
- Attorney-General Discussion paper 1996 (Australia) 161
- AUSTRAC system (Australia) 145, 171
- Australia Card 141, 152, 166, 168, 257–8
- Australian Capital Territory (ACT) 147
- Australian Computer Society (ACS) 165
- Australian Law Reform Commission (ALRC) 151, 173
- Australian Privacy Charter Council 6
- Australian Privacy Foundation (APF) 142, 144, 155, 164–65, 172
- Australian, The* (newspaper) 141
- Automatic Teller Machines 172
- automobile registration 115
- Baker, A. 51, 55, 57
- Bali, Indonesia terrorist attacks 170
- Baltic countries 183
- Banking Act (Hungary) 176
- banking industry 59, 65, 68, 82, 90–93, 114, 176, 186, 189, 198, 216
- Banque de France 114
- Barrier, G. 135
- Barton, Joseph 73
- Basic Law (Hong Kong) 233–36
- Baudry, P. 140
- Baycorp Advantage 144, 146
- ‘Because of the Privacy Act’ (BOPTA) (Australia) 153
- Bellagio conference center 13–14
- Belloeil, A. 135
- Bennett, C.J. 17, 57–8, 75
- Berlau, J. 71
- Berthold, M. 251
- Besser, L. 145
- BGH NJW 1978, 2151 (Germany) 91
- BGH RDV 2005, 62 (Germany) 98
- BGHZ 143, 214 (*Marlene Dietrich*) (Germany) 81, 105
- BGHZ 143,214 (*Caroline v Monaco II*) (Germany) 81
- BGHZ 162, 1 (Germany) 100
- BGHZ 30, 7 (*Caterina Valente*) (Germany) 81
- BGHZ 50, 133 (*Mephisto*) (Germany) 81
- Big Brother* (television series) 97
- Big Brother awards
- Australia 165
- Germany 95
- Hungary 196
- ‘Big Brother’ 57, 76, 101, 107, 122, 189, 207, 220
- Bilefsky, D. 40
- Bill of Rights Ordinance (BORO) (1991) (Hong Kong) 234, 239, 252
- biometrics 37, 68, 140, 170, 220
- Birkelbach, W. 83
- ‘Bonus Card System’ (Germany) 91–92, 267
- BOPTA *see* ‘Because of the Privacy Act’
- Bork, Robert 73
- BORO *see* Bill of Rights Ordinance
- Boxer, Barbara 50
- Braibant, G. 113
- Brandeis, Louis 52
- Brenton, Myron 73
- Brill, Steve 79
- Broadcasting and Communications Commission (Republic of Korea) 228
- Bromberg, T. 145
- Brühann, Ulf 18
- Buchanan, Allen E. 106
- Bull, H.P. 86
- Bundestags-Drucksache VI/2885 (Germany) 83
- Bundestags-Drucksache VII/1027 (Germany) 83
- Bureau of Customs and Border Protection (USA) 39, 102
- Burnham, D. 51, 75
- Bush, George W. 69, 262, 270, 273
- Bushkin, J. 74
- Business Week* 64, 73
- BVerfG 4 (Germany) 89
- BVerfG 4.4.2006 1BvR 518/02 (Germany) 98
- BVerfG NJW 1999, 55 (Germany) 99

- BVerfG NJW 2000, 55 = BVerfGE 109, 279 (Germany) 99
- BVerfG NJW 2004, 2213 = BverfGE 110, 33 (Germany) 99
- BVerfG NJW 2004, 999 (Germany) 99
- BVerfG NJW 2005, 1338 = BVerfGE 112, 304 (Germany) 99
- BVerfG NJW 2005, 1917 =BVerfGE 113, 29 (Germany) 99
- BverfG NJW 2006, 1939 (Germany) 99
- BVerfG Urt. v 27.7.2005 1 BvR 668/04 (Germany) 99
- BVerfGE 112, 304 (*GPS-Observation*) (Germany) 99
- BVerfGE 113, 348 (Germany) 100
- BverwG 22.10.2003 (Germany) 98
- BVerwG NJW 2004, 1191 (Germany) 100
- BverwG NJW 2006, 1116 (Germany) 98
- Bygrave, Lee 7, 11, 14, 30, 34, 35, 46
- Cable Communications Policy Act of 1984* (USA) 59, 60, 68
- Cadoux, L. 115
- California Department of Motor Vehicles 50
- California Law Review* 52
- Campbell Case* (2004) (UK) 236
- Campbell, D. 138
- CAN *see* Citizens' Action Network
- Canada 28, 39, 247, 260, 266
- Canadian Standards Association (CSA) (1996) 6
- Canal+ database 131
- Cantril A.H. 71
- Cantril S.D. 71
- CAPPS II *see* Computer-Assisted Passenger Prescreening System
- Carse, D. 248
- CATO Institute 79
- caution principle 85–6
- CBNV *see* Citibank N.A. Nevada
- CBSD *see* Citibank N.A. South Dakota
- CCTV *see* closed-circuit televisions
- Census Act of 1983 (Germany) 80
- 'Census case' (1983) (BverfGE 65,1) (Germany) 80–81, 85, 88–89, 258, 273
- Center for Advanced Study in the Behavioral Sciences 14
- Center for Democracy and Technology 7, 74
- Central People's Government (Hong Kong) 233
- Central Statistical Office (Hungary) (KSH Group) 175, 178–180
- Centre de coordination pour la recherche et l'enseignement en informatique et société (CREIS) 115, 121
- Chadwick, Paul 159
- Charlesworth, A. 17, 34, 35
- Charter of Fundamental Human Rights of the European Union (2007) 32, 33
- Chief Executive (Hong Kong) 233–5
- Children's Online Privacy Protection Act of 1998 (COPPA) (USA) 60, 67, 77
- China, Peoples Republic of 232–3, 241–2, 253, 255–56
- ChoicePoint 79
- Chosun-Ilbo, The* (newspaper) 227
- Chulov, M. 145
- Chun, Doo-Hwan 208, 216
- Chung Yan-tung, Gillian 236
- Chung, Y.S. 215
- CIP *see* Citibank Privatkunden AG Düsseldorf
- CIS (Hong Kong credit reporting bureau) 248
- Citibank 92–93, 95
- Citibank N.A. Nevada (CBNV) 93
- Citibank N.A. South Dakota (CBSD) 93
- Citibank Privatkunden AG Düsseldorf (CIP) 93
- Citicorp Kartenservice Frankfurt/Main (CKS) 93
- Citivas Group 79
- Citizens' Action Network (CAN) (Republic of Korea) 7, 219
- City Paper* (Washington DC) 64
- Citycorp Card Operations Nordhorn (CCO) 93
- Civil Code (Hungary) 178
- CJ Home Shopping Co. 226
- CKS *see* Citicorp Kartenservice Frankfurt/Main
- ClarityI Case* (2006) (Australia) 147
- Clarke, Roger 61, 142
- Clennell, A. 145

- Clinton, Bill 66, 78, 270
- closed-circuit televisions (CCTV) 120, 145, 166, 196, 219, 232, 249–50
- CNIL *see* Commission nationale de l'informatique et des libertés
- Code of Fair Information Practices (HEW) (USA) 55–8, 62–3
- Code of Practice on Consumer Credit Data (Hong Kong) 247–48
- Code of Practice on the ID number (1997) (Hong Kong) 236
- Codes of Practice (Australia) 161
- COINTELPRO 262
- Cold War 88
- comité d'entreprise (France) 136
- Commission nationale de l'informatique et des libertés (CNIL) (France) 109, 110–11, 112–20, 258, 272
- anti-spam campaign 135–36
- and banking industry 131–32
- challenges to regulatory power 127–28, 132
- criticism 124–26
- fiscal administration 131
- and police databases 129–30
- and telecommunications industry 134
- Commissioner for Personal Data (Hong Kong) 236–7, 242–7, 248–9, 253
- Commissioner on Interceptions of Communications and Surveillance (Hong Kong) 235
- Communication Ministry (Republic of Korea) 222, 225, 228
- Communication Secrets, Act on (1995) (Republic of Korea) 210
- Communication Secrets, Act on (Republic of Korea) 210
- Communications and Surveillance Ordinance (2006) (Hong Kong) 235
- Computer 'informants' 61
- Computer Matching and Privacy Protection Act of 1988 (USA) 60, 61
- Computer-Assisted Passenger Prescreening System (CAPPS II) 70
- 'Computerized Man, The' 55
- Confucius 253
- Conseil constitutionnel (France) 113
- Conseil d'Etat (France) 108, 110–11, 114, 127, 132
- consensus principle 263–67
- consent principle 9, 266–67
- Constitution (Australia) 149–50
- Constitution (EU) 33
- Constitution (Germany) 80, 84, 98
- Constitution (Hungary) 176, 180–81
- Constitution (Republic of Korea) 212
- Constitution (USA) 52–3, 55
- Constitutional Court (Germany) 81
- Constitutional Court (Hungary) 181–2, 203, 259
- Constitutional Court (Republic of Korea) 211–13
- Consultative Committee (component of Convention for the Protection of Individuals (CoE)) 24
- consumer data 91–2, 122, 135, 147, 194, 226, 269
- control of success principle 100
- control principle 85–7
- Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (1997) (EU) 25
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) (CoE) 6, 19
- Additional Protocol 23–4
- Explanatory Report 24, 25
- implementation 24, 25
- principles 22–3
- ratification 20
- Convention of the Rights of the Child (UN) 98
- Convention on Cybercrime (2001) (Hungary) 190
- COPPA *see* Children's Online Privacy Protection Act of 1998
- Couch v US* (1973) 53
- Council Decision 2002/187/JHA (EU) 26
- Council of Europe (CoE) 6, 18, 23–7, 83, 178, 189
- Committee of Ministers (CoE) 20
- Convention (1981) 6, 111, 189
- privacy protection initiatives 19–26

- Council of Europe Recommendations  
 No. R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (1995) 25  
 No. R(97) 5 on the protection of medical data (1997) 25  
 No. R(2002) 9 on the protection of personal data collected and processed for insurance purposes (2002) 25
- Court of Final Appeal (Hong Kong) 233, 235
- Court of Human Rights (EU) 46
- Court of Justice of the European Communities 139
- Court of the European Union 104
- Court TV 79
- Cowen, Zelman 150
- CRAA *see* Credit Reference Association of Australia
- Craig, P. 33
- Cranor, L.F. 73
- credit industry 92–3, 101, 113, 132, 143–4, 146, 151, 216, 247–8, 254, 266, 267
- Credit Information Act (1995) (Republic of Korea) 210, 220, 228
- Credit Reference Association of Australia (CRAA) 143
- Credit Reporting Summit (Australia) 144
- Cripps, A. 145
- CSA *see* Canadian Standards Association
- Csemegi Codex 178
- Csurka, István 197
- Cyber-Terror Response Center (Republic of Korea) 226
- Czech Republic 197–8
- Data Act (1973) (Sweden) 4
- Data Banks in a Free Society* (report, 1969) (USA) 55
- Data Integrity Boards (USA) 61
- data matching 60–61, 107, 108, 110, 127, 131, 134, 169, 231  
 ‘parallel data matching’ scheme 143–4
- Data Protection Act, first (Germany) 83, 87, 89–91
- Data Protection Act, second (Germany) 89
- Data Protection and Freedom of Information Act (DP&FOI Act) (Hungary) 179, 183–4  
 Commissioner 179, 181, 183–5, 187–8, 190, 193, 195–8, 200–201, 204, 206
- Data Protection Principles (Hong Kong) 237, 240–41, 243, 246
- Data Protection Working Party 18
- Data-matching Program (Assistance and Tax) Act (1990) (Australia) 143
- Datenschutz in Verwaltungsinformationssystemen* (book) 85
- de Búrca, G. 33
- Declaration made at the 27th International Conference of Data Protection and Privacy Commissioners at Montreux (2005) 48
- Declaration on Human Rights in Islam (UN Doc. A/45/421/5/21797) 45
- Declaration on the Protection of Privacy on Global Networks (C(98) 177 Annex 1; issued 8–9 October 1998) (OECD) 28
- Democratic People’s Republic of Korea 208
- Dempsey, J.X. 71
- Deng Xiaoping 233
- Department of Commerce (USA) 39
- Department of Foreign Affairs and Trade (Australia) 170
- Department of Health and Human Services (USA) 64
- Department of Health Education and Welfare, Secretary’s Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (1973) 62
- Department of Health, Education and Welfare (HEW) (USA) 6, 55–7  
 Report (1973) 6
- Department of Homeland Security (USA) 40, 51, 70
- Department of Justice (France) 108
- Department of Transportation (USA) 69, 70

- Deutsche Bahn 93  
 Deutsche Forschungsgemeinschaft  
 (German Research Council) 83  
 Deutsche Rentenversicherung 82  
 Deutsche Telekom 96  
 Dhont, J. 41  
 direct marketing 42, 91, 95, 114,  
 135–36, 147, 165, 186, 201, 218,  
 243  
 Direct Marketing Act (Hungary) 176  
 Direction de la sécurité du territoire  
 (France) 129  
 Direction générale des  
 telecommunications (France) 134  
 Directive 95/46/EC on the Protection of  
 Individuals with Regard to the  
 Processing of Personal Data and on  
 the Free Movement of Such Data  
 ('EU Privacy Directive') (1995)  
 30–43  
 adoption process 4, 31–2  
 and air passenger name records 39–40  
 and Australian legislation 161, 167  
 'Binding Corporate Rules' (BCRs)  
 38–9  
 and Council of Europe Convention on  
 personal data 24  
 and EU dispute with USA 15  
 and European Court of Human Rights  
 32  
 and European Court of Justice 32  
 and European Parliament 31  
 and French privacy laws 112  
 and General Agreement on Trade in  
 Services (GATS) 40–41  
 and Gramm-Leach-Bliley Act (USA)  
 65  
 and monitoring regimes 36  
 and national security 36  
 'Safe Harbor' protocol 41, 139  
 'third countries' 37–8, 40, 47  
 transfer of personal data 37–41, 259  
 and Working Party on the Protection  
 of Individuals 37  
 Directive 97/66/EC (EU) 41  
 Directive 2002/58/EC Directive on  
 Privacy and Electronic  
 Communications (EU) 34, 41–2,  
 136  
 Directive 2006/24/EC (EU) 42
- Disclosure of Information by Public  
 Agencies, Act on (1995) (Republic  
 of Korea) 210–11  
 dispute resolution  
 Australia 156–57, 159  
 Hong Kong 244  
 Republic of Korea 217, 221–23  
 District Court (Australia) 149  
 Dix, A. 92  
 DMP (personal medical dossier system)  
 (France) 137–38  
 DNA screening 98  
 'Dog-Shit Girl' incident (Republic of  
 Korea) 223–24  
 Do-Not-Call list (Australia) 147  
 Dorsch, Claudia 100  
 DoubleClick 74  
 Doyle, C. 69  
 DP&FOI Act *see* Data Protection and  
 Freedom of Information Act  
 driver's licences 50–51, 60, 78  
 Driver's Privacy Protection Act of 1994  
 (USA) 50, 60  
 Dubai International Financial Centre  
 (DIFC) Law No. 1 of (2007) 47  
 Duetsche Telekom 96  
 'Duna-gate' scandal (Hungary) 174, 180,  
 197, 203, 259
- Eastweek Case* (2001) (Hong Kong) 239  
*Easy Finder* (Hong Kong magazine) 236  
 Eberle, E. 16  
 Echelon 119  
 ECHR *see* European Convention for the  
 Protection of Human Rights  
*E-Commerce and Privacy: What Net  
 Users Want* (book) 72  
 EFA *see* Electronic Frontiers Australia  
 Eger, J. M. 21  
*Egészséges erotica* (film) 199  
*Eisenstadt v Baird* (1972) 53  
 Election Procedure Act (Hungary) 186–7  
 Electronic Communications Privacy Act  
 of 1986 (USA) 53, 68, 76  
 Electronic Frontiers Australia (EFA) 164  
 Electronic Privacy Information Center  
 (EPIC) 7, 18, 74, 224, 234, 255  
 Electronic Signature Act (1995)  
 (Republic of Korea) 210  
 Electronic Commerce Act (Hungary) 183

- 'Elements of Effective Self Regulation for Protection of Privacy' (1998) 63
- Ellger, R. 21, 31, 39
- Ellison, Larry 78
- Elmajzoub, M. 130
- Emergency Presidential Decrees (Republic of Korea) 208
- Emergency Presidential Order on Real Name Financial Transactions and Protection of Confidentiality (1993) (South Korea) 215–16
- employee data 89–90, 133, 136, 199
- encroachment principle 85–6
- 'Entertainers X-File' incident (Republic of Korea) 223
- EPIC *see* Electronic Privacy Information Center
- Equifax 74
- Ervin, Sam 55, 57, 76
- Eshoo, Anna 73
- ethnic profiling 123
- ETS *see* European Treaty Series
- Etzioni, Amatai 105–6
- EU Privacy Directive *see* Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data
- EURODAC database 130, 205
- Eurojust 43, 26
- European Commission 31, 34, 47, 137, 139, 252
- European Commission Decisions (C(2003) 1731) 39  
2000/518/EC 39  
2000/520/EC 39, 41  
2001/497/EC (EU) 38  
2002/16/EC (EU) 38  
2002/2/EC 39  
2004/535/EC 39  
2004/915/EC (EU) 38
- European Convention for the Protection of Human Rights (1950) (ECHR) 19–21
- European Council Decisions  
1999/468/EC (1999) 39  
2002/187/JHA 26  
2006/729/CFSP/JHA 40  
2007/551/CFSP/JHA 40
- European Council of Ministers 31
- European Court of Human Rights 252
- European Court of Justice 32
- European Court of Justice Cases (C-138/01) 32  
C-101/01 *Bodil Lindqvist* ECR I-129711 (2003) 32, 34  
C-139/01 *Österreichischer Rundfunk and Others* ECR I-4989 (2003) 32  
C-301/06, *Ireland v Council and Parliament* (O.J. C 237) 42  
Joined Cases C-465/00, C-138/01, and C-139/01 *Österreichischer Rundfunk and Others* [2003] (ECR I-4989) 45
- European Court of Justice, Grand Chamber 103
- European Data Protection Supervisor 42
- European Direct Marketing Association 18
- European Economic Area, Agreement on the 31
- European Economic Community 30
- European Economic Treaty 94
- European Parliament (EP) 31, 39, 43, 139
- European Parliament Resolutions  
Resolution of 21 February 1975 on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing (O.J. C 60) (1975) 31  
Resolution of 8 May 1979 on the protection of the rights of the individual in the face of technical developments in data processing (O.J. C 140) (1979) 31  
Resolution of 9 March 1982 on the protection of the rights of the individual in the face of technical developments in data processing (O.J. C 87) (1982) 31
- European Parliament v Council of the European Union and Commission of the European Communities* (2006) (EU) 40
- European Treaty Series (ETS)  
No. 5 (1950) 19  
No. 108 (1981) 19  
No. 164 (1997) 25

- European Union 23–4, 190, 259
- Europol 130, 205
- excess principle 264
- Executive Council (Hong Kong) 233
- Executive Order (2005) (Hong Kong) 235
- Expansion of Computer Networks and the Promotion of Its Utilization, Act on the (1986) (Republic of Korea) 225
- fair and lawful processing principle 22
- Fair Credit Reporting Act of 1970 (USA) 59, 68, 73, 75
- Fair Information Practices, Composite Portrait of 6
- Families with Dependent Children 60
- Family Educational Rights and Privacy Act of 1970 (USA) 59, 68
- FBI *see* Federal Bureau of Investigation
- Federal Bureau of Investigation (FBI) (USA) 69, 262
- Federal Civil Court (Germany) 81, 98
- Federal Constitutional Court (Germany) 258
- Federal Court (Germany) 105
- Federal Data Center (USA) 55
- Federal Data Protection Commissioner (Germany) 83, 270
- Federal Minister of Interior (Germany) 88
- Federal Parliament (Germany) (*Deutscher Bundestag*) 83, 87–8
- Federal Privacy Board (USA) 56–7
- Federal Rules of Criminal Procedure (USA) 68
- Federal Supreme Constitutional Court (Germany) 80–81, 97, 99–100
- Federal Toll Collect Act (Mautgesetz) (Germany) 86
- Federal Trade Commission (USA) 41, 58, 63, 66, 67, 74–5
- fichiers de souveraineté 129
- Fichte, Johann Gottlieb 84
- Fifth Amendment (USA) 52–3
- financial data 65, 127, 130–2, 143–4, 146, 220, 231, 265–8
- Financial Modernization Act of 1999 (Gramm-Leach-Bliley) (USA) 60, 65, 68, 73, 77, 78
- Financial Supervisory Service (Republic of Korea) 220
- Financial Transactions Reports Act 1988 (Australia) 145, 170
- First Amendment (USA) 52–53, 57
- 'First World' concern 29
- FISA *see* Foreign Intelligence Surveillance Act
- Flaherty, D.H. 58, 75, 125
- FM v Macquarie Case* (2005) (Australia) 153
- Ford, Gerald 57, 78
- Ford, P. 167
- Foreign Intelligence Surveillance Act (FISA) (USA) 68
- Forum des droits sur l'internet (France) 116
- 'Four Corners' 155
- Fourteenth Amendment (USA) 52–3
- Fourth Amendment (USA) 52–3
- Framework Act on Electronic Commerce (1995) (Republic of Korea) 210
- Framework Decision (EU) 42–3
- France Télécom 134
- Frayssinet, J. 111
- Free Congress Foundation 76
- Freedom of Information Act (1982) (Australia) 151
- Freese, Jan 18
- Fried, C. 52
- Froomkin, A.M. 50
- FTRA (Australia) 171
- function creep 143, 171–72
- Fundamental Rights of the European Union 33
- Gallagher, Cornelius 55
- GAMIN system 114, 119, 121, 133
- Gandy, Oscar 61, 71
- GAO *see* General Accounting Office
- Garfinkel, S. 51
- Garstka, H. 104
- Gaskin v United Kingdom* (1989) 46
- Gassmann, Hans-Peter 18
- GATS *see* General Agreement on Trade in Services
- Geiger, H. 31
- Gellman, R. 57
- Gendarmerie brigades (France) 118

- General Accounting Office (GAO) (USA) 70
- General Agreement on Trade in Services (GATS) 40–1, 94
- General Comment 16 of 23 March 1988 (U.N. Doc. A/43/40) 46
- Georgetown Business School 66
- German Discounts Act (Rabattgesetz) 92
- German Football Association (Deutscher Fußball-Bund – DFB) 97
- German National Railway 92–93
- German Private International Law 94
- German Railcard Case 83
- German Research Council *see* Deutsche Forschungsgemeinschaft
- Gesetz- und Verordnungsblatt für das Land Hessen 83
- Gesetz zur Bekämpfung des internationalen Terrorismus vom 9.1.200 (Law on the fight against international terrorism) 99
- Ghai, Y. 233
- Ginsburg, T. 208
- ‘Girl from Dávod’ case (Hungary) 185–86
- Girot, J.L. 112
- GSM-SIM card 86
- Google 48, 230–31
- Gore, Al 66
- Grace, John 13
- Gramm-Leach-Bliley Act *see* Financial Modernization Act of 1999
- Greenleaf, Graham 10–12, 39, 41, 43, 44, 45, 48, 142–4, 153, 155, 157–9, 161, 167–8, 171–3, 238, 252, 257, 259, 262, 265–6, 268–9, 271–2
- GRID 122
- Griswold v Connecticut* (1965) 53
- Grosso v US* (1968) 53
- Guernsey 94
- Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72, 20 February 1990) (UN) 29
- Guidelines for Consumer Protection in the Context of Electronic Commerce (1999) (OECD) 28
- Guidelines for Cryptography Policy (OECD) 28
- Guidelines for Librarians on the USA PATRIOT Act 69
- Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002) (OECD) 28
- Guidelines for the Security of Information Systems C(92)188/FINAL (1992) (OECD) 28
- Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980) (OECD) 6, 19, 26, 27, 28, 29
- Guidelines on privacy and data protection (UN resolution 45/95) (December 1990) 29–30
- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) (OECD) 6, 151–2, 167, 189, 210, 252
- Gurak, L.J. 74
- Haelan Laboratories, Inc. v Topps Chewing Gum, Inc.* 105
- Hálapénz.hu* case (Hungary) 187–88
- Half Price Plaza 218
- Hammit, H. 50
- Harlan, Justice John Marshall 53
- harmonization of privacy regimes 21, 33, 48, 106, 111–12, 139, 190
- Harris, Louis and Associate, Inc. 72
- Harvard Law Review* 52
- Hauser, D. 88
- Hawke/Keating Labor government (Australia) 152
- Hayden, T. 58
- Health and Welfare Access Card (Australia) 142, 171
- Health Insurance Commission (HIC) (Australia) 142
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) (USA) 60, 64, 65, 78
- Heimann, E. 128
- Heisenberg, D. 15, 17, 41
- Herold, Horst 88
- HEW *see* Department of Health, Education and Welfare
- HIC *see* Health Insurance Commission
- High Court (Australia) 149

- High Court (Hong Kong) 235  
 Higher Education Act (Hungary) 183  
 Hijmans, H. 42  
 HIPAA *see* Health Insurance Portability and Accountability Act of 1996  
 HKLRC *see* Hong Kong Law Reform Commission  
 HKMA *see* Hong Kong Monetary Authority  
 Hodge, A. 145  
 Hoffsaes, C. 123  
 Holocaust Center, Jerusalem 200  
 Holocaust Center, New York 200  
 Holocaust documents 200, 202  
 Hondius, F. W. 20, 27, 262  
 Hong Kong Law Reform Commission (HKLRC) 234–6, 238–40, 251, 253, 255  
 Hong Kong Monetary Authority (HKMA) 248  
 Hong Kong Post 245  
 Horne, D. 166  
 House Bill (HR 16373) (USA) 56  
 House of Representatives, United States 50, 55–7, 59, 68  
 House Special Subcommittee on Invasion of Privacy (USA) 55  
 Howard Liberal Party (Australia) 170  
 Howard, John 160–61, 170–72  
 Human Rights Committee of the United Nations 149  
 Human Rights Convention 98  
 Human Rights League 121  
 Hungarian Academy of Science 205  
 Hungarian Civil Liberties Union 196  
 Hungarian Institute of Public Opinion Research (MKI) 191, 193  
 Hungarian Justice and Life Party 197  
 Hustinx, Peter 13  
 IBM *see* International Business Machines Corporation 95  
 ICAC *see* Independent Commission Against Corruption  
 ICCPR *see* International Covenant on Civil and Political Rights  
 ID Card (Hong Kong) 230–31, 236–8, 250  
 identification numbers 74, 123–4, 127, 236–7, 259  
 Identification Numbers Act (1996) (Hungary) 183  
 identity cards 78–9, 118, 141–2, 171–2, 207, 230–31, 236–8, 250  
 identity fraud 215–16  
   by South Korean Presidents 216  
 identity theft 73  
*IDs-Not That Easy* (report) 79  
 ILO *see* International Labour Organization  
 Imaginons un réseau internet solidaire (IRIS) 120–21  
 Independent Commission Against Corruption (ICAC) (Hong Kong) 235  
 Independent Police Complaints Council (IPCC) (Hong Kong) 230, 235, 246  
 India 4  
 InfoBase 147  
 InfoFilia (the Hungarian Data Protection and Freedom of Information Foundation) 179  
 Information Infrastructure Task Force (USA) 66  
 Information Policy Committee 63  
 Information Policy Committee of the White House's Information Infrastructure Task Force 63  
 Information Privacy Principles (IPP) (Australia) 152, 156  
 information quality principle 22  
 'information society' 101, 122, 138, 226  
 information technologies innovation 2–3, 29, 96, 107–108, 115, 119, 121–2, 203, 212, 224, 227, 274  
 information technology professionals 194–95, 199  
 informational self-determinism principle 81, 97–99  
 Informatique et libertés legislation (1978) (France) 111–12, 121, 133, 136, 138  
 Informatique fichier and citoyenneté (France) 121  
 ING Life (insurance company) 231  
 Institut national de la statistique (INS) (France) 107, 108, 127  
 Insurance Act (Hungary) 176  
 insurance industry 88, 113–14, 198, 217, 231

- Intel Corporation 74, 95  
 International Business Machines Corporation (IBM) 95  
 International Chamber of Commerce 18  
 International Conference of Data Protection and Privacy Commissioners 225  
 International Covenant on Civil and Political Rights (ICCPR) 19, 45, 149, 234, 252  
 International Data Protection Contract, German Train (DB) 93  
*International Herald Tribune* 216  
 International Labour Organization (ILO) 18  
 International Working Group on Data Protection and Telecommunications 18  
 Internet 115–16, 65–7, 72, 93, 135, 201, 205, 209, 218  
   cookies 66, 93  
   fraud 226  
   Internet protocol (IP) numbers 96  
   monitoring 99, 137  
   pornography 223  
 Internet Crime Investigation Center (Republic of Korea) 226  
 Interpol 130  
 IPCC *see* Independent Police Complaints Council  
 IPP *see* Information Privacy Principles  
 IRIS *see* Imaginons un réseau internet solidaire  
 Isle of Man 94  
 ITBB 238  
 Ivan Szekely 11  
 Jackson, M. 150  
*Jane Doe v ABC case* (2007) (Australia) 149  
 Japan 208, 259  
 Jeong, J.H. 227  
 Jewish Holocaust 200  
 John von Neumann Society of Computer Science 178  
 Joint cases 2004/496/EC OJ 2004 L 183, p. 83; OJ 2005 L 255 (2006) (EU) 103  
*JoongAng Daily* (newspaper) 209, 211  
 June Struggle (Republic of Korea) 208  
 Junkbusters 74  
 Justice Department (USA) 68  
 Kádár, János 178  
 KAIT *see* Korea Association of Information and Telecommunication  
 Kalven, H. 52  
 Kant, Immanuel 84  
 Karanja, S.K. 43  
*Katz v United States* (1967) 53  
 Katz, J.E. 71  
 KGB (Soviet Union) 180  
 Kilian, Wolfgang 11, 89, 258, 262, 265–7, 270, 272  
 Kim, H.E. 215  
 Kim, Young-Sam 215–16  
 Kirby, Justice Michael 13, 18, 27, 151  
 Kirchner, J. 61  
 Kirsh, W.J. 31  
 KISA *see* Korea Information Security Agency  
*Klass v Germany* (1978) 46  
*Kommentar zum Grundgesetz für die Bundesrepublik Deutschland* (book) 85  
 Konzerndatenschutzbeauftragten 82–83  
 Koo Sze Liu 251  
 Korea Association of Information and Telecommunication (KAIT) 218  
 Korea Information Security Agency (KISA) 221, 223, 225–26  
 Korea Progressive Network Jinbonet (KPN) 219–20  
 Korea, North *see* Democratic People's Republic of Korea  
 Korean Financial Supervisory Service 220  
 Korean War 208, 214  
 Korff, D. 34  
 Kowloon City Magistrates' Court 243  
 KPN *see* Korea Progressive Network Jinbonet  
 Krüpe, Christiane 100  
*Kruslin v France* (1990) 46  
 KSH Group *see* Central Statistical Office (Hungary)  
 Kuner, C. 35, 39  
 Kwok-hung, Leung 235, 251

- L'événement* (magazine) 117  
 Labor Government (Australia) 141–2  
 Lam, T. 246  
*Lamont v Postmaster General* (1965) 57  
 Lan Kwai Fong (Hong Kong) 249  
 Langan, K.J. 61  
 Lau, Steven 242, 249  
 Laudon, K.C. 51  
 law enforcement 99, 118, 129–30, 189–90, 205, 226, 230, 234–5  
 Law for the Protection of Personal Data of 2000 (Argentina) 47  
 Law on the Protection of Personal Data of 2003 (Turkey) 47  
 Law Society (Hong Kong) 242  
 Lawson, P. 45  
*Le Monde* (newspaper) 107, 258  
 Leahy, Patrick 77  
*Leander v Sweden* (1987) 46  
 Lee Myung-Bak 228  
 Lee, L.T. 68, 250  
 legality principle 263  
 Legislative Council (LegCo) (Hong Kong) 234–5, 238  
 legitimacy principle 85–6  
*Lenah Game Meats Case* (2002) (Australia) 149  
 LG Berlin CR 2005, 530 (Germany) 100  
 LG Magdeburg DuD 2006 (Germany) 86  
 LG München (1.2.2001 12 0 13009/00) (Germany) 82  
 Libraries 68–9  
 Lilly, J.R. 68  
 Lim Su-Kyung 224  
*Lineage II* (videogame) 217  
 Linowes, D. F. 51  
 Litan, R.E. 40, 65  
 'Little Brothers' 189  
 'Little Sisters' 122  
 Liu, Koo Sze  
 London Metropolitan police 2  
 London terrorist attacks 42  
 Long, Edward 73, 51  
 'Longhair' (Hong Kong legislator) *see* Kwok-hung, Leung  
 'lottery jackpot case' (Hungary) 185  
 Lotus 74  
 Lotus MarketPlace: Households 74  
 'Lucky Country, The' 166  
 Lutterbeck, B. 85, 87  
 Lycos Europe 96  
 Lyon-Caen, G. 137  
 Madrid terrorist attacks 42  
 Magaziner, Ira 66  
 Maglio, M. 105  
 Magyar Telecom 204  
 Maisl, H. 115  
 Majtényi, László 184, 197, 206  
 Malanszuk, P. 104  
 Mallmann, Christoph, *Datenschutz in Verwaltungs-Informationssystemen* (book) 85, 87  
*Malone v United Kingdom* (1984) 46  
 Markey, Edward 77  
 Marshall Plan 26  
 Martin, K. 68–9  
 Marx, Gary 61  
 MATRIX *see* Multistate Anti-Terrorism Information Exchange  
 Mayer, T. 96  
 McGuire, R. P. 21  
 McLeish Robin 12, 251, 259, 271  
 McNealy, Scott 78  
 media violations of privacy 185, 214, 223, 236  
 medical data 64, 98, 112–13, 119–20, 133, 137–8, 140, 146, 187, 217  
 Medical Data Act (Hungary) 176  
 Medical Services Act (1995) (Republic of Korea) 210, 228  
 Medicare card (Australia) 145–46  
 Meller, P. 40  
 Metro AG 95  
 Michael, J. 29  
 Microsoft Inc. Media Player 96  
 Mill, John Stuart 74  
*Millenniumi Országjáró* (magazine) 186  
 Miller, A.R. 51–2  
 minimality principle 22  
 Minister of Justice (France) 109  
 Ministère de l'Intérieur (France) 118  
 Ministry of Administration and Security (Republic of Korea) 228  
 Ministry of Education and Human Resources Development (Republic of Korea) 213  
 Ministry of Government Administration and Home Affairs (Republic of Korea) 211

- Ministry of Health (France) 114  
 Ministry of Information and Communication (Republic of Korea) 227, 270  
 Ministry of Justice (Hungary) 179, 189  
 Ministry of the Interior (Hungary) 175, 186, 202, 206  
 Minitel 115–14  
 MKI *see* Hungarian Institute of Public Opinion Research  
 MMR 2005, 674 (Germany) 99  
 Moore, S. 79  
 Moran, Jim 50  
 Morison Report (1973) (Australia) 151  
 motor vehicles departments 50, 60, 73  
 Mulligan, D.K. 74  
 Multistate Anti-Terrorism Information Exchange (MATRIX) (USA) 70  
*My RR Card* (song) 207
- NAACP v Watkins* (1958) 53  
 National Academy of Sciences (USA) 55  
 National Assembly (Hungary) 184, 187, 190  
 National Assembly (Republic of Korea) 223, 227  
 National Education Information System (NEIS) (Republic of Korea) 212–13, 258  
 National ID Card (USA) 78–79  
 National Information Infrastructure Advisory Council (NIIAC) (USA) 63, 66  
 National Intelligence Service (NIS) (Republic of Korea) 211  
 National Police Agency (Republic of Korea) 226  
 National Privacy Principles (NPPs) (Australia) 161  
 National Research Council (USA) 79  
 National Science Foundation, Program on Ethics and Values of Science, Engineering and Technology (USA) 13  
 National Security Act (Hungary) 176  
 National Socialist regime (Germany) 84  
 National Teachers' Union 213
- National Telecommunications and Information Administration and Office of Management and Budget (USA) 63  
 NATO *see* North American Treaty Organization  
 Nazi regime, Germany 261–2  
 NC Soft 217  
 NEIS *see* National Education Information System  
*Népszabadság* (newspaper) 185  
 Netherlands 261–62, 274  
 'netizens' 223–24  
 New South Wales Privacy and Personal Information Protection Act (Australia) 158–59  
 New Territories (Hong Kong) 232  
*New York Times* 15, 78  
 New Zealand privacy practices 247  
 NGOs *see* non-governmental organizations  
 Niblett, G. B. F. 26  
*Niemietz v Germany* (1992) 46  
 NIIAC *see* National Information Infrastructure Advisory Council  
 Ninth Amendment (USA) 52  
 NIR code (numéro d'inscription au répertoire national d'identification des personnes physiques) (France) 123, 127, 131 123–24, 127  
 NIS *see* National Intelligence Service  
 Nixon, Richard M. 78  
 NJW 1999, 1777 (Germany) 98  
 NJW 2004, 1191 (Germany) 98  
 NJW 2006, 1939–1951 (Germany) 99  
 NJW 2006, 2029 (Germany) 103  
 No Camera Group (Hungary) 196  
 Nolan, J. 142  
 non-governmental organizations (NGOs)  
 Australia 144, 150, 158, 164–5  
 Hong Kong 249, 251  
 Hungary 179, 195–6  
 international 18  
 Republic of Korea 219  
 North American Treaty Organization (NATO) 190, 205  
 Northern Territory (Australia) 159  
 Norway Personal Data Act (2000) 36  
 NPPs *see* National Privacy Principles  
 Nutger A.C.M. 26

- Objektiv* (news program) 185  
 Octopus Card (Hong Kong) 231  
 OECD 30  
 Office of Management and Budget (OMB) (USA) 57, 60, 61, 63  
 Office of Technology Assessment (OTA) (USA) 61  
 Official Gazette (Republic of Korea) 211  
 Ok, K.J. 218  
 OLG Düsseldorf DUD 2005, 171 (Germany) 100  
 OLG Frankfurt CR 2005, 830 (Germany) 100  
 Olympic Games, Seoul (1988) 208  
 Omnibus Crime Control and Safe Streets Act (USA) 53  
 Omnibus Right to Privacy Act (USA) 59  
 Online Privacy Alliance (USA) 66, 76  
*OPC Annual Report* (Australia) 143, 162  
*OPC Review* (Australia) 165  
 openness principle 27, 263  
 Opinion Research Corporation 73  
 'opt-in opt-out' policies 9, 74, 135, 147  
 Option Consommateurs 7  
 Oracle Corporation 78  
 'ordre public' 94  
 Organisation for Economic Cooperation and Development (OECD) 6, 18, 26–30, 139, 209  
 original purpose principle 153  
 Orwell, George 76, 88, 121, 220  
 'Orwells' (awards) 165  
 Osswald, A. 83  
 OTP (Hungarian National Savings Bank) 192  
  
 Packard, Vance 73  
 Palladium 96  
 Paramaguru, A. 159  
 Park, Chung-hee 208  
 Park, Whon-Il 11, 218, 255, 258, 262, 268, 270, 272  
 Parliament (Australia) 141, 152, 156, 158, 161, 170, 172  
 Parliament (France) 111  
 Parliament (Hungary) 181, 183–4, 187, 193, 197, 270  
 Parliament of German Democratic Republic 87  
  
 Parliamentary Commissioner for Data Protection and Freedom of Information (Hungary) 176, 179, 181, 184, 187, 197, 200, 202  
 Parliamentary Commissioners, Act on (1993) (Hungary) 184  
 passports 170  
*Paul v Davis* (1976) 54  
 Payback (database) 82  
 PCO Annual Report 2004–05 (Australia) 145  
 Penal Code (France) 138  
 Penal Code of 1878 (Hungary) 178  
 Pentagon (Department of Defense – USA) 138  
*Pentium III* processor 74  
 People's Solidarity for Participatory Democracy 219  
 Personal Data (Privacy) Ordinance (Hong Kong) 230–31, 238–240, 246–7, 254  
 personal data definition 239–40  
 Personal Data Protection Center (Republic of Korea) 215, 221  
 personal identification 2, 87, 122–3, 146, 168, 175, 181, 202, 227, 87  
 Personal Information Collection Statements (Hong Kong) 251  
 Personal Information Dispute Mediation Committee (PIDMC) (Republic of Korea) 217, 221–3, 268  
 Personal Serial Number (for computer use) 74  
 Péterfalvi, Attila 187, 196  
 PETs *see* Privacy Enhancing Technologies  
 Pfeifer, M. 86  
 Pfitzmann, K. 104  
 Phillips, D. 40  
 PIDMC *see* Personal Information Dispute Mediation Committee  
 Pike, G.H. 69  
 Pinegar, K. R. 21  
 Platten, N. 31  
 PNR data *see* Air Passenger Name Records  
 Podlech, Adalbert 80, 85, 86, 88  
 Points for Possible Inclusion in Draft International Standards for the Protection of the Rights of the

- Individual against Threats Arising from the Use of Computerized Personal Data Systems (Doc E/CN.4/1233) (UN) 29
- Police Act (Hungary) 176
- 'policy entrepreneurs' 17–18
- political privacy 53
- Pollio, M.C. 65
- Postabank 186
- Pour les droits des citoyens face à l'informatisation de l'action sociale 120, 133
- PPSC *see* Privacy Protection Study Commission
- President of the Republic (France) 108
- President of the Republic (Hungary) 179, 193
- Presidential Order Act (1997) (Republic of Korea) 216
- 'primary groups' 3
- Prime Minister (France) 108, 118
- Prime Minister, Office of the (Republic of Korea) 228
- Privacy & American Business and Price Waterhouse, Inc. 72
- Privacy Act (1974) (USA) 4, 57, 58, 59, 61, 76, 258
- Privacy Act (1988) (Australia) 142, 150, 153, 155–63
- Privacy Amendment (Private Sector) Bill (2000) (Australia) 161
- Privacy and American Business* (survey) 72–3
- Privacy Charter (APC) (1992) (Australia) 6–7, 164–5
- Privacy Charter Council (Australia) 6
- Privacy Commissioner (Australia) 156–61, 168, 271
- Privacy Commissioner (Canada) 10
- Privacy Committee Act (1975) (Australia) 151–52
- Privacy Committee of New South Wales (Australia) 151, 160
- privacy culture 3
- Australia 166–68
- Germany 97–98
- Hong Kong 252–54
- Hungary 196–8
- Republic of Korea 214–18
- United States 74–76
- Privacy Directive (EU) *see* Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data
- Privacy Enhancing Technologies (PETs) 205, 221
- Privacy Framework *see* Asia-Pacific Economic Cooperation (APEC), Privacy Framework
- Privacy in Peril* (book) 6–7
- Privacy International 7, 18, 74, 83
- Privacy Law Project 2003 (Hong Kong) 245
- Privacy Laws & Business (2007) 48
- privacy notices principle 267
- Privacy Policy Statements (Hong Kong) 251
- privacy protection as a human right 8–9, 33, 45–6, 52–3, 112, 178, 181, 203
- Privacy Protection Study Commission (PPSC) (USA) 57, 58, 59, 62
- privacy protection vs. institutional needs 262–63, 275
- Privacy Rule (USA) 64–5
- 'privacy watchers' 7, 261, 274–5
- private sector legislation
- Australia 160–163
- France 109, 114
- Germany 87, 89–90
- Hong Kong 237–9, 254
- Hungary 176, 198
- international 20, 29, 46
- Republic of Korea 224–25
- United States 56–8
- Program on Ethics and Values of Science, Engineering and Technology (USA) 13
- Project Match 60
- Promotion of Information and Communications Network Utilization and Information Protection, Act on (1995) (Republic of Korea) 210
- Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (COM(90) 314 final – SYN 287; O.J. C 277) (1990) 31

- Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM(2005) 475 final 42
- Prosser, William 52
- Protection of Workers' Personal Data (ILO) 18
- Public Agency Data Protection Act (1995) (Republic of Korea) 210, 211, 218, 221–22, 225
- Public Agency Data Protection Act (Republic of Korea) 210
- Public Election and the Prevention of Election Corruption, Act on the (Republic of Korea) 229
- Public Election and the Prevention of Election Corruption, Act on the (Republic of Korea) 229
- Public Interest Computer Association (USA) 61
- Public Interest Research Group 76
- public offices principle 264
- public opinion on privacy protection
- Australia 163–66
  - France 117–22
  - Germany 94–97
  - Hong Kong 249–52
  - Hungary 191–96
  - Republic of Korea 211–14
  - United States 71–74
- public sector legislation
- Australia 155–60
  - France 134
  - Germany 101, 104
  - Hong Kong 238–9, 241
  - Hungary 176
  - international 29, 46
  - Republic of Korea 210–11
  - United States 56, 58
- Pueblo, USS (US naval vessel) 208
- Puplick, Chris 159
- purpose specification principle 22
- Pursuant to the Election Procedure Act (Hungary) 186–87
- Queen's University (Canada) 192
- Queensland (Australia) 160
- radio-frequency identification (RFID) chips 3, 95–6, 105, 140, 228–9
- RAF, 63<sup>rd</sup> Squadron *see* Royal Air Force, 63<sup>rd</sup> Squadron
- Reagan, Ronald 78
- Real ID Act 51
- Real Name Financial Transaction System (Republic of Korea) 215–16
- Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den ss. 100a, 100b. StPO und anderer verdeckter Ermittlungsmaßnahmen 100
- Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (2007) (OECD) 28
- Records Act (Hungary) 176
- Records, Computers, and the Rights of Citizens* (1973) (report – HEW) 55, 62
- rectification principle 23
- Red Army Faction 88
- REF International Chapter 241, 256
- Regan, Priscilla 11, 16, 57–8, 65, 68, 258, 264, 272
- Registration of Persons Ordinance (ROPO) (Hong Kong) 236
- Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data (O.J. L 8) 42
- Reichman, Nancy 61
- Reidenberg, J.R. 16, 17, 65, 224
- release or sharing principle 264
- Reno v Condon* (2000) 50
- Renseignements généraux (France) 118, 129
- Repertoire national d'identification des personnes physiques (France) 108
- Reports of Judgments and Decisions of the European Court of Human Rights 2000–I 46
- resident registration number (Republic of Korea) 207, 214–15
- Resolution 15/1991 (IV. 13.) (Hungary) 181–2

- Resolution (73) 22, Protection of the  
 Privacy of Individuals vis-à-vis  
 Electronic Data Banks in the  
 Private Sector (CoE) 20
- Resolution (74) 29–20 Protection of the  
 Privacy of Individuals vis-à-vis  
 Electronic Data Banks in the Public  
 Sector (CoE) 20
- responsibility principle 264
- revenu minimum d'insertion (RMI)  
 (France) 134
- ReverseAuction.com 67
- RFID *see* radio frequency identification  
 chips
- right to anonymity in public expression  
 53
- Right to Financial Privacy Act of 1978  
 (USA) 59, 68
- 'Robinson' lists 201
- Rockefeller Foundation 13–14
- Rodotà, Stefano 18
- Roe v Wade* (1973) 53
- Roh Tae-Woo 216
- Rosen, J. 2004
- Rosenberg, Jerry 73
- Roßnagel, A. 104
- Rothfeder, J. 64
- Roy Morgan Research 164–5
- Royal Air Force (RAF), 63<sup>rd</sup> Squadron  
 262
- Rudd Labor government (Australia) 172
- Rule, James B. 10, 14, 51, 75, 101  
*Privacy in Peril* 6–7
- Rules of procedure on the processing  
 and protection of personal data at  
 Eurojust (O.J. C 68) 43
- Rummery Case (2004) (Australia) 157
- Russell Sage Foundation 55
- SAFARI (database) 107, 108, 110, 258
- Safe Harbor protocol 15–17, 41, 103,  
 139, 264, 270
- Salzburg Forum 205
- Sandoval, G. 74
- SAP (software company) 95
- Sapphire/SQL Slammer virus 209
- SAR *see* Special Administrative Region
- Scheja, G. 102
- Schengen Information System (SIS) 43,  
 114, 130
- Schengen Region (Germany) 190
- Schengen, Convention of (1990) 43
- Schober Information Group 91
- SCHUFA 82, 90–91, 266–7
- Schwartz, P.M. 16, 39, 65, 224
- screening search methods 88
- security principle 23
- Seip, Helge 27
- Selective Service records (USA) 51
- self-regulation 58, 66, 126, 140, 160–61,  
 204, 218
- Senate Bill (S. 3418) (USA) 56
- Senate Judiciary Committee  
 Subcommittee on Constitutional  
 Rights (USA) 55
- Senate, United States 50, 55–7, 68
- sensitivity principle 23
- Seoul Central District Court 217
- Seoul City Hall 211
- Seoul District Court 213
- Seoul Prosecutors' Office 224
- September 11 attacks 67, 78–9, 98–9,  
 102, 104, 138
- Series A of the Publications of the  
 European Court of Human Rights  
 46
- Shaeffer, Rebecca 50, 64
- Shaffer, G. 40, 41
- Shattuck, J. 61
- SIM cards 232
- Simitis, Spiros 4, 15–16, 31, 33, 104
- Singapore 260
- Sino-British Declaration (1985) 233
- SIS *see* Schengen Information System
- Social Science Research Council (SSRC)  
 (USA) 55
- Social Security Number (SSN) (USA)  
 78, 107
- Social Security records (USA) 51
- SOFRES (France) 117–18
- Sorbets, C. 140
- South African Law Commission (2005)  
 47
- South Australia 160
- South Carolina and Driver's Privacy  
 Protection Act of (1994) 50
- South China Morning Post* (newspaper)  
 230, 235–6
- Soviet bloc 203, 272
- SPAM Act 2003 (Australia) 147

- spamming 116, 135–6, 147, 201, 225  
 Special Administrative Region (SAR) (Hong Kong) 232  
 Special Branch Police (Australia) 165  
 specified purpose principle 85–6  
 SSN *see* Social Security Number  
 SSRC *see* Social Science Research Council  
 Standing Committee of the National Peoples Congress (China) 233–4  
 Stanford University 14  
 Starke, J.G. 142  
 Stasi (German Democratic Republic secret police) 180  
 State of Hessen privacy protection legislation (Hessisches Datenschutzesetz) (Germany) 83  
 State Parliaments (Australia) 141–2, 150  
 State Population Registration Office (Hungary) 181  
*Statistique et développement review* (French journal) 117  
 Steinmüller, Wilhelm 80, 85, 87  
 Stender-Vorwachs, S. 99  
 STIC database *see* Système de traitement des infractions constatées  
 stored-value cards 231–32  
 student data 213, 258  
 Sun Microsystems 78  
 Sung, S. 214  
 sunset-provisions 100  
 Supreme Constitutional Court (Germany) 97, 99–100  
 Supreme Court (Republic of Korea) 214  
 Supreme Court (USA) 50–54, 57, 59, 64, 73  
 Supreme Public Prosecutors' Office (Republic of Korea) 226  
 surveillance 61, 145, 169–71, 174, 196, 216, 232, 235, 245, 249–50  
*Sweezy v New Hampshire* (1957) 53  
 Swire, P.P. 40, 65, 73  
 Switzerland 39  
 Système de traitement des infractions constatées (STIC) database 129–30  
 Szabó, M.D. 199  
 Székely, Ivan 179, 191, 192, 199, 259, 262, 270, 272  
 Szerencsejáték Rt. (Hungarian state gambling company) 185  
*Talley v CA* (1960) 53  
 Tang, Raymond 242, 249  
 Tasmania (Australia) 149–50  
 Information Privacy Bill (2007) 160  
 Tassone, A.R. 71  
 tax data 142–3  
 Tax File Number (TFN) (Australia) 142  
 Tchibo Direct GmbH 95  
 Technology for the People (Hungary) 196  
 Tele Services Data Protection Act (Germany) 96  
 Telecommunications (Interception) Act 1979 (Australia) 145  
 telecommunications 41–2, 66, 96, 99, 115–16, 134, 145, 170, 217, 230, 232, 243, 271  
 Telecommunications Business Act (1995) (Republic of Korea) 210  
 Telecommunications Ordinance (Hong Kong) 234  
*Teledienstedatenschutzgesetz AG Darmstadt* (30.06.2005, 300 C 397/04) 96  
 telemarketing 73, 134, 226  
 Tenants Unions (Australia) 162  
*Terminal* (magazine) 120  
 TFN *see* Tax File Number  
 'The Hunt for the French' 258  
*The Private Man* (book) 150  
 theft of data 88, 155, 215  
 Third Amendment (USA) 52  
 Third Republic formation (Hungary) 179, 259  
 TICA database 162  
 TICA determinations (Australia) 158, 162  
 Tingle, John 141  
 T-Online 95  
 Toonan, Nicholas 149–50  
*Toonan v. Australia* (1994) (Australia) 149–50  
 'Total Information Awareness' (TIA) 138  
 Toysmart.com 67, 74  
 transborder data flow 23–4, 43–4, 94, 102, 113, 139, 155  
 TransCore 79  
 transparency principle 23, 100  
 Transportation Security Administration (TSA) (USA) 70  
 Transunion 248

- traveler data 39, 40, 42, 69, 70, 103, 200–201
- Treaty establishing a Constitution for Europe (EU) 33
- Treaty on establishing the European Community (EU) 33
- Treaty on European Union (1992) 32, 34
- TSA *see* Transportation Security Administration
- Tsang, Donald 236
- UDHR *see* Universal Declaration of Human Rights
- UK *see* United Kingdom
- UN Guidelines *see* Guidelines Concerning Computerized Personal Data Files
- UN *see* United Nations
- UNESCO 48, 98
- UNHRC *see* United Nations Human Rights Committee
- United Kingdom (UK) 232–3, 236, 253, 259, 266
- United Nations (UN) 18, 29–30, 48
- United Nations General Assembly Resolutions  
217 A (III) (1948) 19  
2200A (XXI) (1966) 19  
2450 of 19 December (1968) 29
- United Nations Human Rights Committee (UNHRC) 149, 234
- United Nations Secretary-General 29
- United States House Committee (1966) 55
- Universal Declaration of Human Rights (UDHR) 5–6, 19, 45
- Universal Declaration on the Human Genome and Human Rights (UNESCO) 98
- University of Heidelberg (later Darmstadt) 80
- University of Hong Kong 251
- University of Regensburg (later Bremen) 80
- US Senate and House Committees (1974) 57
- US v Miller* (1976) 59
- USA PATRIOT Act (2001) 67–71, 138  
Improvement and Reauthorization Act of (2005) 69
- US–VISIT *see* United States Visitor and Immigrant Status Indicator
- Veda Advantage 144, 146, 162
- Végyvári 174
- VGH Kassel NJW 2005, 2727 (Germany) 100
- Vichy regime (France) 123
- Victoria (Australia) 159
- Victoria Labor government (Australia) 161
- Victoria Park Case* (1937) (Australia) 149
- Victoria's Secret catalog 73
- Victorian Civil and Administrative Tribunal (VCAT) 159
- Video Privacy Protection Act of 1988 (USA) 60, 73
- 'VIP list scandal' (Hungary) 186
- visa applications 138
- VISA card 92–93
- Visitor and Immigrant Status Indicator (US–VISIT) (USA) 70
- Vitale* card 137
- Vitalis, Andre 11, 108, 115, 119, 123–4, 128, 140, 258, 268, 272
- Von Hannover v Germany* (2004) 46
- Wacks, R. 251
- Wainwright Case* (2004) (UK) 236
- Wall Street Journal* 74
- 'war on terror' 10, 42, 67, 70–1, 169–71, 273
- Warren, Samuel 52
- Wassermann, Rudolf 85
- Watergate scandal 57, 73, 258, 273
- Waters, N. 155, 159
- Watkins v US* (1957) 53
- Waymann, J.L. 79
- Weichert, T. 86
- Weiss, L.B. 61
- Western Australia 160
- Westin, Alan F. 18, 51–2, 55, 57, 72
- Whalen v Roe* (1977) 54
- Whitman, James Q. 16, 17, 105
- wiretapping 145, 211, 234–5, 270
- Woo, Roderick 242, 244
- Working Party on the Protection of Individuals 37, 39, 40

- Workplace Surveillance Act 2005, NSW  
(Australia) 145
- Works Council Act (Germany) 90
- World Cup Soccer Games  
(2002) 211  
(2006) 96–7
- World Soccer Games Organisation  
Committee for the German Soccer  
Association 95
- World Trade Organization (WTO) 48
- World War I 273
- World War II 84, 123, 177, 231, 236,  
261–2, 274
- WTO *see* World Trade Organization
- Yad Vashem Archives 200
- Yahoo! 245
- Yahoo! China 242
- Yahoo! Hong Kong (YHHK) 242
- Yeh, B.T. 69
- Yi, C.B. 218
- Yugoslavia 183