Harvard Journal of Law & Technology
Volume 11, Number 3 Summer 1998

TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE

Edited by Philip E. Agre[1] & Marc Rotenberg.[2]
Cambridge, Mass.: MIT Press. 1997.
<http://mitpress.mit.edu>
Pp. 325. $25.00 (hard). ISBN 0-262-01162-X.

I. INTRODUCTION: THE MACHINE AS METAPHOR

In many respects, we no longer "use" technology so much as we "live" in it. It is relatively common to have business acquaintances who only know us through our contributions to e-mail discussions or through our voices on their voice mail. It is even more common to have relationships with other people that are marked by rare personal interactions and frequent electronic communications. Even our interactions with the physical world can be electronically mediated, with remote cameras or microphones acting as our "eyes and ears," and solenoids or motors acting as our "arms and legs."[3]

In personal interactions, it is common to control the identity we project by controlling what information we give out about ourselves. This is often what we mean when we talk about privacy; some topics are "too private" to discuss, and some stories about us are "too private" to retell.[4] In electronic interactions, our persona exists in a space that is impossible for us to monitor completely; it is difficult to keep track of which organizations and systems store data about us even when we have

---

1. Philip Agre is Assistant Professor of Communication, University of California, San Diego.

2. Marc Rotenberg is Director, Electronic Privacy Information Center, Washington, D.C.; Adjunct Professor, Georgetown University Law Center. Rotenberg also participated as a panelist at the *Harvard Journal of Law & Technology*'s 1997 Symposium on Crime and Technology.

3. A product called iCam provides a striking example of the power electronic media give for projecting our presence into other physical spaces. *See* Perceptual Robotics, Inc. (visited May 7, 1998) <http://www.perceptualrobotics.com>.

4. Admittedly, many writers have attempted to define privacy, and such efforts have not yet generated consensus. Justice Louis Brandeis called privacy "the right to be let alone." Olmstead v. United States, 277 U.S. 438, 478 (1928) (dissenting opinion). One of the contributors to *Technology and Privacy*, Rohan Samarajiva, argues that "the right to be let alone" is quixotically atomistic and impractical. He suggests as an alternative "the capability to explicitly or implicitly negotiate boundary conditions of social relations" (p. 283) (footnote omitted).

complete knowledge of where such data might reside — and we seldom have such complete knowledge. *Technology and Privacy: The New Landscape* attempts to address data privacy topics in light of the new role that electronic environments play in shaping our individual identities.

II. THE AUTHORS

Technology and Privacy: The New Landscape is an edited series of papers. In the introduction, Philip Agre suggests that readers should view it as an integrated work whose chapters merely happen to be written by different authors. Although the book does not read as seamlessly as that, the various authors clearly deal with a cluster of common themes. They also make frequent reference to each other's arguments and previous works, which enhances the reader's ability to understand the ways in which the various analyses relate to the overall discussion.

The book's mixture of practitioner knowledge and academic literature enhances its values. Of the eleven authors, only four are listed as having academic appointments (pp. 311–12).[5] The majority of the rest hold posts at various technology research or privacy advocacy institutions. Yet, the book gives up little, if anything, in academic rigor: the papers are rife with references to both the seminal and the obscure, and most of the authors are conscientious about supporting their assertions.

III. FEATURES OF THE NEW LANDSCAPE

A. International Scope

One strength of the book is that many of the authors consider the cross-border effects of privacy policies and communication technologies. So many writers have observed that the international nature of the Internet "changes everything" that it is almost an empty bromide. The authors here do not dispute the importance of the Internet; indeed, Agre's "Introduction" acknowledges that the Internet and other forms of computer networking contributed to the creation of "the new landscape" (pp. 3–4). However, their analyses suggest that the international and comparative law aspects of privacy policy are more influenced by shifts

5. A fifth author, David Flaherty, still holds a tenured professorial position despite his current post as Privacy Commissioner for British Columbia.

in social forces than by shifts in technology. The Internet becomes one driver behind changes in social reality, but it is not the only one and not the most fruitful locus of analysis.

In "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" Colin Bennett's[6] thesis is that privacy policies, at least in the European Union ("EU"), are converging toward a common set of provisions (p. 106). He suggests that cross-border networks provide the necessary condition for this convergence, but that the process is not spontaneous. Rather, he attributes the past similarity in policies to the frequent contact and close, informal relationships between policymakers in different countries (p. 103). In the new landscape, however, growth in cross-border data flows has made it a necessity, rather than a luxury, for policymakers to remain in close contact with one another. Because each policymaker's constituency now depends on such data flows, so does each policymaker's public support. This forms a lever by which nations can influence each other's privacy laws; as with trade in goods and services, trade in data can be subject to unilateral embargo (p. 109).

Provision for such an embargo exists within the EU's 1995 Directive on the Protection of Personal Data and on the Free Movement of Such Data (pp. 105–06).[7] Under the Directive, any nation that does not offer "adequate" data protection cannot receive data from EU nations. Canada has recently revised its data protection statutes; according to Bennett, Canada was responding specifically to the threat posed by the EU Directive (p. 111). This provides both example and proof that nations can use "penetrative" data protection policies as a mechanism for influencing each other's law (p. 111).

While Bennett explains the political effects of the EU Directive, Viktor Mayer-Schönberger[8] looks at its conceptual underpinnings. Like Bennett, Mayer-Schönberger focuses on the social construction of data privacy, with technology as a part of the dynamic but not the prime mover. He groups the policies of Western nations into three "generations," all of which failed in some key aspect. Within this framework, the 1995 EU Directive represents the vanguard of a more effective fourth generation. The countries that adopted first-generation

---

6. Colin Bennett is Associate Professor of Political Science, University of Victoria, Victoria, British Columbia, Canada.

7. European Union, Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31.

8. Viktor Mayer-Schönberger is associated with the Austrian Institute for Law & Policy and with the University of Vienna Law School, Vienna, Austria.

privacy laws created executive-branch bureaucracies (p. 224). These bureaus had a mandate to control data processing in both public and private organizations. To Mayer-Schönberger, this approach was flawed because the laws were rooted in certain static notions about technology. They aimed to regulate large, discrete "data banks" and "data files" (p. 224); once these technologies were replaced by smaller, more numerous, networked data-gathering mechanisms, the policies no longer gave clear direction (p. 225). The second generation of policy moved away from specific technical concepts toward individualistic privacy rights (p. 226); the third wave improved on the second by adding individual participation as a democratic value (p. 229). Nevertheless, both generations were flawed because individuals contracted out of their rights so frequently (pp. 229–32). Mayer-Schönberger contends that this act usually appeared voluntary, but was actually rooted in the power imbalance between individuals and data-accumulating organizations (p. 232). For example, one does not give one's social security number to the bank because one wants to, but because one cannot realistically live without a checking account.

Mayer-Schönberger suggests that policies like the 1995 EU Directive combine the previous approaches to good effect (pp. 232–33). The concept of privacy as a fundamental right remains, and the regulatory bureaucracy exists to prevent contractual arrangements which undermine those fundamental rights. In his essay "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," Simon Davies[9] argues that this approach is not just laudable, but crucial. In possibly the most trenchant article of the book, he argues that privacy has been transformed from a right to a commodity (pp. 144, 160–61). While Mayer-Schönberger credits pseudo-voluntary contractual arrangements with causing the failure of second- and third-generation privacy policies, Davies examines the conceptual shift that allows such a system to operate (pp. 159–60). The international effect of this conceptual shift is that privacy can "flow" across borders as if it were a good; corporations in one nation can contract with citizens of another to use the citizens' personal data in privacy-threatening ways. Applying Davies' analysis (pp. 160-61) indicates that it would be difficult to dismantle such a market once it was entrenched. Thus, while the 1995 EU Directive quite properly formulates data privacy as a non-fungible right, it might not be enough to reclaim the data privacy which citizens have already surrendered.

---

9. Simon Davies is Director General, Privacy International, Washington, D.C.

B. New Threats

The international analyses define the extent of the new landscape; the other authors examine its features. Here, the overall tone of the book is not encouraging; most of the authors agree that individuals face increasing barriers to "being left alone." Policymakers might use law to combat these threats with relative ease if it were clear which actors should be restrained. The new landscape, however, is marked by threats from both public and private actors — many of whom are encouraged by a complacent public.

1. Public Sector Threats

Cheaper computing power and innovative new surveillance technologies have given governments the means to collect and analyze greater amounts of personal information. Welfare state and crime-prevention imperatives have given governments the will. The book is rife with examples of this, including matching of database records across different government agencies (pp. 198–99), closed-circuit television to enable constant surveillance of high-crime areas (pp. 150–52), electronic toll facilities with the ability to record vehicle movements (p. 160), and the U.S. government's proposal to allow government "escrow" of cryptography keys (pp. 258–68). These illustrations are interesting, to be sure, but perhaps cover overly-familiar ground. The authors make their greatest contribution when they discuss the conceptual and structural roots that make these new intrusions possible.

Several authors mention that the very framework of the debate puts privacy advocates at a disadvantage. Simon Davies notes: "Whether through design or osmosis, information users employ a common set of terms that are hostile to privacy. In the parlance of banks, police, and government agencies, privacy is a value rather than a right" (p. 152). In public discourse, "values" don't carry the weight that "rights" do, so it becomes more difficult to defend privacy relative to public security, public health, or even efficiency.[10] This difficulty often proves fatal. One fascinating statement comes from David Flaherty,[11] a former academic who now holds a post in the government of British Columbia:

---

10. Protection from crime is a particularly strong example. One stark example of public safety trumping individual privacy is North Carolina's Web-accessible database of the names, addresses, and partial criminal records of convicted sex offenders.

11. David Flaherty is Information and Privacy Commissioner for British Columbia, Victoria, British Columbia, Canada.

> In classic liberal fashion, I emphasized in my book[12] the need to balance privacy against competing values and legitimate governmental purposes. My efforts . . . strike me as naive in retrospect: the striking of balance within government is so much against the privacy interests of individuals that it is a wonder we have any privacy left . . . . What is good for government is always thought by those in government to be good for the public at large (p. 173).[13]

2. Private Sector Threats

The earliest discussions of technology and privacy focused on the specter of Orwellian government control over daily life.[14] In the new landscape, private actors collect much more personal information than they did even five years ago, and the data is stored in decentralized collections that are harder to control.

Rohan Samarajiva[15] discusses what he calls "the surveillance imperative," which drives businesses to collect ever greater quantities of data on each customer (pp. 278–81). Competition has driven prices down to the point where producers need to find other ways to differentiate themselves and retain customers. Most frequently, companies will tightly focus their marketing efforts on a very narrow, but lucrative, demographic group. They may then offer value-added services that require an ongoing relationship with the consumer. For example, cars come with warranties that require the owner to return to the dealer; frequent-flyer programs bind the customer to a single airline. The most advanced producers may also implement agile manufacturing and other processes that allow them to tailor their products to a demographic of one. All of these processes require a company to

---

12. DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989).

13. Compared with Davies' strident tone, Flaherty's observations are all the more jarring because he was previously a moderate, but four years "inside" government have brought him closer to Davies' extreme viewpoint.

14. *See, e.g.*, MYRON BRENTON, THE PRIVACY INVADERS (1964); MORRIS L. ERNST & ALAN U. SCHWARTZ, PRIVACY: THE RIGHT TO BE LET ALONE (1962).

15. Rohan Samarajiva is Associate Professor of Communication, School of Journalism and Communication, Ohio State University, Columbus, Ohio. Dr. Samarajiva is on leave from the university until the middle of 1999, and is currently serving as the Director General of Telecommunications, Sri Lanka. *See* Ohio State University School of Journalism and Communication, *Rohan Samarajiva* (visited May 20, 1998) <http://communication.sbs.ohio-state.edu/sjc/faculties/samarajiva.html>.

accumulate finely-grained data about its potential customers, their preferences, and their habits.[16]

Furthermore, consumers have substantial incentive to participate in the data-gathering scheme. Because the payoff of a frequent-flyer program is so substantial, we will willingly tell airlines our addresses and credit card numbers, then let them accumulate information on our travels. Samarajiva argues that interactive media services create the greatest incentive for the customer to reveal deep information about interests (p. 289). When we customize our news feeds or order books from the World Wide Web, we give marketers remarkably detailed information on what interests us and what we might know about the world.

The authors contend that these practices are problematic, even when we do hand over information voluntarily, because they shift privacy from a right to a commodity and reduce the social expectation of privacy. Davies laments that "commodification is inimical to privacy," because "it implies that a few 'fundamentalists' will force a rise in the production cost of an item" if they request greater privacy in their economic transactions (p. 161). Other authors also discuss the illusion of voluntariness. Where all producers in a given market require an intrusive quantity of personal data, as with banks, "the data subject is asked to choose between giving consent and losing advantages, privileges, rights, or benefits, some of which may be essential to the subject in a given situation" (p. 128). Davies takes this analysis a step further, noting that the structure of data-collection systems itself feeds back into society's conception of what is acceptable behavior: "There is some anecdotal evidence that this pseudo-voluntary approach may have the effect of neutralizing privacy concerns. It may be widely viewed that those who do not 'volunteer' bring problems upon themselves" (p. 159).

---

16. People familiar with information technology will recognize that these business practices are enabled by cheap storage, fast relational databases, and the rise of "data warehousing" technology. Although Samarajiva contends that these practices are fairly recent, driven by new economic forces that create an imperative to go beyond price and quality (pp. 278–79), he does not spend time examining these forces. Some may, therefore, disagree that the economic imperative is new and contend instead that technological change has enabled companies to act on an urge that was always there. This is perhaps a debate for the economic historians.

C. New Protections

Despite the new difficulties that privacy advocates face, the authors also describe new tools for privacy protection. The book presents a two-pronged approach to the problem: solutions can be part of the technology itself, or can be implemented in the policies surrounding the social use of the technology. Several of the authors grapple with the question of when one method is more effective or appropriate than the other. They also discuss what such technologies and policies might look like once implemented.

1. Technology Protections

Several of the authors discuss privacy-enhancing technologies ("PETs"), a general category which includes all technologies that might allow individuals to control the boundaries of their interactions with others. In "Privacy-Enhancing Technologies: Typology, Critique, Vision," Herbert Burkert[17] sets the conceptual frame by describing the various ways that system architects can build privacy into their designs. In a given transaction, the system can "keep secrets" about the subject, the transactional object, the action performed, or the system itself (pp. 125–28). These four loci of privacy interact to either increase or decrease the overall level of privacy that a system offers. A web browser, for example, may protect the subject by not revealing information about the name or identity of the person using it. If, however, it reveals information about its host machine, and the machine reveals the identity of its user, then the subject security is lost because the designers did not build in privacy at the system level. He stresses that many PETs protect privacy because of the way they are applied rather than because of any inherent qualities. The new landscape, however, at least allows us to apply more technologies in a privacy-enhancing way.

David Phillips[18] extends this analysis, using cryptography as his example. The explanation of public-key cryptography[19] in "Cryptography, Secrets, and the Structuring of Trust" forms the prelude

---

17. Herbert Burkert is Senior Researcher, German National Research Center for Information Technology, St. Augustin, Germany, and Assistant Professor, University of St. Gallen, Switzerland.

18. David Phillips is a Ph.D. candidate, Annenberg School for Communication, University of Pennsylvania, Philadelphia, Pennsylvania.

19. Although certainly not the first attempt to explain public-key cryptography to technology laypeople, Phillips' primer is one of the most lucid.

to Phillips' main point, which is a new conceptual framework for comparing PETs. His framework looks to the distribution of "trust." He defines trust as a situation in which an agent performs a task on behalf of a principal who lacks the resources to verify the quality of the agent's work (pp. 244, 272). PETs are generally characterized by their power to redistribute "trust," so that the principal can use multiple agents, each of which need be only partially trusted. Third-party escrow systems, for example, involve multiple parties, none of which can unilaterally breach the privacy of the transaction (pp. 259, 263).

2. Policy Protections

Lawyers will be particularly interested in the book's policy prescriptions. Overall, the suggestion is that PETs are not, by themselves, the advance that will ultimately protect privacy. Rather, institutional policies must foster attention to privacy issues. The authors' suggestions are tentative and descriptive, rather than comprehensive and concrete. Successful policies, they say, will include a strong, vigilant party responsible for monitoring privacy violations. Such policies would also focus on individuals rather than data or processes.

Mayer-Schönberger, in his comparative analysis of European privacy laws, notes that countries have been most successful where they have created executive bureaus responsible for privacy protection (pp. 228, 234). In "Does Privacy Law Work?," Robert Gellman[20] examines the history of U.S. privacy law and concludes that the absence of such a bureau has deprived the law of force (pp. 201, 213). The most interesting voice in this debate is David Flaherty's, since he is the head of such an enforcement bureau. He warns that such an agency is effective in proportion to its independence and authority. He acknowledges that having a privacy advocate on the "inside" carries the "risk of [the advocate] being co-opted by a desire to go along and get along" with other arms of the government (p. 180). Because his office has no power to impose criminal sanctions on officials who do not comply, his "concern for independence is counterbalanced by the desire to build an effective network in government circles to facilitate the mediatory role of our office in settling most of the requests for reviews of access decisions that come to us" (p. 180).

The book also suggests that data-protection policies are only a portion of the solution. A holistic, person-centered approach to privacy

---

20. Robert Gellman is a privacy and information policy consultant in Washington, D.C.

is necessary. Davies notes that the European emphasis on "data and not people" has allowed virtually unlimited accumulation of information provided that the act of accumulation took place according to fair procedures (p. 156). Flaherty notes that in many situations where the individual has the choice to surrender information or not, data-accumulators will structure transactions so as to obscure this choice. The Canadian national pharmacy database has the technical capability to protect each citizen's record with a password supplied by that citizen, but the person behind the counter will seldom, if ever, suggest that a customer make this choice (p. 188). Colin Bennett suggests that the speed of technological change makes the importance of personal boundaries the only constant. In order to maintain the law's adaptability to new situations, he suggests that privacy policies be structured as standards rather than rules (p. 104).

IV. WHERE DO WE GO FROM HERE?

Technology and Privacy: The New Landscape gives the reader a good overview of emerging privacy problems. Solutions are somewhat harder to come by; this reflects, I think, the newness and difficulty of the problems. This book presents some interesting analytical tools that will help legal thinkers invent solutions. One of the biggest stumbling blocks is that individuals' interests are not self-consistent. We cannot assume a stark conflict between the individual interest in privacy protection and the institutional interest in data collection. Individuals cannot construct identity without (selectively) revealing information about themselves. These revelations are often neither completely voluntary nor completely involuntary, but lie on a spectrum of greater or lesser risk.

The problem is to determine what level of risk is acceptable, and whether individuals should always make their own calculations given the power environment in which they operate. Several of the authors make reference to the economics of information. As information becomes more important and more fungible, perhaps it will take on more characteristics of property, which would give us a clearer blueprint for creating privacy-protection policy. If information is as important as money, perhaps policymakers will find it compelling to analogize data-accumulators to money-accumulators — and place controls on the formers' activities much as we now place controls on banks.

Antoun Nabhan