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 Co-operation 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-Il 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, foreswearing 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.