PRIVACY IMPACT ASSESSMENT
PRIVACY IMPACT ASSESSMENT

Edited by

David Wright
*Trilateral Research & Consulting, London, UK*

Paul De Hert
*Vrije Universiteit Brussel, Belgium*
Privacy, like the weather, is something everyone talks about. But unlike the weather, there is much that should, and can, be done about it. This welcome volume documents and explains an important tool for doing that. It should be in the library of any professional concerned with collecting, processing, using or determining the fate of personal data (whether as policy-setter, administrator or researcher). This state-of-the-art book describes the most comprehensive tool yet available for policy-makers to evaluate new personal data information technologies before they are introduced.

Privacy impact assessment aims to contribute to organisational practice, as well as culture. It recognises that machine-processed data on persons requires special protections, particularly when new tools are involved. It anticipates problems, seeking to prevent, rather than to put out fires. The PIA model is based on avoiding future problems by learning from the past and imagining how new technologies might bring new problems – including that intriguing class of the “unknown unknowns”.

PIA is very much a work in development and offers a general model whose content needs to be adjusted depending on the specifics of the case. One size does not fit all. The variation these chapters consider precludes a standard form, at least with respect to substance and the range and degree of attention to potential problems.

Details of the assessment and expectations of what is appropriate will vary depending on the institution/organisation and goals – private vs. government (and within government national security and crime control as against education or welfare); the role played; location (as in geographical co-ordinates or in public or private places, as in visible and/or accessible); whether data is immediately available or requires technical enhancements or otherwise pried out or constructed, the kind of data – sensitive vs. non-sensitive and intimate vs. non-intimate personal information; the tool and fullness of the form of data it offers (audio and video documenting

---

1 These observations draw from various articles at www.garymarx.net and Marx, Gary T., Windows into the Soul: Surveillance and Society in an Age of High Technology, University of Chicago Press [forthcoming].

2 Of course, as several of the chapters note, a perennial problem and trade-off is intervening too early or too late. Runaway trains can’t very well be called back, even as those who build fast trains need the freedom to experiment.
behaviour vs. merely noting location); identification – unique, masked, fully anonymous or group identification; and the fate of the data – is it shared with the subjects, is it sealed, destroyed or available to the public; and the costs of trying to prevent a risk relative to its seriousness and the likelihood of its occurring. It will also vary at different stages of data collection, analysis and use, and for local, historical, cultural and social factors.

What is being assessed? Most of the chapters in the volume use privacy broadly to refer to information pertaining to an individual, particularly as it is machine-processed. It begins when the borders of the person are crossed to either take information from or impose it upon a person. Privacy is a general term and there are endless arguments about what it applies to and if it is the best term to capture contemporary concerns.

Most of the authors in this book are implicitly using the form of information privacy identified by Westin – this emphasises control by the subject. This implies an individual right and the actors’ ability to make choices. The assumption is that individuals will be well served by a policy when they decide for themselves what personal information to release. What matters is choice and treating the data in accord with Fair Information Practices. That is admirable, but it leaves untouched other important issues.

Applying the conventional principles for the machine processing of information just to information privacy will seem too narrow for many observers. Other issues of great salience for citizens and society are slighted such as the implications for social stratification; for fairness (when the choices are specious or not equally available); for human rights and for silently creating creeping precedents that might lead to unwanted results. Other forms of privacy may also be ignored.

Noting this limitation, Paul De Hert (Chapter 2) considers the need for assessments concerned with human rights more broadly than privacy may (or may not directly) connect with. Raab and Wright (Chapter 17) discuss extending assessments to take more explicit account of various surveillance activities that may touch privacy but are not synonymous with it in its narrow sense.

Whether privacy is the best term to apply to current personal data and new surveillance issues is subject to debate. In an informative exchange in Surveillance & Society, Colin Bennett acknowledges the limitations of the concept but makes a strong case for using privacy as a catch-all term for a variety of relevant information issues beyond itself. In popular culture and for interest groups, the term is becoming inclusive of an array of data issues that may connect to privacy, but go far beyond it.

---

This discussion leads us to ask: what is the PIA tool intended to prevent or, alternatively, what goals to drive forward? What does (and should) the assessment assess and why? This is forejudged to a degree by using the term privacy. But that choice can be problematic since the latter is such a general concept and can refer to such varied phenomena. Some clarification of the terms *private* and *public* and *surveillance* may be helpful.

**Untangling Terms**

*If this [dissemination of FBI criminal history records] is done properly, it’s not a breach of privacy.*

Clarence Kelley, FBI Director

Privacy is related to a broader family of terms such as publicity, surveillance, anonymity and secrecy. If PIA is to be an effective tool, there is need for a broad and systematic view of the setting and for conceptual differentiation in terminology.

How do surveillance and privacy relate? Surveillance is often wrongly seen to be the opposite of privacy. Kelvin emphasised this role of privacy as a nullification mechanism for surveillance. But at the most basic level, surveillance is simply a way of discovering and noting data that may be converted to information. This obviously can involve invasions of privacy as with the employee in a lab testing for AIDS who sold information on positive results to a mortuary.

Yet surveillance can also be a means of protecting privacy. Consider biometric identification and audit trails required to use some databases, or defensive measures such as a home security video camera. Privacy for whom and surveillance of whom and by whom and for what reasons need to be specified in any assessment.

Depending on how it is used, active surveillance can affect the presence of privacy and/or publicity. As nouns, the latter can be seen as polar ends of a continuum involving rules about withholding and disclosing, and seeking or not seeking, information. Depending on the context, social roles and culture, individuals or groups may be required, find it optional, or be prohibited from engaging in these activities, whether as subjects or agents of surveillance and communication.

The right to privacy can be matched by a right to publicity. There might even be a need for *Publicity Impact Assessments* to be sure that personal information is collected and, when appropriate, given access to a wider public.

Such assessments would be sure that surveillance and/or communication of results are mandated rather than prohibited! One form involves a right to know as with freedom of information rules. Another form can be seen in the right to be acknowledged and noted, implied in the idea of citizenship, for example, in being entitled to have a driver’s licence, register to vote or obtain a passport or a national identity.

---


identity card. In some ways, this is the reverse of an expectation not to be defamed or lied about.

When the rules specify that a surveillance agent is not to ask certain questions of (or about) a person and the subject has discretion about what to reveal, we can speak of privacy norms. When the rules specify that information must be revealed by the subject or sought by the agent, we can speak of publicity norms (or better perhaps disclosure norms). The subject has an obligation to reveal and/or the agent has an obligation to discover. With publicity norms, there is no right to personal privacy that tells the agent not to seek information, nor that gives the subject discretion regarding revelation. Rather there is the reverse – the subject has an obligation to reveal and/or the agent to discover. This also suggests a way of broadening assessments regarding personal data. Here the goal is visibility rather than data protection. A source of confusion in discussions of both privacy and publicity involves the failure to differentiate these as adjectives from nouns.

Private and Public as Adjectives

Information as a normative phenomenon involving moral expectations (whether for protection or revelation and whether based on law, policy or custom) can be differentiated from the actual empirical status of the information as known or unknown. For this, we need the related terms private and public – adjectives that can tell us about the status of information. Whether information is known or unknown has an objective quality and can be relatively easily measured. For example, in face-to-face encounters, the gender and face of a stranger are generally known, regardless of place in the street, an office or a home. The information is “public”, as in readily accessible. In contrast, their political or religious beliefs are generally invisible and unknown. Of course, normative expectations of privacy and publicity do not always correspond to how the adjectives public and private are applied to empirical facts. Thus,

9 There may, however, be rules about the subsequent recording, communication and use of such information.
10 Identification may be controlled through anti-mask laws or conversely through requiring veils for females or the display of religious or other symbols (tattoos, brands, badges) or clothing indicating status.
11 Revelation, of course, may be mandated by rules requiring the wearing of symbols indicating these. This paragraph also assumes that in most cases people “are” what they appear to be, i.e., no cross-dressing.
the cell phone conversations of politicians and celebrities that have privacy protections may become public. Information subjected to publicity requirements such as government and corporate reports and disclosure statements may be withheld, destroyed or falsified. Information not entitled to privacy protections, such as child or spouse abuse, may be unknown because of the inaccessibility of the home to broader visibility. The distinction here calls for empirical analysis of the variation in the fit between the rules about information and what actually happens to it.

Privacy and publicity can be thought of in literal and metaphorical spatial terms involving invisibility-visibility and inaccessibility-accessibility. The privacy offered by a closed door and walls and an encrypted e-mail message share information restriction, even as they differ in many other ways. Internet forums are not geographically localised, but in their accessibility can be usefully thought of as public places, not unlike the traditional public square where exchanges with others are possible.

There would be more agreement, or at least greater clarity, if assessments of privacy were clearer about whether they are talking about respect for the rules protecting privacy or the empirical status of information as known or not known. When the laws are followed, former FBI director Clarence Kelley (in the quote that begins this section) can correctly claim that they haven’t been breached with respect to privacy. But he could not claim that, as an empirical matter, privacy is not altered when such records are created and circulated.12

**Types of Privacy**

Privacy is a multi-dimensional concept with fluid and often ill-defined, contested and negotiated contours, depending on the context and culture. PIAs should be clear about what privacy means for the context with which they are concerned (and often more than one meaning will apply).

Within informational privacy with which the chapters here are largely concerned, we find the conditions of anonymity and pseudo-anonymity, often referred to as being necessary for another type of privacy involving seclusion and being left alone. Personal borders are obviously more difficult to cross if an individual cannot be

12 There can, of course, be verbal prestidigitation, not to mention bad faith, in simply defining away invasions of privacy as non-existent because the law or rules are followed. The deeper issue is what degrees of control does the individual have over personal and private information and are the lines appropriately drawn given a society’s values and broader transcendent values of human dignity and life.

There are also other sources of confusion such as the legal definition of geographical places and information as public or private, custom and manners (e.g., averting the eyes) and roles which offer varying degrees of access to information. See Marx, Gary T., “Identity and Anonymity: Some Conceptual Distinctions and Issues for Research”, in J. Caplan and J. Torpey (eds.), *Documenting Individual Identity*, Princeton University Press, 2001.
reached via name or location. The conditions around revelation or protection of various aspects of identity are central to the topic.

Informational privacy encompasses physical privacy. The latter can refer to insulation resulting from natural conditions such as walls, darkness, distance, skin, clothes and facial expression. These can block or limit outputs and inputs. Bodily privacy is one form of this. This is seen in crossing the borders of the body to implant something such as a chip or birth control device or to take something from it such as tissue, fluid or a bullet.\(^{13}\)

A related, taken-for-granted form is aesthetic privacy\(^{14}\) which refers to the separation, usually by a physical barrier of bedroom or bathroom, of activities involving one’s “private parts” (a curious term given public knowledge of the limited variation of the parts) and unguarded moments. Alderman and Kennedy discuss a number of such cases in which the shock of discovering a violation surfaces norms of which we are hardly aware because they are so rarely violated.\(^{15}\) Clothes and manners also sustain this. The concern over full body airport scans is also illustrative.

Informational privacy can be further descriptively considered as it ties to institutional setting (e.g., financial, educational, health, welfare, employment, criminal justice, national security, voting, census); places and times; the kind of data involved such as about religion or health, apart from the setting; participant roles (communications privacy as involving two-party, one-party or no-party consent); and aspects of the technology such as wire or wireless, phone, computer, radio or TV. PIAs need to consider setting, data type and means – factors that are central to legislation and regulation and rich in anomalies.\(^{16}\)

In emphasising informational privacy, several other commonly considered forms such as decisional\(^{17}\) or proprietary\(^{18}\) privacy are slighted. These primarily involve application or use, rather than information discovery.

Defining cases in the US such as *Griswold v. Connecticut* 381 U.S. 479 (1965) and *Roe v. Wade*, 410 U.S. 11 (1973) involve decisional privacy with respect to personal and intimate matters such as family planning, birth control, same sex

---

\(^{13}\) The physical border perspective has limits too, thus taking/giving a urine, breath sample or photo involves using things that have already left the body and are different and beyond the literal physical protective border. The situation is the same for garbage. The borders in such cases are cultural – note the tacit assumption that one’s garbage isn’t to be examined – at least in a personally identifiable way.


\(^{16}\) Thus, in the US, the Federal Communications Commission has jurisdiction over content delivered over a wire but not that by satellite. In countries such as Germany and France, privacy rights are defined in reference to broad constitutional principles such as the dignity of the person, while in the US, the particular technology or institution plays a much larger defining role.


marriages or physician-assisted suicide. Proprietary privacy – use of a person’s information without consent for commercial and other purposes also involves control and liberty questions and the extension of market principles to symbolic material that is often immaterial (at least physically).

While distinct, informational privacy shares with the other forms inclusion in the broader category of privacy as control over access to the person or at least the person’s data, these may be connected. Thus, if individuals can control their personal information – whether not having to reveal their purchase of birth control pills (when this was illegal) or keeping paparazzi from taking pictures, then they need not worry about that information being used.

In addition to conceptual elaboration and reflection on the broader consequences of data collection, privacy assessment needs can be analysed in more detail when protective activities and problem avoidance are connected to a series of sequential stages that can be observed in the process (and processes) of data generation and use. Various types of privacy problem do not occur randomly, but tend to cluster at particular social locations.

**Data Stages**

Privacy protection is not like a vaccination that occurs once and is over. Rather it is part of an enduring process involving a series of separate actions.

Table 1 lists seven kinds of activity called *surveillance strips* that follow each other in logical order. The strips are temporally, conceptually, empirically and often spatially distinct.

Over time, the distinct action fragments of these stages combine into stories about personal data and illustrate the emergent character of surveillance and privacy as multi-faceted abstractions made up of many smaller actions. These are not unlike the frames in comic books (although not intended to be entertaining and the patterns are more like the fluid, jumpy sequences of cyberspace explorations than the rigid frame ordering of the comic book).

When viewed sequentially and in their totality, these elements constitute *surveillance occasions.* A surveillance occasion begins when an agent is charged with

<table>
<thead>
<tr>
<th>Table 1 Seven surveillance strips</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) tool selection</td>
</tr>
<tr>
<td>(2) subject selection</td>
</tr>
<tr>
<td>(3) data collection</td>
</tr>
<tr>
<td>(4) data processing/analysis [raw data] numerical/narrative</td>
</tr>
<tr>
<td>(5) data interpretation</td>
</tr>
<tr>
<td>(6) uses/action – primary, secondary uses/users and beyond</td>
</tr>
<tr>
<td>(7) data fate (restricted, sealed, destroyed, made public – conditions and time periods for such actions)</td>
</tr>
</tbody>
</table>

the task of gathering information. Following that, the seven phases in Table 1 can be considered. Studying the behavioural sequences of tool selection, subject selection, data collection, data processing, interpretation, resulting action (or inaction) and fate of the data offers a way to order the basic behaviours occurring within the family of direct surveillance actions. The stages are the direct pressure points where most problems will be found.

Sometimes these occur almost simultaneously as when a motion sensor is triggered, a message is sent to a central computer, an alarm sounds and a door is locked or a retinal pattern is matched to a given identity and a computer unlocks or when a video camera does not save what unproblematic passes before it. But for a goodly proportion of applications, as with drug testing or data mining, these consist of different activities and stages and involve a division of labour with agent roles played by various actors.

In a given story, the stages may develop in a serial fashion as one stage logically leads to the next (e.g., from data collection to analysis) or it may stop early on (a tool and subject are identified but no data is collected, or the data is not analysed or applied). Looking across many cases suggests a variety of ideal-type career patterns (with different stopping and turning points). However, once data has been gathered, questions regarding the data’s fate (the last item in the chain) can always be asked. Apart from any policies regarding destruction, sealed, limited or open access, in practical terms, the data’s fate is affected by the form the data takes and how it is communicated. A paper record that exists in only one copy in a locked filing cabinet obviously differs greatly from a postable computer record that can endlessly recirculate, whatever the policies on access.

Most of the privacy and related problems with which PIAs are concerned occur (when present) at one of the stages in Table 1. The kind of problem may differ by stage – thus violations of consent are likely at data collection, of fairness and validity at processing and interpretation, of discrimination at use and of confidentiality at data fate.

It would be useful to have a checklist of problems that can occur and (when possible) of ways of avoiding them, or ameliorating them when they can’t be prevented. The list would include various kinds of physical, psychological and social harm and unfairness in application and use; minimising invalid or unreliable results; not crossing a personal boundary without notice or permission (whether involving


Decisions about who is responsible for doing the surveillance and the design of the technology could be treated as the initial strips as well. However, attention here is on the next stage directly associated with doing the surveillance.

This is said mindful of the fact that it is always possible to make ever greater differentiations within the categories identified and to push the causal chain back farther. For example, with respect to the data collection phase, contrasts can be made based on the tool, the sense involved, the kind of activity or the goal. The Table 1 conceptualisation captures the major natural breaks in activity once a problem in need of personal information has been defined and an agent designated.
coercion or deception or a body, relational, spatial or symbolic border). Other problems to be avoided involve violating trust and assumptions that are made about how personal information will be treated (e.g., no secret recordings, respect for confidentiality, promises for anonymity, for the compartmentalisation of kinds of data, and for their protection or destruction).

What are the trade-offs, advantages, disadvantages and conflicts in the various policy options for dealing with these problems (including doing nothing because of the rarity of some or because costs of prevention are deemed too great)? When do solutions bring new problems? How clear are the means and quality of evidence for assessing these issues?

Lists are one thing and can be a bit like waving the flag. Who, after all, would favour invalid results or violating trust? There is a strong need for research on the frequency and social locations of such problems. When are they common, patterned and systemic as against being infrequent, random and idiosyncratic?

Knowledge and policy are better served when these elements are differentiated. The stages in Table 1 can direct research on the correlates and location of particular kinds of problems. Awareness of the stages of the process can help in assessing the seriousness and likelihood that a risk will occur and the costs of prevention (whether by not using, regulating or amelioration after the fact).

The likelihood of prevention is also greatly affected by the stage. Just saying “no” to a data collection request (if honoured) is the ultimate prevention. But as the process moves from collection to the final fate, controls become more challenging. In the initial stages, the relevant actors and locations for accountability are known – but over time, if the information spreads out in wider circles and is combined with other data, as often happens, control weakens. The form of the data matters as well – the type of format, encryption, self-destroying, identity-masking, in a single highly secure file or in a more open system, The ointment-out-of-the-tube metaphor for digitised data speaks volumes.

Slices, Not Loaves

If the wise suggestions this specialised volume recommends were implemented, there would be far fewer problems associated with the collection and processing of personal data. However, the authors are hardly naïve reformers promising salvation if only their preferred solutions are followed. Limits are identified, as are ways of working within or around many of them.

Sceptical pundits removed from any responsibility for action can, of course, snipe from the sidelines about PIAs and their limits. PIAs are generally not mandated, requiring voluntary introspection and self-restraint on the part of goal-focused (often bottom line) organisations.22 Businesses are not democracies and government’s national security and crime functions require levels of secrecy. When a PIA

---

22 There are a few exceptions as several chapters here note such as in Europe for RFID and in the US for e-government.
is carried out, results may not become public. Will a PIA’s requirements be imple-
mented? Or will PIAs serve as window dressing disingenuously prohibiting, while
hiding behaviour that would be unacceptable if made public? Will they become
another ritualised hurdle to jump over (or under) for busy practitioners with more
important goals?

In an effort to learn and to legitimate, the ideal PIA involves relevant “stakehold-
ers”. This democratic impulse is admirable, but who decides who is a legitimate
stakeholder? – e.g., do those arrested, but not charged or found guilty, have a seat at
the table when decisions are made about preserving DNA? Do free speech as well as
privacy advocates serve on a telecommunications committee charged with assessing
a new technology?\(^{23}\)

PIA faces the challenge of preventing a particular kind of future which involves
new elements. It goes beyond routine audits of compliance with established rules
and policies. Since the future hasn’t yet happened, its assessment is forever
vulnerable to challenges and doubts.

Given still other challenges – from political pressures to lack of resources, it
is noteworthy that the stellar policy analysts in this book have not given up. They
are thoughtful realists – dealing humbly, yet hopefully, with terribly complicated
contemporary questions. In situations drenched in trade-offs, legitimate conflicts of
interest and uncertainty, the lack of a full loaf should not be bemoaned, rather one
should be grateful for slices of insight and the amelioration that PIAs can bring
through transparency and a commitment to democratic values.

Cambridge, Massachusetts

Gary T. Marx

\(^{23}\) The failure to not include types of consumers in the decision to roll out caller-ID created prob-
lems for US telephone companies in the 1980s. Those with unlisted numbers and shelters for
abused women lost control over their phone numbers by technological fiat and there was much
public outcry which led to revised policies.
## Contents

**Foreword by Gary T. Marx: Privacy Is Not Quite Like the Weather** ........................................... v

**Part I Setting the Scene**

1. **Introduction to Privacy Impact Assessment** ........................................... 3
   David Wright and Paul De Hert
   1.1 Growing Interest .............................................................................. 3
   1.2 A Few Key Definitions .................................................................. 5
   1.3 A PIA Timeline ............................................................................. 8
   1.4 Why Carry Out a PIA? ................................................................... 10
     1.4.1 To Manage Risks .................................................................... 10
     1.4.2 To Derive Benefits .................................................................. 16
   1.5 Variations in PIA Approaches ....................................................... 17
   1.6 Open Issues .................................................................................. 23
     1.6.1 Scale and Scope of the PIA ..................................................... 24
     1.6.2 Who Should Perform the PIA? ................................................ 25
     1.6.3 Should Engaging External Stakeholders Be Part of the PIA Process? ................................................................................. 26
     1.6.4 Should PIAs Be Published? ..................................................... 27
     1.6.5 Should PIAs Be Mandatory? ................................................... 28
     1.6.6 Should the DPA or Privacy Commissioner “Approve” a PIA? ...................................................................................... 29
     1.6.7 Should a PIA Apply to the Development of New Policy? ...................................................................................... 30
     1.6.8 Two or More Organisations Collaborating on a PIA . ...................................................................................... 30
     1.6.9 Are Trans-national PIAs Feasible? ........................................... 31
   1.7 Objectives and Scope of This Book .................................................. 31

2. **A Human Rights Perspective on Privacy and Data Protection Impact Assessments** ........................................... 33
   Paul De Hert
   2.1 Terminology .................................................................................. 33
   2.2 Data Protection Impact Assessments ............................................. 34
   2.3 Privacy Impact Assessment: What Is Privacy? .............................. 38
2.4 Privacy Impact Assessments: Privacy and Permissible Limitations .............................................. 40
2.5 The Technology Should Be Used in Accordance with and as Provided by the Law (First PIA Element) .................................................. 45
   2.5.1 Open Questions About the Transparency and Legality Requirement ........................................... 48
2.6 The Technology or Processing Should Serve a Legitimate Aim (Second PIA Element) .................. 49
2.7 The Technology Should Not Violate the Core Aspects of the Privacy Right (Third PIA Element) ........ 51
2.8 The Technology Should Be Necessary in a Democratic Society (Fourth PIA Element) ...................... 54
   2.8.1 Necessity, Evidence and Politics ................................................................. 56
2.9 The Technology Should Not Have or Give Unfettered Discretion (Fifth PIA Element) ......................... 59
2.10 The Technology Should Be Appropriate, Least Intrusive and Proportionate (Sixth PIA Element) ........ 61
   2.10.1 Appropriateness and the Least Intrusive Method ................................................. 63
   2.10.2 The Fair Balance Requirement, Evidence and Precaution ................................................. 66
   2.10.3 The Fair Balance Requirement, Stakeholder Participation and Impact Assessments ................. 70
2.11 The Technology Should Not Only Respect Privacy Requirements But Also Be Consistent with Other Human Rights (Seventh PIA Element) ............................................. 72
2.12 Conclusion ...................................................................................................................... 74

3 (Regulatory) Impact Assessment and Better Regulation .......... 77
   David Parker
   3.1 The Development of (Regulatory) Impact Assessment ............................................................. 79
   3.2 Use of RIA/IAs in the UK ................................................................................................. 81
   3.3 RIA/IAs and the European Commission ............................................................................ 92
   3.4 Conclusions ..................................................................................................................... 95

4 Prior Checking, a Forerunner to Privacy Impact Assessments ..... 97
   Gwendal Le Grand and Emilie Barrau
   4.1 Introduction .................................................................................................................... 97
   4.2 How Prior Checking Has Been Implemented .................................................................... 98
   4.2.1 Prior Checking Has Been Transposed in the National Legislation of Most Member States and Is Used by Most Member States .......................................................... 98
   4.2.2 Prior Checking Is Limited to Operations Likely to Present Specific Risks in Most Countries . 99
   4.2.3 Categories of Processing Operations, When They Are Defined, Are Not Homogeneous .... 100
   4.2.4 Exemptions Are Foreseen in Half of the Countries ................................................... 102
4.2.5 Prior Checking in the Context of National Legislative Measures and Regulations is Carried Out in Half of the Countries ........ 103

4.3 How Prior Checking Has Worked in Practice ........ 105
4.3.1 Prior Checking Takes Different Forms at National Level; Data Protection Authorities Use Several Tools ........ 105
4.3.2 The Format and Publicity of the Data Protection Authorities’ Decisions Are Not Harmonised Across Europe ........ 106
4.3.3 Data Protection Authorities Usually Set a Time Limit to Complete Prior Checking ........ 107
4.3.4 In the Context of Prior Checking, Notifications by the Controller Usually Do Not Include More Information than Notifications for Other Types of Processing ........ 108
4.3.5 Data Protection Authorities Have Developed Specific Instruments or Procedures for Processing Operations Subject to Prior Checking .......... 109
4.3.6 Decisions of the Data Protection Authorities Can Generally Be Appealed Before an Administrative Court ........ 110
4.3.7 Data Controllers Who Start Processing Operations Without Notifying the Data Protection Authority Most Likely Get Fined .... 110

4.4 Lessons Learned from Prior Checking ........ 111
4.4.1 Assessment of the Current Prior Checking System and Potential Evolutions ........ 111
4.4.2 Data Protection Authorities Use Tools to Complement Prior Checking ........ 112
4.4.3 What Role for Privacy Impact Assessments? .... 112

4.5 Conclusion ........ 115

Part II Five Countries Lead the Way

5 PIAas in Australia: A Work-In-Progress Report ........ 119
Roger Clarke
5.1 Introduction ........ 119
5.2 The Nature of PIAs ........ 120
5.3 The History and Status of PIAs in Australia ........ 120
5.3.1 Pre-2000 ........ 122
5.3.2 Post-2000 ........ 123
5.3.3 The 10 Contexts ........ 124
5.4 PIA Guidance Documents ........ 137
5.4.1 Evaluation Criteria ........ 137
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.2</td>
<td>The Victorian Privacy Commissioner’s Guide</td>
<td>138</td>
</tr>
<tr>
<td>5.4.3</td>
<td>The Australian Privacy Commissioner’s Guide</td>
<td>139</td>
</tr>
<tr>
<td>5.5</td>
<td>Future Developments</td>
<td>142</td>
</tr>
<tr>
<td>5.5.1</td>
<td>The States and Territories</td>
<td>142</td>
</tr>
<tr>
<td>5.5.2</td>
<td>The OAPC/ICO</td>
<td>144</td>
</tr>
<tr>
<td>5.5.3</td>
<td>The ALRC’s Recommendations</td>
<td>144</td>
</tr>
<tr>
<td>5.5.4</td>
<td>The Government’s Response</td>
<td>146</td>
</tr>
<tr>
<td>5.6</td>
<td>Conclusions</td>
<td>147</td>
</tr>
<tr>
<td>6</td>
<td>Privacy Impact Assessment – Great Potential Not Often Realised</td>
<td>149</td>
</tr>
<tr>
<td>6.1</td>
<td>Introduction</td>
<td>149</td>
</tr>
<tr>
<td>6.2</td>
<td>A Useful Analogy?</td>
<td>150</td>
</tr>
<tr>
<td>6.3</td>
<td>What Is PIA?</td>
<td>150</td>
</tr>
<tr>
<td>6.4</td>
<td>PIA and Privacy by Design</td>
<td>150</td>
</tr>
<tr>
<td>6.5</td>
<td>PIA and Privacy Auditing</td>
<td>151</td>
</tr>
<tr>
<td>6.6</td>
<td>Who Should Be the Client?</td>
<td>152</td>
</tr>
<tr>
<td>6.7</td>
<td>In an Ideal World . . .?</td>
<td>153</td>
</tr>
<tr>
<td>6.8</td>
<td>Using PIA Findings to Effect Change</td>
<td>153</td>
</tr>
<tr>
<td>6.9</td>
<td>Some Examples of PIA</td>
<td>155</td>
</tr>
<tr>
<td>6.9.1</td>
<td>Online Authentication for e-Government in New Zealand</td>
<td>155</td>
</tr>
<tr>
<td>6.9.2</td>
<td>Retention and Linkage of Australian Census Data</td>
<td>156</td>
</tr>
<tr>
<td>6.9.3</td>
<td>The Australian Financial Reporting Regime</td>
<td>156</td>
</tr>
<tr>
<td>6.9.4</td>
<td>Individual Identifiers for e-Health in Australia</td>
<td>157</td>
</tr>
<tr>
<td>6.9.5</td>
<td>Hong Kong Smart Identity Card</td>
<td>158</td>
</tr>
<tr>
<td>6.10</td>
<td>Conclusion</td>
<td>160</td>
</tr>
<tr>
<td>7</td>
<td>Privacy Impact Assessments in Canada</td>
<td>161</td>
</tr>
<tr>
<td>7.1</td>
<td>Introduction</td>
<td>161</td>
</tr>
<tr>
<td>7.1.1</td>
<td>The Canadian Privacy Legislative Framework</td>
<td>162</td>
</tr>
<tr>
<td>7.2</td>
<td>The Conduct of PIAs in Canada</td>
<td>164</td>
</tr>
<tr>
<td>7.2.1</td>
<td>The Legal Basis for Privacy Impact Assessments</td>
<td>164</td>
</tr>
<tr>
<td>7.2.2</td>
<td>Who Conducts PIAs?</td>
<td>166</td>
</tr>
<tr>
<td>7.2.3</td>
<td>Private Sector PIAs</td>
<td>168</td>
</tr>
<tr>
<td>7.2.4</td>
<td>When PIAs Are Required</td>
<td>169</td>
</tr>
<tr>
<td>7.2.5</td>
<td>PIAs Involving State Security, Law Enforcement and International Projects and Agreements</td>
<td>171</td>
</tr>
<tr>
<td>7.2.6</td>
<td>PIA Characteristics and Methodology</td>
<td>172</td>
</tr>
<tr>
<td>7.2.7</td>
<td>The Audit and Review of PIAs</td>
<td>175</td>
</tr>
<tr>
<td>7.2.8</td>
<td>The Publication of PIAs</td>
<td>180</td>
</tr>
<tr>
<td>7.3</td>
<td>Conclusions</td>
<td>182</td>
</tr>
</tbody>
</table>
8 Privacy Impact Assessment in New Zealand – A Practitioner’s Perspective
John Edwards
8.1 Introduction ........................................... 187
8.2 Background ........................................... 188
8.3 A Short History of Privacy Impact Assessment
in New Zealand ........................................... 188
8.4 Undertaking Privacy Impact Assessments ........ 193
8.5 Timing ....................................................... 194
8.6 The Cost of Privacy Impact Assessment ............ 195
8.7 For Whom Is the Report Prepared? ................. 196
8.8 Problems with Privacy ................................. 196
8.9 Independence ............................................ 199
8.10 Givens ..................................................... 199
8.11 Scope Constraints ....................................... 200
8.12 Legal Professional Privilege Applies ................ 201
8.13 After the Assessment? ............................... 202
8.14 Conclusion .............................................. 203

9 Privacy Impact Assessment in the UK .............. 205
Adam Warren and Andrew Charlesworth
9.1 Introduction ........................................... 205
9.2 Legislative and Policy Framework .................. 207
9.2.1 Legislation ........................................... 208
9.2.2 Policy .................................................... 210
9.3 The UK PIA Process .................................... 211
9.4 Case Study: Office for National Statistics (ONS), 2011 Census 214
9.5 Lessons Learnt .......................................... 216
9.6 Future Developments .................................. 221
9.7 Conclusion .............................................. 223

10 PIA Requirements and Privacy Decision-Making in US Government Agencies ............... 225
Kenneth A. Bamberger and Deirdre K. Mulligan
10.1 Introduction ........................................... 225
10.2 The US PIA Requirement and Its Implementation ...... 228
10.3 Challenges Inherent in the PIA Model .............. 230
10.3.1 Limits of Process .................................... 230
10.3.2 Substantive Barriers to Oversight .................. 231
10.4 Seeking Ways to Overcome Barriers to PIA Success:
Learning from the US Experience ...................... 235
10.4.1 Lessons from NEPA .................................. 236
10.5 Suggestions from the US PIA Experience: The RFID Cases .... 237
10.5.1 The Cases in Brief ................................... 238
10.5.2 Possible Elements of Variance ...................... 240
10.6 Status and Independence of Embedded Privacy Experts .......... 241
10.7 Expert Personnel, Integrated Structure and the PIA Tool ........ 245
Contents

10.7.1 Creating Accountability in the Absence of Oversight: The Privacy and Integrity Advisory Committee ................................ 248
10.8 Directions for Further Inquiry .................................................. 249

Part III PIA in the Private Sector: Three Examples

11 PIA: Cornerstone of Privacy Compliance in Nokia .......................... 253
Tobias Bräutigam
11.1 Introduction ................................................................. 253
11.2 Definitions ................................................................. 255
  11.2.1 Privacy ............................................................ 255
  11.2.2 Personal Data ....................................................... 256
  11.2.3 PCI DSS .......................................................... 256
  11.2.4 PIA, PISA ......................................................... 256
  11.2.5 Nokia .............................................................. 256
11.3 Nokia’s Approach to Privacy .................................................. 256
  11.3.1 Governance Model ................................................. 257
  11.3.2 Other Measures in Support of Privacy ......................... 259
  11.3.3 Reasons for Conducting Privacy Assessments ............. 260
11.4 The Process, or How Privacy Assessments Are Conducted .......... 261
  11.4.1 Two Kinds of Privacy Assessments ........................... 261
  11.4.2 Undertaking a PISA .............................................. 261
  11.4.3 The PIA Process – Deviations from PISA ................. 263
11.5 The Content of Privacy Assessments ....................................... 264
  11.5.1 The PISA Template .............................................. 264
  11.5.2 The PIA Template ................................................ 267
11.6 Areas for Improvement ...................................................... 269
  11.6.1 Quality of the Requirements That Are Assessed ............ 269
  11.6.2 Resources ......................................................... 270
  11.6.3 Awareness ........................................................ 270
  11.6.4 Evaluating Findings ............................................. 271
  11.6.5 Information Not Available ..................................... 271
  11.6.6 Corrective Actions .............................................. 271
  11.6.7 Speed of Execution .............................................. 271
11.7 Conclusion and Summary: 10 Recommendations ....................... 271
  11.7.1 Start Small, But Start ............................................ 272
  11.7.2 Awareness ........................................................ 272
  11.7.3 Privacy Assessments Need to Be Supported by a Governance Model .. 272
  11.7.4 Definitions of Requirements Must be as Self-Explanatory as Possible .. 273
  11.7.5 Include Open Questions in the Assessments ............... 273
  11.7.6 Specialisation .................................................... 273
  11.7.7 Cultivate a Culture of Continuous Improvement and Open Communication .. 273
12 How Siemens Assesses Privacy Impacts .............................. 275
Florian Thoma
12.1 Siemens at a Glance ........................................... 275
12.2 Terminology .................................................... 276
12.3 Some Challenges ................................................ 276
12.4 The Data Protection Officer’s Tasks ............................ 277
12.5 Prior Checking .................................................. 278
12.6 Processor Audits ............................................... 279
12.7 Group IT System Assessment: Inter-company Agreements ... 280
12.8 Assessment of Offshoring and Outsourcing Projects ......... 281
12.9 Advantages of Privacy Impact Assessments ......................... 282
12.10 Involvement of Data Protection Authorities ...................... 283
12.11 Moving Forward .............................................. 283

13 Vodafone’s Approach to Privacy Impact Assessments ............. 285
Stephen Deadman and Amanda Chandler
13.1 Introduction ...................................................... 285
13.2 Vodafone’s Core Business Operations .......................... 286
13.3 The External and Industry Environment ........................ 287
13.4 Vodafone’s Policy and Approach to Privacy Risk Management 287
13.4.1 Governance and Accountability ................................ 288
13.4.2 Principles .................................................... 288
13.5 Privacy Impact Assessments .................................... 289
13.6 Vodafone’s Privacy Programme .................................. 289
13.7 The Role of the PIA in the Vodafone Privacy Programme ...... 290
13.7.1 Strategic Privacy Impact Assessment ......................... 290
13.7.2 Case Study – Location Services ............................. 291
13.8 PIA and the Privacy Risk Management System (PRMS) ....... 295
13.8.1 Strategic Aims and Objectives of the PRMS ................. 295
13.8.2 Key Operational Controls in the PRMS ..................... 296
13.9 The Role of the Privacy Officer .................................. 301
13.10 The Role of Privacy Impact Assessment in the PRMS ........... 302
13.11 Conclusion – The Value of Privacy Impact Assessments ....... 303

Part IV Specialised PIA: The Cases of the Financial Services Industry and the RFID PIA Framework

14 The ISO PIA Standard for Financial Services ....................... 307
John Martin Ferris
14.1 Introduction ...................................................... 307
14.2 Overview of the ISO 22307:2008 Voluntary Consensus Standard .................................................. 308
14.2.1 A PIA Is Useful During Any Phase of a System’s Life Cycle 308
14.2.2 A PIA Requires a Process Including a Plan 309
14.2.3 A PIA Needs an Adequate Description of the System 310
14.2.4 A PIA Standard Should Be Neutral on Frameworks That Support a PIA Development 310
14.2.5 A PIA Is Not a Privacy Audit 313
14.3 History of ISO 22307:2008 313
14.4 Voluntary Consensus Standards 315
14.4.1 ISO TC 68 316
14.4.2 Business Challenges of ISO TC 68 and Voluntary Consensus Standards 316
14.4.3 ISO TC 68 Security and Privacy Work 319
14.4.4 Choosing Voluntary Consensus Standards 319
14.5 Summary 321

15 The RFID PIA – Developed by Industry, Endorsed by Regulators 323
Sarah Spiekermann
15.1 Introduction – The History of the RFID PIA 323
15.2 Preliminary Considerations Before Engaging in a PIA 327
15.3 Initial Analysis to Determine the Scope of PIA 329
15.4 PIA Risk Assessment Process 333
15.4.1 How Is the Risk Assessment Done Step By Step? 334
15.5 PIA Reporting 344
15.6 Conclusion 344

16 Double-Take: Getting to the RFID PIA Framework 347
Laurent Beslay and Anne-Christine Lacoste
16.1 An Introduction to the RFID Recommendation 347
16.2 Conditions of Involvement of the Art. 29 WP 348
16.3 The Different Actors Involved in the Recommendation 349
16.3.1 The European Data Protection Supervisor 349
16.3.2 The European Network and Information Security Agency 349
16.3.3 Industry 350
16.3.4 National Authorities and Agencies 350
16.4 From a Negative Opinion of the WP29 to a Positive One 350
16.4.1 The July 2010 Opinion of the Art. 29 WP and the Issue of Risk Analysis 350
16.5 Endorsement of the Art. 29 WP: Consequences and Further Steps 354
16.6 PIA in Perspective 356
16.6.1 PIA for RFID Applications and Impact Assessments in a Regulatory Process 356
16.6.2 The Issue of Representativeness of the Industry Group .......................... 356
16.6.3 PIA Procedure: A Voluntary Action ................................................. 357
16.6.4 The PIA Framework for RFID: An Example for Other Technological Fields? .............................................................. 358
16.7 Conclusion: Efficiency of PIA and Residual Risk: A Difficult Compromise .......................... 358

Part V Specific Issues

17 Surveillance: Extending the Limits of Privacy Impact Assessment .. 363
Charles Raab and David Wright
17.1 Introduction ........................................................... 363
17.2 Objections to Subjecting Surveillance to PIA .................................. 364
17.2.1 A Brake on Technical Progress ............................................. 364
17.2.2 Some Surveillance Involves Central Functions of the State .............. 365
17.2.3 Some Surveillance Involves Commercial Sensitivity ...................... 366
17.2.4 Some Surveillance Involves More Than One Country ..................... 367
17.2.5 Ineffectiveness Would Be Revealed by a PIA ................................ 368
17.2.6 PIA Is Too Narrowly Focused ................................................. 369
17.3 Types of Surveillance ...................................................... 369
17.3.1 Watching ............................................................... 370
17.3.2 Listening ............................................................... 370
17.3.3 Locating ............................................................... 370
17.3.4 Detecting ............................................................... 371
17.3.5 Dataveillance ............................................................ 372
17.3.6 Assemblages ............................................................. 372
17.3.7 Surveillance: Causes of Concern ............................................ 373
17.4 Who Are the Surveillants, and Why Do They Use Surveillance? ........ 374
17.4.1 Public Sector ............................................................ 374
17.4.2 Private Sector ........................................................... 375
17.4.3 Society ................................................................. 375
17.5 Assessing Surveillance Effects: Privacy and Beyond ........................ 376
17.6 Conclusion ................................................................. 382

18 The Madrid Resolution and Prospects for Transnational PIAs .. 385
Artemi Rallo Lombarte
18.1 The Madrid Resolution ...................................................... 385
18.1.1 Origin of the Document ................................................... 385
18.1.2 The Contents of the Madrid Resolution ................................... 387
18.2 Privacy Impact Assessments in the Madrid Resolution ...................... 390
18.3 Reception of the Madrid Resolution ........................................... 392
18.3.1 Towards a Binding International Instrument ............................... 392
18.3.2 Mexico: First Country to Incorporate the Resolution into Its Legal System 394
18.3.3 Europe: Influence of the Madrid Resolution on the “Future of Privacy” 394
18.4 Conclusions 395

19 Privacy and Ethical Impact Assessment 397
David Wright and Emilio Mordini
19.1 Introduction 397
19.2 Governance Issues in the Practice of an Ethical Impact Assessment 401
19.2.1 The Role of Ethics 401
19.2.2 Consulting and Engaging Stakeholders 402
19.2.3 Accountability 404
19.2.4 Providing More Information, Responding to Complaints and Third Party Ethical Review 405
19.2.5 Good Practice 406
19.3 Ethical Principles 406
19.3.1 Respect for Autonomy 407
19.3.2 Dignity 407
19.3.3 Informed Consent 408
19.3.4 Justice 409
19.4 Social Cohesion 410
19.4.1 Nonmaleficence (Avoiding Harm) 410
19.4.2 Beneficence 412
19.4.3 Social Solidarity, Inclusion and Exclusion 415
19.4.4 Sustainability 415
19.5 Conclusions 416

20 Auditing Privacy Impact Assessments: The Canadian Experience 419
Jennifer Stoddart
20.1 Introduction 419
20.2 Supporting the Performance of PIAs 421
20.2.1 PIAs Are Only as Good as the Processes That Support Them 422
20.2.2 Frameworks Lacking Critical Control Elements Are More Likely to Fail 425
20.3 Improving PIA Processes 429
20.3.1 PIAs Should Be Integrated with Other Risk Management Processes 430
20.3.2 PIA Requirements Need To Be Streamlined 430
20.4 Need for Strategic Privacy Impact Assessment 432
20.5 Enhancing Public Reporting Requirements to Improve PIAs 433
20.6 Conclusion: Evaluating the Effects of Our Audit 434
21 Privacy Impact Assessment: Optimising the Regulator’s Role
Blair Stewart

21.1 Introduction
21.2 Approach
21.3 Part A: Getting Started
21.4 Part B: Getting Through
21.5 Part C: Getting Results
21.6 Part D: Getting Value
21.7 Closing Comments

22 Findings and Recommendations
David Wright and Paul De Hert

22.1 PIA Policy Issues: Recommendations for a Better Framework on PIA
22.1.1 PIAs Should Be Conducted by Any Organisation Impacting Privacy
22.1.2 PIA Needs Champions, High Level Support and an Embedded Privacy Culture
22.1.3 A PIA Should Be “Signed Off” by a High-Level Official and Tied to Funding Submissions
22.1.4 Risk Management Should Be a Part of PIA, and PIA Should Be Part of Risk Management
22.1.5 Privacy Commissioners Should Play a Key Role in PIA
22.1.6 Prior Checking and PIA Should Be Complementary, But Their Mutual Relationship Needs More Study
22.1.7 Transparency Contributes to the Success of a PIA
22.1.8 Publish the Results of the PIA and Communicate with Stakeholders, Including the Public
22.1.9 Guard Against Conflicts of Interest
22.1.10 Ensure Third-Party Review and Audit of PIAs
22.1.11 Common Standards and Good Practice Need To Be Better Identified
22.1.12 Create a Central Registry of PIAs
22.1.13 Multi-agency and Transnational Projects Should Be Subject to PIA
22.1.14 Should PIAs Be Mandatory?

22.2 PIA Practice: Guidance for Individual PIAs
22.2.1 When Is a PIA Necessary?
22.2.2 Determine the Objectives, Scale and Scope of the PIA
22.2.3 Initiate a PIA Early, When It Is Possible to Influence Decision-Making
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.2.4 Who Should Initiate and Conduct the PIA?</td>
<td>465</td>
</tr>
<tr>
<td>22.2.5 Describe the Proposed Project and Map the Information Flows</td>
<td>466</td>
</tr>
<tr>
<td>22.2.6 Identify and Engage Stakeholders</td>
<td>466</td>
</tr>
<tr>
<td>22.2.7 A Compliance Check Is Only Part of a PIA</td>
<td>470</td>
</tr>
<tr>
<td>22.2.8 A PIA Should Address All Types of Privacy</td>
<td>471</td>
</tr>
<tr>
<td>22.2.9 ... and Other Values Too</td>
<td>472</td>
</tr>
<tr>
<td>22.2.10 With Stakeholders, Identify the Risks and Impacts of the Project</td>
<td>473</td>
</tr>
<tr>
<td>22.2.11 Questions</td>
<td>473</td>
</tr>
<tr>
<td>22.2.12 Identify Options (Controls) for Avoiding or Mitigating Negative Privacy Impacts</td>
<td>474</td>
</tr>
<tr>
<td>22.2.13 Justify the Business Case for the Residual Risk and Maintain a Risk Register</td>
<td>474</td>
</tr>
<tr>
<td>22.2.14 Review and Update the PIA as the Project Progresses</td>
<td>475</td>
</tr>
<tr>
<td>22.2.15 Prepare the PIA Report and Implement the Recommendations</td>
<td>476</td>
</tr>
<tr>
<td>22.2.16 Training and Raising Awareness</td>
<td>476</td>
</tr>
<tr>
<td>22.2.17 PIA Has Value – Get It!</td>
<td>477</td>
</tr>
<tr>
<td>22.3 Room for Improvement and Concluding Remarks</td>
<td>478</td>
</tr>
<tr>
<td>About the Authors</td>
<td>483</td>
</tr>
<tr>
<td>References</td>
<td>493</td>
</tr>
<tr>
<td>Index</td>
<td>519</td>
</tr>
</tbody>
</table>
Contributors

Kenneth A. Bamberger  University of California, Berkeley, CA 94720-7200, USA, kbamberger@law.berkeley.edu

Emilie Barrau  Commission Nationale de l’Informatique et des Libertés (CNIL), Paris, France, emilie.barrau@notaires.fr

Robin M. Bayley  Linden Consulting, Inc., Victoria, BC, Canada, rmbayley@shaw.ca

Colin J. Bennett  University of Victoria, Victoria, BC, Canada, cjb@uvic.ca

Laurent Beslay  European Data Protection Supervisor (EDPS), Brussels, Belgium, laurent.beslay@jrc.ec.europa.eu

Tobias Bräutigam  Nokia Corporation, Espoo, Finland, tobias.brautigam@nokia.com

Amanda Chandler  Vodafone Group, London, UK, amanda.chandler@vodafone.com

Andrew Charlesworth  Department of Computer Science, School of Law, Bristol University, Bristol, UK, A.J.Charlesworth@bristol.ac.uk

Roger Clarke  Xamax Consultancy Pty Ltd, Canberra, Australia, Roger.Clarke@xamax.com.au

Stephen Deadman  Vodafone Group, London, UK, stephen.deadman@vodafone.com

Paul De Hert  Vrije Universiteit Brussels (LSTS), Brussels, Belgium; Tilburg University (TILT), Tilburg, The Netherlands, paul.de.hert@vub.ac.be

John Edwards  Barrister and Solicitor, Wellington, NZ, jedwards@actrix.gen.nz

John Martín Ferris  Ferris & Associates, Inc., Washington, DC, jmferris@erols.com

Anne-Christine Lacoste  European Data Protection Supervisor (EDPS), Brussels, Belgium, Anne-Christine.Lacoste@edps.europa.eu
Gwendal Le Grand  Commission Nationale de l’Informatique et des Libertés (CNIL), Paris, France, glegrand@cnil.fr

Emilio Mordini  Centre for Science, Society and Citizenship (CSSC), Rome, Italy, emilio.mordini@cssc.eu

Deirdre K. Mulligan  School of Information, UC Berkeley, Berkeley, CA 94720-4600, USA, dkm@ischool.berkeley.edu

David Parker  Cranfield School of Management, Cranfield University, Cranfield, UK, david.parker@cranfield.ac.uk

Charles Raab  University of Edinburgh, Edinburgh, Scotland, c.d.raab@ed.ac.uk

Artemi Rallo Lombarte  Former Director of the Spanish Data Protection Agency (2007–2011) and Constitutional Law Professor at Universitat Jaume I, 12071 Castelló de la Plana, Spain, rallo@dpu.uji.es

Sarah Spiekermann  Vienna University of Economics and Business (WU Wien), Vienna, Austria, sspieker@wu.ac.at

Blair Stewart  Office of the Privacy Commissioner, Wellington, New Zealand, Blair.Stewart@privacy.org.nz

Jennifer Stoddart  Privacy Commissioner of Canada, Ottawa, ON, Canada, Lindsay.Scotton@priv.gc.ca

Florian Thoma  Siemens AG, Munich, Germany, Florian.Thoma@siemens.com

Adam Warren  Department of Geography, Loughborough University, Leicestershire, UK, A.P.Warren@lboro.ac.uk

Nigel Waters  Pacific Privacy Consulting, Nelson Bay, NSW, Australia, nigelwaters@pacificprivacy.com.au

David Wright  Trilateral Research & Consulting, London, UK, david.wright@trilateralresearch.com