INTRODUCTION

Securing Privacy in the Internet Age

Anupam Chander

Anupam Chander is professor of law, University of California, Davis and visiting professor, Yale Law School. *The author is grateful to Maren Ahnberg, Joseph Boufadel, Christopher Camp, Audrey Goodwater, Kathryn Lee, and Ryan Walters for excellent research assistance, and to coeditors Lauren Gelman and Margaret Jane Radin for the vision that made this book possible. The author also thanks Deans Rex Perschbacher and Kevin Johnson for their support.*

A child born in 2008 will have many of the major and minor events of her life recorded in digital form. Her performance as a rabbit in a primary school play will be filmed on digital video cameras. Her school papers will be submitted and the grades recorded on digital media. The forms she fills out during her life will often be stored electronically. Doctors will dictate or type notes from her visits on computers. Radiologists in distant offices will interpret many of the tests ordered by her doctors. Computers might even sequence her genome and test it for disease susceptibility. Her running shoes might record her daily local running regimen, while her mobile phone provider records her travels across town and the identities of her friends. Security cameras will record her activities in public and private spaces. She will share the photos from her vacations online. Her parody of a favorite professor in a law school skit may find its way onto YouTube. Her emails and instant messages to friends may linger on computer servers. She will do much of her banking and buying online. This twenty-first-century child will face a lifetime's worth of personal events that will be catalogued, compiled, and digested by remote computers. In a

networked, digitized world, as Lawrence Lessig presciently warned, "Your life becomes an ever-increasing record."[1]

The goal of this volume is to reduce the risks that this information about this child of the Internet Age will be misused. Law can help limit such risks—by incentivizing more limited collection of information, more robust security for stored information, and the purging of information over time.

Privacy becomes difficult to sustain in a world characterized by the ready flow of information. The threat to privacy cannot be trivialized as an irrational fear of unwanted electronic solicitations. Rather it takes more sinister form in identity theft, fraud, stalking, increased expenditures for security, hesitations about otherwise desirable marketplace transactions, spying on people, intrusions into intimacy, difficulty in obtaining employment or insurance, and increased conformity to social norms. To put a monetary figure on just one of these harms, consider a report for the Federal Trade Commission, which estimates that consumers lost $5 billion in 2003 due to identity theft.[2] Making our systems for securing private information more robust becomes an economic imperative.

As recent debacles involving financial information collectors such as ChoicePoint and MasterCard reveal, protecting privacy turns centrally on something as mundane as securing computer databases and setting the terms for access. Yet privacy and security typically are considered in isolation, with academic attention focused on granting individuals rights against corporations that seek to exploit information about them, and corporate attention focused on protecting corporate information in the face of determined hackers. Advocates of privacy have sought to protect individuals from snooping corporations, while advocates of security have sought to protect corporations from snooping individuals. *Securing Privacy in the Internet Age*, growing out of a major symposium at the Stanford Law School, brings the two goals together. It gathers many of the world's leading academics, litigators, and public policy advocates, putting their heads together in a common endeavor to enhance privacy security. The traditional bugbear of privacy has been the government, which can take on the role of the Orwellian Big Brother, monitoring any deviations from publicly approved behavior—but the principal focus of the authors in this collection is the fraternity of Little Brothers—the corporations and individuals who seek to profit from gathering personal information about others.

In the main, the experts we have drawn together agree that the privacy of individuals is unduly compromised by the burgeoning digital databases

pooling personally identifiable information. Although this problem has been anticipated since the dawn of the computer age, the Internet Age heightens the risks because of a number of factors:

1. Databases can be shared readily over electronic networks
2. The volume and quality of activities engaged in online increase the types of activity susceptible to easy cataloging
3. The Internet increases the vulnerability of databases to remote hackers

Most of the authors find the legal infrastructure inadequate to secure privacy: in Daniel Solove's indictment, "The problem is caused in significant part by the law, which has allowed the construction and use of digital dossiers without adequately regulating the practices by which companies keep them secure."[3]

In 2007—after seemingly weekly disclosures of large-scale breaches of privacy security covering a wide array of data collection services, from consumer service agencies such as ChoicePoint, Lexis-Nexis, MasterCard, the Veteran's Administration, and even the local doctor's office, the existence of a problem seems hard to deny.

CURRENT LAW ON SECURING PRIVACY

The law securing privacy in the United States is cobbled together from a disparate array of federal statutes, a few state laws, and common law. There is no overarching framework, but rather episodic privacy protections for limited domains and in certain circumstances. For the most part, existing federal statutes applicable to privacy predate the Internet Age. Statutes such as the Right to Financial Privacy Act of 1978 and the Electronic Communications Privacy Act of 1986 were designed principally to combat governmental intrusions into privacy. Attempts to deploy these statutes against the collection of personal information have generally tripped over the fact that they permit either party in a communication to divulge that communication to others, thus permitting a Website to authorize others to collect information given to that Website by Web surfers.

Congress has enacted *sui generis* rules for certain special cases. The Gramm-Leach-Bliley Act (GLB), for example, imposes special protections for information gathered by financial institutions. Similarly, the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare service providers to take various steps to safeguard privacy, including the

ubiquitous privacy notices whose receipt you are asked to certify with every medical appointment. Although HIPAA's privacy requirements have been visibly in place for years, HIPAA's security requirements became effective only in 2005. HIPAA may have a broader reach than may at first be apparent. Its security rule covers not just healthcare providers but also their "business associates," including potentially everything from transcription services to law firms. The principal World Wide Web-era innovation is the Children's Online Privacy Protection Act (COPPA), which requires Websites to obtain parental permission before gathering personal information online from children under thirteen.

Given the lacunae in federal law, which has preferred narrowly applicable privacy rules, California recently stepped into the breach with its own Online Privacy Protection Act (Cal OPPA). That statute, which requires companies to post privacy notices, applies not just to California companies but to any company, presumably worldwide, that gathers personal information online from Californians. Another California statute, California Civil Code § 1798.82, requires companies to disclose breaches of security with respect to personal information of any resident of California if this personal information includes the person's name and any of the following (1) social security number, (2) driver's license number, or (3) financial account access information. Unlike many of their federal counterparts, both California statutes grant private rights of action, § 1798.82 explicitly and Cal OPPA via California's unfair competition law. Given the breadth of the California legislation and the importance of the California market to the national economy, California privacy law may become the de facto national standard. Indeed, in the recent ChoicePoint debacle, ChoicePoint initially planned to reveal the breach of its database only to California residents, who were covered by § 1798.82. After complaints from residents across the country, the company rapidly decided that it could not treat Californians as a privileged class, and extended its disclosure to encompass all Americans.

But to understand American law securing privacy, it is not sufficient to look at federal or state law. Brussels has proved itself an important source of norms securing privacy, imposing broad obligations on American data collectors with facilities in Europe or American entities processing European data. Asian, Latin American, and African states may not be far behind in imposing demands on foreign collectors of information regarding their citizens.

SECURITY AND PRIVACY VALUES

Despite their close link in practice, security and privacy are differing values, with separate motivation. Security seems the less contested value. Few people argue for less security, though many question how much of society's resources should be devoted to it and how best security is to be attained. But security holds pitfalls as well. Robust encryption can defeat government surveillance of criminal as well as legitimate activity. Excessive focus on security can dampen risk-taking endeavors, threatening innovation and increasing costs.

Privacy is a complicated value. Privacy helps restrain the world from prying intrusions into personal affairs, but at the same time immunizes private realms from the demands of justice. Feminists in particular have sought to bring the light of law into the private realm, exposing the oppression in domestic spheres—while at the same time seeking to preserve a realm of privacy with respect to a woman's right to choose to have a child. Gay rights proponents, confronted with a sometimes hostile majority population, often prefer fewer infringements on privacy. Libertarians might also prefer fewer infringements on privacy, yet are generally not inclined to protect that privacy through the expansion of the law. Not only do they distrust the state, they worry that one person's ability to protect privacy might intrude on another's right to speak about that person. Perhaps the strongest lobby against increased privacy protection is business, which prefers as much information about potential customers as possible—that is, knowledge about who wants what where. Databases of consumer information are increasingly a principal corporate asset; privacy protections would limit the creation and deployment of such databases, and thereby erode their value.

Privacy and security are not the only values in designing an information regime. There are many other values, including innovation; efficient production and distribution; access to cheaper goods and services, especially for the poor; simplicity; functionality; and free speech. Society accordingly must approach privacy security with care—protecting against the intrusions of a database society with ever-more powerful search algorithms and ever-more sophisticated thieves, while ensuring robust commerce, innovation, and wide distribution of society's goods.

Privacy and security are linked, but they are not identical. An institution that gathers information can breach an individual's privacy even without a security lapse simply by giving that information away voluntarily. That is, privacy breaches do not arise solely from security lapses. Data collectors

transfer private information not only unintentionally to hackers but also intentionally to affiliated companies.

SECURING PRIVACY BREACHES AND CONSENT

There are four types of actions that might constitute a breach of privacy security:

1. *Data Gathering*: The collection and maintenance of personal information contrary to the wishes of the data subjects
2. *Data Misuse*: The use of personal information in ways contrary to the wishes of the data subjects
3. *Data Sharing*: The voluntary disclosure of personal information by data collectors to third parties in ways contrary to the wishes of the data subjects
4. *Security Breach*: The unauthorized accessing of personal information held by data collectors

The absence of consent plays a central role in all of these breaches, but consent here is a fraught concept. Does the availability of the right to opt out of information gathering establish consent for data gathering when the right is not exercised? Lilian Edwards observes, "Consent, a seemingly simple idea, is much less clear when faced in terms of opt-in and opt-out, pre-ticked tick boxes, half-buried links to privacy policies, and incomprehensible legal language."[4] The Children's Online Privacy Protection Act requires "verifiable parental consent," thus requiring affirmative actions on the part of a parent more akin to opt-in to data collection. Similarly, the European Data Protection Directive requires consent to be "unambiguous." The "safe harbor" under this directive for United States companies, however, permits consent to be expressed through "opt-out" (except for very sensitive information, such as that about race, sex, and religion). Most businesses strongly prefer opt-out systems, recognizing that few consumers will take the trouble to flip the privacy setting to deny data collection. Raymond Nimmer believes that this suggests consumer indifference to the exploitation of personal information. But it is possible that, for many, the failure to opt out of data collection reflects not indifference to that collection but rather a lack of awareness. It is also possible that consumers often find the process of opting out too cumbersome to be worthwhile. Overall, it seems hard to conclude that opt-out systems reflect consumer choice adequately, let alone "unambiguously," as required by the European Data Protection Directive.

Notice and consent seem inadequate to establish privacy security. The privacy notices given with every hospital visit pursuant to HIPAA are destined, after the most cursory of glances, for the trashcan. That is not to say that notice is unhelpful. California's simple requirement that breaches of privacy security must be notified to California residents led to the disclosure of the large-scale ChoicePoint intrusion, an intrusion that would have likely passed without notice in the absence of the California law.

ESTABLISHING PRIVACY SECURITY

Security is a process, not a product.[5] Security consists of an ongoing process of identifying threats and vulnerabilities and taking appropriate responses. A firewall, a password, and a lock on the door to the computer server room are not a one-size-fits-all solution. The process of establishing privacy security must be multidimensional, recognizing that privacy security will thrive only through careful attention to an array of components, including the following:

1. What information can be collected from the individual
2. How information can be used by the data collector
3. With whom that information may be shared by the data collector
4. How securely the information, once collected, is maintained
5. The process of authenticating identity

Because no single corporation controls all of these components, privacy security is best viewed from the societal level. This is simply another facet of the economics of information. There are too many externalities in the choices required in information regimes—for example, what kind of authentication to use, what kind of data to gather, and for what purposes information may be used—to expect the price system to ensure an optimal level of privacy security. The marketplace is also unequipped to address the methods by which privacy security is undermined. The harms that arise are often difficult to trace to the source of the breach.

WHAT IS TO BE DONE

Although the experts agree that a problem exists, they do not agree on what must be done. The difference of opinion is to be expected—the writers include, for example, on one side, a lawyer pressing full-time for increased federal regulation of privacy and security (Chris Hoofnagle) and, on the other side, a legal academic who has a more skeptical view of regulation (Raymond Nimmer).

Three broad approaches are offered:

1. *Laissez-faire/Market*: Some experts favor a laissez-faire approach, with the market dictating a solution
2. *Common law*: Others seek to regulate via the common law, offering more vigorous or novel uses of existing law to discipline privacy security abuses
3. *Statutory*: Many contributors would like to see additional regulation of entities that gather and process data

Many authors have faith that the common law can improve privacy and security. Daniel Solove recommends the imposition of fiduciary duties on data collectors. Jennifer Chandler offers the possibility of a product-liability-type of claim against the makers of "unreasonably insecure software." Marcy Peek proposes the use of claims for restitution to make data collectors pay for their unjust enrichment from personal information. But there are many impediments to such suits. Privacy infractions often represent the kind of losses that traditional legal claims proved inadequate to handle. They often involve small harms to individuals, worthwhile to pursue in judicial setting only through the aggregation of multiple claims. Class actions would thus seem like the ideal vehicle for vindicating wrongs and disciplining those who are careless about protecting others' privacy. But Jonathan Sobel, Karen Petrulakis, and Denelle Dixon-Thayer, reporting from the front lines, tell us that class action lawyers typically need something more: a statutory setting of damages and attorneys' fees to avoid individualized determination of harm, which proves difficult both at the class certification stage and at the remedy stage. Ian Ballon notes that certification of class actions may be impossible when users enter into click-through agreements that send disputes to arbitration, a forum that is inhospitable to class relief. Sobel and his coauthors conclude that private litigation has thus far "failed" in the absence of federal statutes authorizing specified damages and attorneys' fees.

The price of privacy security should not be a loss of innovation or inordinate constraints on business. As Susan Brenner argues, too heavy a regulatory hand might stifle business. If grocers, clothing stores, and the like could not share information with third parties without consent, such companies might find it difficult to conduct routine back office transactions such as customer and inventory management and credit processing, processes that are often outsourced. The concern about hampering technology through excessive regulation is perhaps most clear with radio frequency identification tags

(RFIDs), which allow products to identify themselves wirelessly to nearby readers. In Japan, schools are planting RFIDs in children's backpacks for additional safety, though some worry about the misuse of surveillance data. Want to know more about what you eat? RFID technology permits Japanese steak consumers to determine, for example, that a source cow was born on January 5, 2001; supervised by Toshiyuki Arimura of Miyazaki prefecture; and shipped to Marusho Foods on February 13, 2003, where it was processed on the next day.[6]

But perhaps RFIDs may be safer for cattle than for people. For example, *Wired* magazine advised its American readers to bring a hammer down on the RFID chip implanted in the latest passports.[7]

OUTLINE OF THE BOOK

Securing Privacy in the Internet Age begins with a review of the existing landscape of security and privacy law.

Reviewing Existing Security and Privacy Law

Thomas J. Smedinghoff offers an overview of the obligations of businesses to provide information security. He suggests that a panoply of laws, both statutory and common law, result in a cognizable legal standard for information security. He finds a consistency between the various rules that have developed—from those protecting the privacy of children to those protecting health or financial information. He argues that security measures must be calibrated to the particular context of risk and threat. He delineates the questions that a corporation's executives, lawyers, and compliance officers should ask in designing security systems. Smedinghoff mentions the special concerns that arise when a company outsources certain of its business processes. Outsourcing, of course, has become almost as politically controversial as it is endemic to modern business practice. He observes that "you can outsource the work, but not the responsibility."

Ian C. Ballon reviews three of the major statutes that impose security obligations on companies:

1. The Gramm-Leach-Bliley Act, which covers customer information held by financial institutions
2. The Health Insurance Portability and Accountability Act, which covers individual health information held by health plans, healthcare clearinghouses, and most healthcare providers

3. California's security reporting statute, California Civil Code § 1798.82, which requires any company doing business in California to disclose breaches of databases holding personal information

Neither GLB nor HIPAA provides a private cause of action, and thus enforcement of these obligations is limited to the federal government. The principal federal agency enforcing security obligations is the Federal Trade Commission, which has settled charges of insecure practices with respect to consumer information against such prominent corporations as Eli Lilly & Co., Guess, and even Microsoft.

Jonathan K. Sobel, Karen J. Petrulakis, and Denelle M. Dixon-Thayer review the existing landscape and conclude that privacy security law in large part consists of the contracts created between data collectors and data subjects, often through privacy policies posted on Websites. If Sobel and his coauthors are correct, then the question is whether consumers will value their privacy sufficiently to ensure it via contract or whether they will cede it readily for small favors or conveniences. This is ultimately a question of market alienability—should personal information be readily available for sale if the individual is willing to sell it? Complicating the discussion is that market inalienability operates at two levels at least—alienation from the data subject to the data collector, and alienation from the data collector to third persons, such as credit services.

So what do these privacy contracts say? Andrea M. Matwyshyn studies the evolution of contracts offered by the Websites of seventy-five publicly traded companies. She compares the terms of use and privacy policies at two points in time—the late 1990s and March 2004. Although terms of use and privacy policies were not common in the late 1990s, she finds that they have become increasingly common with time. She finds that companies have increased the detail in their privacy policies, while seeking to transfer risk to users through terms-of-use policies. She sees the results as distressing, and suggests that consumers seek technological tools to protect their privacy.

If we want to learn privacy security law, we must look not just at Washington, D.C., or Sacramento (or even the "code" produced in Redmond, Washington, or Silicon Valley), but also Brussels. The European Union, Timothy Wu tells us, has enacted the world's most stringent and broad data privacy law. Will this law become de facto our own? Will the world's strictest law govern, as multinational enterprises bring their operations in line with it, or will the world's weakest law govern, as corporations relocate to offer their services

from unregulated jurisdictions? Wu suggests that the answer will differ, depending on the type of regulatory problem at issue.

Promoting Privacy and Security Through the Common Law

Daniel J. Solove observes that the abuse of personal information arises out of leaks of information, which themselves arise out of insecure computer systems. He argues that the law has concentrated its energies on the abuses that actually emerge, where it might better concentrate on the underlying insecurity that leads indirectly to the abuses. He suggests two legal theories that might motivate better security: (1) a fiduciary duty imposed on data collectors to keep information private and (2) tort claims for data insecurity leading to either emotional distress or increased risk of future harm. Solove recognizes that the damages in such anticipatory cases are likely to be small, and suggests that aggregation of multiple small claims might still lead to an effective private attorney general. Solove also promotes an invigorated role for the Federal Trade Commission, which has on occasion sought to improve privacy and security practices in, for example, Microsoft's Passport system and Guess.com Inc.'s customer information database.

Marcy E. Peek focuses on what she calls "shadow offenders"—companies that traffic in personal data without any direct commercial or contractual relationship with the data subject. She turns to the common law remedy of restitution as a method to discipline such third-party actors, who are not by definition reached by contractual claims. She argues that restitution can provide a remedy when a plaintiff's damages are hard to measure but a defendant's profits are clear. The broad reach of the restitution claim will prove attractive to privacy advocates but alarming to corporations, which are accustomed to benefiting from information gathered from disparate sources without necessarily compensating all data subjects.

Jennifer A. Chandler analogizes what she calls "unreasonably insecure software" to a defective product, subject therefore to a strict liability claim in tort. She argues that the market in software does not represent an ideal security-cost trade-off because of market failure—due to heavy concentration in production; information failures, especially on the part of the ordinary software purchaser; and negative externalities of insecurity. She rejects the possibility of direct regulation of software standards to guarantee security because regulation (1) is slow, (2) is subject to industry capture, and (3) may impose a one-size-fits-all approach rather than a more tailored security standard.

Chandler explores the possibility of bringing a claim for negligence against the developers of unreasonably insecure software. She recognizes doctrinal hurdles that a purchaser of software would face in such a novel products liability case. She suggests that a particular type of plaintiff might have better success in bringing such a suit. This is the victim of a distributed denial of service (DDOS) attack, whose computer is temporarily disabled by other computers ("zombies," in the inventive language of computer scientists) that barrage a victim's computer with requests that exhaust that computer's resources.[8] To wage such an attack, the attacker takes advantage of security lapses in the zombies' computer systems. Unlike many consumers of insecure software, victims of DDOS attacks cannot be readily dismissed for having contracted with a software provider to purchase the faulty software. Although Chandler's paradigmatic case is not software insecurity leading to the breach of privacy but rather insecurity leading to business interruption, she illuminates the doctrinal difficulties of a products liability claim for harm arising from unreasonably insecure software.

Shubha Ghosh and Vikram Mangalmurti propose more generally that information security systems be subject to strict liability for insecure systems. Holding software companies to this high standard would create strong incentives to improve security. Ghosh and Mangalmurti consider a number of difficult doctrinal issues raised by their approach. Is software a product (subject to a strict liability standard) or a service (subject to a negligence standard)? Should open source software systems be subject to strict liability? Ghosh and Mangalmurti offer some thoughtful initial suggestions on these and other questions.

Promoting Privacy and Security Through Statutory Reforms

Chris Jay Hoofnagle, of the leading privacy advocacy group Electronic Privacy Information Center, offers the example of Clifford J. Dawg, a canine cardholder of a Chase Manhattan Platinum Visa Card since 2004. Mr. Dawg does not need his master to buy him doggie treats because an overeager bank has supplied him with credit. This carefree attitude also infects credit reporting agencies, who are all too willing to share information with their clients because that is how they make money. By "freezing" credit information, Hoofnagle would require prior approval—either on a blanket basis or on a one-off basis—from the individual before the credit agency could release information about him or her. Potential identity thieves would find it more difficult to ob-

tain information about a possible victim. And this change would reduce the number of unsolicited credit card offers to man's best friend.

Edward J. Janger and Paul M. Schwartz offer the only argument for regulation that many economists understand: market failure. They argue that there are externalities to security breaches of financial information held by financial institutions and payment intermediaries. They suggest that information about security breaches is a "public good" and thus likely to be undersupplied if the market is left to itself. The externality arises in part because sensitive data, once released to the public domain, do not carry their own provenance. Because of this, consumers and others with an interest in preventing such leaks may not be able to discipline the institution releasing (intentionally or accidentally) the data. This argument might suggest a strong disclosure mandate, requiring financial institutions to report publicly releases of data that should be held private. But Janger and Schwartz challenge intuitions by suggesting that less disclosure of privacy breaches in financial data might improve privacy protections. They suggest the creation of an anonymous disclosure intermediary to which a financial institution could turn in the event of a leak. Because of anonymity, the financial institution would not suffer any reputational harm from the disclosure of the leak, a disclosure that it might be reluctant to make otherwise. The intermediary could then inform both other financial institutions and the individuals whose data were leaked about the problem, permitting them to adopt mitigating measures.

The technological cutting edge of this book is most evident in Jonathan Weinberg's appraisal of the privacy implications of RFIDs, described by Senator Leahy as "barcodes on steroids." Weinberg's early study of this emerging technology helps us recognize that the technological architecture is crucial to protecting privacy. Consider the possibility of limiting the unwanted release of information (or "blabbing," as Weinberg colorfully puts it) by requiring that the RFID tag emit not a single unique identifier but a series of random pseudonyms, understandable only by authorized readers. Even the most technical issue has hidden consequences for privacy; for example, if the tag's meaning is subject to open standards, it can be deciphered by anyone; if the meaning is restricted to proprietary databases, only those with access to those databases can interpret the tag. Weinberg identifies three specific privacy threats. First, RFIDs might be used to profile a person, with tag readers recognizing the tagged items carried by that person. Second, RFIDs enable surveillance because the tags, once tied to a particular person,

can be used to identify that person's physical location. Finally, information gained from an RFID can be used to take an action in response. Weinberg considers a number of ways to alleviate the privacy risk, from the voluntary adoption by the RFID industry of more privacy protecting technological standards to legislation mandating protections, such as the ability to easily identify and remove an RFID.

Susan W. Brenner proposes perhaps the most potent and, for data collectors, terrifying regulatory reform: a new criminal statute creating a misuse of personal data offense. Treating personal information as a kind of property, she concludes that certain kinds of data collection are theft. She recognizes that this poses a problem for most privacy invasions because, for any individual, the harm may be difficult to establish. She thus suggests that the "data crime" would not turn on harms to individual victims but rather on the systemic harm to society. Implementing this crime as a "public welfare" offense, she seems to favor doing away with *mens rea* in favor of strict liability.

The idea of a national ID card may send shudders down the spines of privacy advocates, but A. Michael Froomkin offers a thoughtful case for it nonetheless. Froomkin seeks to lessen the alarm by arguing that we already have a national ID card system in place de facto. The de facto system arises from the coincidence of the following events: (1) large legislatively authorized databases for specialized purposes, (2) the use of credit cards and other identifying cards that enable companies to amass enormous databases of personal information, (3) the increasing use of surveillance cameras by both public and private actors, and (4) the advances in computing technologies that have enabled companies to amass such enormous databases. A *de jure* system would have the virtue that it could build in privacy protections. One clear benefit of such a system is that, with appropriate biometric or other security measures, it would provide the possibility of better authentication, thereby reducing the possibility of identity theft. What remains unclear to the editors is whether the creation of a regulated *de jure* system would mean the elimination or control of an unregulated de facto system.

Promoting Privacy and Security Through the Market

Offering a dissenting view, Raymond T. Nimmer argues that advocates of increased privacy regulation seek data control, specifically, the reordering of the relationship between individuals and businesses with respect to information. He observes that United States law generally permits either side of a transac-

tion to exploit information gained through that transaction in the absence of a confidentiality agreement between the parties. For Nimmer, privacy regulations such as the European Union's Data Privacy Directive impose costs on ordinary transactions not justified by consumers' increased control over information. Nimmer accordingly prefers the status quo for the great bulk of consumer transactions, requiring individuals to act affirmatively to control information.

Jay P. Kesan, Ruperto P. Majuca, and William J. Yurcik argue for private insurance as the most efficient method for spurring optimal investment in information security. As long as premiums are tied to the level of self-protection measures undertaken by the firm, cyberinsurance is consistent with such measures. They offer an economic model of a firm's security behavior to make their case that a firm will likely benefit from insuring against the losses that might arise from an information security breach. If they are right, smart corporations should be purchasing such insurance, and indeed, they suggest that this is increasingly the case.

NOTES

1. Lawrence Lessig, *Code and the Laws of Cyberspace* 152 (2000).

2. Federal Trade Commission, *Identity Theft Survey Report* 4 (Sept. 2003).

3. *See* Daniel J. Solove, The New Vulnerability: Data Security and Personal Information, Chapter 6 in this volume.

4. Lilian Edwards, The Problem with Privacy: A Modest Proposal, 18 *Int'l Rev. L., Comp. & Tech.* 309, 323 (Nov. 2004).

5. *See* Thomas J. Smedinghoff, Defining the Legal Standard for Information Security, Chapter 1 in this volume.

6. *RFID in Japan*, June 1, 2004, available at http://ubiks.net/local/blog/jmt/archives3/cat_applications.html.

7. Jenna Wortham, Disable Your Passport's RFID Chip, *Wired* 46 (Jan. 2007).

8. *See generally* Margaret Jane Radin, Distributed Denial of Service Attacks: Who Pays? (Part I), 6 *Cyberspace Lawyer* 2 (Dec. 2001); Distributed Denial of Service Attacks: Who Pays? (Part II), 6 *Cyberspace Lawyer* 2 (Jan. 2002).