The Digital Person
Technology and Privacy in the Information Age

Daniel J. Solove
the digital person
Ex Machina: Law, Technology, and Society
General Editors: Jack M. Balkin and Beth Simone Noveck

The Digital Person
Technology and Privacy in the Information Age

Daniel J. Solove
the digital person
Technology and Privacy in the Information Age
daniel j. solove
In loving memory of

my grandma,

Jean
Contents

Acknowledgments ix

1 Introduction 1
  The Problems of Digital Dossiers 2
  Traditional Conceptions of Privacy 7
  Rethinking Privacy 8
  A Road Map for This Book 9

i computer databases

2 The Rise of the Digital Dossier 13
  A History of Public-Sector Databases 13
  A History of Private-Sector Databases 16
  Cyberspace and Personal Information 22

3 Kafka and Orwell: 27
  Reconceptualizing Information Privacy 27
  The Importance of Metaphor 27
  George Orwell’s Big Brother 29
Franz Kafka's Trial 36
Beyond the Secrecy Paradigm 42
The Aggregation Effect 44
Forms of Dehumanization:
   Databases and the Kafka Metaphor 47

4 The Problems of Information Privacy Law 56
   The Privacy Torts 57
   Constitutional Law 62
   Statutory Law 67
   The FTC and Unfair and Deceptive Practices 72
   A World of Radical Transparency:
      Freedom of Information Law 73
   The Law of Information Privacy and
      Its Shortcomings 74

5 The Limits of Market-Based Solutions 76
   Market-Based Solutions 76
   Misgivings of the Market 81
   The Value of Personal Information 87
   Too Much Paternalism? 90

6 Architecture and the Protection of Privacy 93
   Two Models for the Protection of Privacy 93
   Toward an Architecture for
      Privacy and the Private Sector 101
   Reconceptualizing Identity Theft 109
   Forging a New Architecture 119

7 The Problem of Public Records 127
   Records from Birth to Death 127
The Impact of Technology
The Regulation of Public Records

8 Access and Aggregation: Rethinking Privacy and Transparency
The Tension between Transparency and Privacy
Conceptualizing Privacy and Public Records
Transparency and Privacy:
  Reconciling the Tension
Public Records and the First Amendment

iii government access

9 Government Information Gathering
Third Party Records and the Government
Government–Private-Sector Information Flows
The Orwellian Dangers
The Kafkaesque Dangers
Protecting Privacy with Architecture

10 The Fourth Amendment, Records, and Privacy
The Architecture of the Fourth Amendment
The Shifting Paradigms of Fourth Amendment Privacy
The New Olmstead
The Emerging Statutory Regime and Its Limits

11 Reconstructing the Architecture
Scope: System of Records
Structure: Mechanisms of Oversight
Regulating Post-Collection Use of Data
Developing an Architecture
12 Conclusion 223

Notes 229
Index 267
About the Author 283
It is often said that books are written in solitude, but that wasn’t true for this one. The ideas in this book were created in conversation with many wise friends and mentors. I owe them immense gratitude. Michael Sullivan has had an enormous influence on my thinking, and he has continually challenged me to strengthen my philosophical positions. Paul Schwartz has provided countless insights, and his work is foundational for the understanding of privacy law. Both Michael’s and Paul’s comments on the manuscript have been indispensable. I also must thank Judge Guido Calabresi, Naomi Lebowitz, Judge Stanley Sporkin, and Richard Weisberg, who have had a lasting impact on the way I think about law, literature, and life.

Charlie Sullivan deserves special thanks, although he disagrees with most of what I argue in this book. He has constantly forced me to better articulate and develop my positions. I may never convince him, but this book is much stronger for making the attempt.

So many other people are deserving of special mention, and if I were to thank them all to the extent they deserve, I would more than double the length of this book. Although I only list their names, my gratitude extends much further: Anita Allen, Jack Balkin, Carl Coleman, Howard Erichson, Timothy Glynn, Rachel Godsil, Eric Goldman, Chris Hoofnagle, Ted Janger, Jerry Kang, Orin Kerr, Raymond Ku, Erik Lillquist, Michael Risinger, Marc Rotenberg, Richard St. John, Chris Slobogin, Richard Sobel, Peter Swire, Elliot Turrini, and Benno Weisberg.
I greatly benefited from the comments I received when presenting my ideas, as well as portions of the manuscript, at conferences and symposia at Berkeley Law School, Cornell University, Emory Law School, Minnesota Law School, Seton Hall Law School, Stanford Law School, and Yale Law School.

My research assistants Peter Choy, Romana Kaleem, John Spaccarotella, and Eli Weiss provided excellent assistance throughout the writing of this book. Dean Pat Hobbs and Associate Dean Kathleen Boozang of Seton Hall Law School gave me generous support.

Don Gastwirth, my agent, shepherded me through the book publishing process with great enthusiasm and acumen. With unceasing attention, constant encouragement, and superb advice, he helped me find the perfect publisher. Deborah Gershenowitz at NYU Press believed in this project from the start and provided excellent editing.

Finally, I would like to thank my parents and grandparents. Their love, encouragement, and belief in me have made all the difference.

This book incorporates and builds upon some of my previously published work: Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stanford Law Review 1393 (2001); Access and Aggregation: Privacy, Public Records, and the Constitution, 86 Minnesota Law Review 1137 (2002); Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 Southern California Law Review 1083 (2002); and Identity Theft, Privacy, and the Architecture of Vulnerability, 54 Hastings Law Journal 1227 (2003). These articles are really part of a larger argument, which I am delighted that I can now present in its entirety. The articles are thoroughly revised, and parts of different articles are now intermingled with each other. The argument can now fully unfold and develop. Privacy issues continue to change at a rapid pace, and even though these articles were written not too long ago, they were in need of updating. The arguments originally made in these articles have been strengthened by many subsequent discussions about the ideas I proposed. I have been forced to think about many issues more carefully and with more nuance. My understanding of privacy is a work in progress, and it has evolved since I began writing about it. This book merely represents another resting place, not the final word.
Many solutions to the problems of privacy and information are market-based, relying on property rights or contractual default rules to regulate the flow of information. Does the market already adequately protect privacy? Or can the market, with minor tinkering, develop effective privacy protection? Or must a more radical reconstruction of the market be undertaken?

**Market-Based Solutions**

*Property Rights and Contract.* The notion of “control of personal information” is one of the most dominant conceptions of privacy. As privacy expert Alan Westin declares: “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”¹ Numerous other scholars embrace this definition.²

Theorists who view privacy as control over information frequently understand it within the framework of property and contract concepts. This is not the only way control can be understood, but the
leading commentators often define it in terms of ownership—as a property right in information. Understood in such terms, control over something entails a bundle of legal rights of ownership, such as rights of possession, alienability, exclusion of others, commercial exploitation, and so on. This is what leads Westin to conclude: “[P]ersonal information, thought of as the right of decision over one’s private personality, should be defined as a property right.” The market discourse focuses the debate around who should own certain kinds of information as well as what the appropriate contractual rules should be for trading personal information.

Therefore, in addition to property rights, contract law plays an important role in regulating privacy. Parties can make contractual agreements about privacy at the outset of forming a relationship. In certain instances, courts have held that even though the contract did not specifically mention privacy, it is an implied term in the contract. The common law tort of breach of confidentiality embodies this view. It enables people to sue for damages when a party breaches a contractual obligation (often implied rather than express) to maintain confidentiality. This tort primarily protects the privacy of the patient-physician relationship. The tort also has been used to protect against banks breaching the confidences of their customers.

Implied contractual terms are a form of default rule in the contract. Contractual default rules are the initial set of rules that regulate market transactions. These rules are merely a starting point; they govern only when the parties to a transaction do not negotiate for a different set of rules. As legal scholar Ian Ayres and economist Robert Gertner explain, “default rules” are rules “that parties can contract around by prior agreement” while “immutable rules” (or inalienability rules) are rules that “parties cannot change by contractual agreement.” Most market proponents favor default rules that can be bargained around. Market solution proponents, however, are certainly not in agreement over the types of property entitlements and contractual default rules that should be required. But once these are established, then the market can do the rest. People and companies can buy and sell personal information and make contracts about the protection of privacy. For example, a number of commentators
recommend contractual solutions to safeguard privacy, such as where consumers license the use of their data to businesses.9

Although some might argue that personal information is owned by the individual to whom it pertains based on a natural rights theory or some form of inherent connection, many commentators who approach privacy in terms of property rights assign initial entitlements instrumentally. They claim that the market will achieve the ideal amount of privacy by balancing the value of personal information to a company (i.e., its commercial value in the marketplace) against the value of the information to the individual and the larger social value of having the information within the individual’s control.10 The role of law is to assign the initial entitlements. Thus, the debate in this discourse centers around who should own certain kinds of information.

So who should own personal information when people transact with businesses? The individuals to whom the information pertains? Or the companies that collect it?

Judge Richard Posner suggests that the law should often favor the companies over the individuals. Posner translates control of information into property concepts. Society should provide individuals a property right in true information about themselves when it will foster more efficient transactions.11 With regard to the sale of customer lists, Posner argues that “the costs of obtaining subscriber approval would be high relative to the value of the list.” He concludes: “If, therefore, we believe that these lists are generally worth more to the purchasers than being shielded from possible unwanted solicitations is worth to subscribers, we should assign the property right to the [companies]; and the law does this.”12

In contrast, law professor Richard Murphy concludes that in many instances, contractual default rules mandating confidentiality of personal information are more efficient than default rules permitting disclosure.13 For Murphy, privacy has “substantial economic benefits” because “[u]nless a person can investigate without risk of reproach what his own preferences are, he will not be able to maximize his own happiness.”14

Likewise, Jerry Kang views personal information as a form of property and advocates for a market solution. He recognizes that there are compelling non-market perceptions of privacy that view privacy as a
human value and that this way of understanding privacy is “poorly translated, if at all, into efficiency terms.” Nevertheless, he favors the market approach. Kang recognizes that merely assigning a default rule as to the ownership of information will be ineffective because individuals lack convenient ways to find out what information about them is collected and how it is used. Thus, he advocates a contractual default rule that “personal information may be processed in only functionally necessary ways” and that parties are “free to contract around the default rule.” Kang claims that inalienability rules would be too paternalistic because individuals should be able to sell or disclose their information if they desire. Inalienability rules will risk “surrendering control over information privacy to the state.”

Internet law expert Lawrence Lessig also recommends a market-based approach. He argues that a property regime permits each individual to decide for herself what information to give out and “protects both those who value their privacy more than others and those who value it less.” Lessig notes that our existing system of posting privacy policies and enabling consumers to opt in or out has high transaction costs because people do not have “the time or patience to read through cumbersome documents describing obscure rules for controlling data.” Therefore, Lessig recommends that computer software be crafted to act akin to an “electronic butler,” negotiating our privacy concerns: “The user sets her preferences once—specifies how she would negotiate privacy and what she is willing to give up—and from that moment on, when she enters a site, the site and her machine negotiate. Only if the machines can agree will the site be able to obtain her personal data.” In other words, Lessig suggests a technological implementation for a market system where people have property rights in their information.

**Self-Regulation.** Some commentators—especially people in the database industry—argue that the market is functioning optimally and is already adequately accounting for privacy concerns. The market, they argue, is already treating personal information as a property right owned by individuals. Companies have increasingly been adopting privacy policies, which can operate as a form of contractual promise limiting the future uses of the information. The exchange of
personal information for something of value is already beginning to take place. Many websites require people to supply personal information in order to gain access to information on the website. Under the market approach, this practice can be justified as an information trade. In order to receive such services as book recommendations, software upgrades, free email, and personal web pages, users must relinquish personal information not knowing its potential uses. In short, useful information and services are being exchanged for personal information, and this represents the going “price” of privacy.

Moreover, there are market incentives for companies to keep their data secret and to be honest about their data collection. There have been a number of instances where companies have canceled various initiatives due to public outcry over privacy. For example, in response to privacy concerns, Yahoo! eliminated the reverse telephone number search from its People Search site. In the early 1990s, in response to a public outcry, Lotus Corporation scrapped plans to sell a database containing the names, addresses, income brackets, and lifestyle data of 120 million citizens. In 1996, Lexis-Nexis announced its P-TRAK Personal Locator, which would provide addresses, maiden names, and SSNs of millions of people. After an intensive 10-day outcry by Internet users, Lexis-Nexis canceled P-TRAK. In 1997, AOL halted its plans to sell customers’ phone numbers to direct marketing firms.

Furthermore, proponents of self-regulation argue that information flow has many beneficial uses. Legal scholar Fred Cate contends that information flow makes the consumer credit system cheaper and faster, “enhances customer convenience and service,” and enables businesses “to ascertain customer needs accurately and meet those needs rapidly and efficiently.” Many people want some targeted marketing and enjoy receiving information about products more tailored to their tastes.

Cate points out that self-regulation is “more flexible and more sensitive to specific contexts and therefore allow[s] individuals to determine a more tailored balance between information uses and privacy than privacy laws do.” The most effective way for people to protect their privacy, Cate contends, is to take actions themselves.

Law professor Eric Goldman argues that “consumers’ stated privacy concerns diverge from what consumers do.” People are quick to
say in the abstract that they want privacy, but when offered money or discounts in return for their personal information, they readily relinquish it. “[P]eople won’t take even minimal steps to protect themselves,” Goldman asserts, “[s]o why should government regulation do it for them?” Finally, Goldman argues, “online businesses will invest in privacy when it’s profitable.”

Thus, the self-regulation proponents conclude that to the extent that consumers want their privacy protected, the market will respond to this demand and appropriately balance it against other interests. The fact that privacy is not afforded much protection demonstrates that people value other things more than privacy—such as efficient and convenient transactions.

Misgivings of the Market

Understanding the privacy problem of databases in terms of the Kafka metaphor—our helplessness and vulnerability in the face of the powerful bureaucracies that handle our personal data—reveals that there are several deficiencies in market solutions.

The Limitations of Contract Law. Although contract law can protect privacy within relationships formed between parties, it does not redress privacy invasions by third parties outside of the contractual bonds. Warren and Brandeis recognized this problem back in 1890 when they spoke of new photographic technologies. Cameras had been quite large, and people had to pose to have their picture taken. This would likely require people to establish some sort of contractual relationship with the photographer. But the development of cheaper portable cameras in the 1880s enabled strangers to take pictures without the subject ever knowing.

Today, our personal information is increasingly obtained by people and organizations that have never established any relationship with us. For example, as public health law expert Lawrence Gostin notes, the law of patient-physician confidentiality “is premised on the existence of a relationship between a physician and a patient, although most health information is not generated within this relationship.” Information is often maintained not just by one’s physician, but one’s
health plan, government agencies, health care clearinghouse organizations, and many others.

Problems with Bargaining Power. There are great inequalities in bargaining power in many situations involving privacy, such as employment contracts or contracts between big corporations and individuals. How many people are able to bargain effectively over their contracts with their Internet Service Providers, cable providers, telephone companies, and the like? Oscar Gandy observes that “individuals are largely ‘contract term takers’ in the bulk of their economic relations with organizations.” People frequently accede to standardized contract terms without putting up much of a fight.

Nor does it appear that market competition is producing a wide menu of privacy protections. Companies only rarely compete on the basis of the amount of privacy they offer. People often do not weigh privacy policies heavily when choosing companies. For example, people rarely choose phone companies based on their privacy policies.

Self-regulatory proponents would respond that this fact indicates that privacy isn’t very important to most people. If people really cared about privacy, the self-regulators argue, then they would refuse to deal with companies offering inadequate levels of privacy. But as Paul Schwartz contends, there are coordination problems because “individuals may have difficulty finding effective ways to express collectively their relative preferences for privacy.”

Although more companies that routinely collect and use personal information are posting privacy policies, these policies have several difficulties. Privacy policies are often written in obtuse prose and crammed with extraneous information. But market proponents—especially those favoring self-regulation—counter that many people don’t bother to read privacy policies. This may not necessarily stem from their turgid prose, but from the fact that consumers don’t want to take the time to read them. Perhaps people just don’t care.

However, perhaps the lack of interest in privacy policies may stem from the fact that the policies hardly amount to a meaningful contract, where the parties bargain over the terms. Privacy policies are little more than “notices” about a company’s policies rather than a
contract. Privacy policies tend to be self-indulgent, making vague promises such as the fact that a company will be careful with data; that it will respect privacy; that privacy is its number one concern. These public relations statements are far from reliable and are often phrased in a vague, self-aggrandizing manner to make the corporation look good. What consumers do not receive is a frank and detailed description of what will and will not be done with their information, what specific information security measures are being taken, and what specific rights of recourse they have. People must rely on the good graces of companies that possess their data to keep it secure and to prevent its abuse. They have no say in how much money and effort will be allocated to security; no say in which employees get access; and no say in what steps are taken to ensure that unscrupulous employees do not steal or misuse their information. Instead, privacy policies only vaguely state that the company will treat information securely. Particular measures are not described, and individuals have no control over those measures.

Most privacy policies provide no way for customers to prevent changes in the policy, and they lack a binding enforcement mechanism. Frequently, companies revise their privacy policies, making it even more difficult for an individual to keep track. Yahoo!’s privacy policy indicates that it “may change from time to time, so please check back periodically.”32 AOL once told its subscribers that their privacy preferences had expired and that if they did not fill out a new opt-out form, then their personal information would be distributed to marketers.33 Further, personal information databases can be sold to other businesses with less protective privacy policies, especially when a company goes bankrupt. For example, in 2000, Internet toy retailer Toysmart.com filed for bankruptcy and attempted to auction off its personal information database of over 200,000 customers.34 Dot-com bankruptcies create a breakdown in the relationship between companies and consumers, resulting in little incentive for the bankrupt company to take measures to protect consumer data. Personal information databases are often a company’s most valuable asset and could be sold to third parties at bankruptcy to pay off creditors.35

Second, to the extent that privacy policies do provide individuals with privacy protection, it is often provided with an opt-out system,
in which personal data can be collected and used unless the individual expressly says no. Opt-out systems require individuals to check a box, send a letter, make a telephone call, or take other proactive steps to indicate their preferences. However, these steps are often time-consuming. There are too many collectors of information for a right of opt-out to be effective. Without a centralized mechanism for individuals to opt-out, individuals would have to spend much of their time guarding their privacy like a hawk.

The Direct Marketing Association (DMA) has established a system where consumers can be placed on a no-solicitation list. This is essentially a database of people who do not want to be in databases. The service records their preference, but does not remove their name from any list. The database is then sent to the subscribing companies so that they can stop mailings to those names. However, many people are unaware of this option, numerous companies are not members of the DMA, and many members fail to comply with DMA guidelines. As legal scholar Jeff Sovern argues, opt-out systems provide little incentive to companies to make opting-out easy; “companies will incur transaction costs in notifying consumers of the existence of the opt-out option and in responding to consumers who opt out.” Since companies want to use personal information, their incentive in an opt-out system is to make opting-out more difficult.

These problems arise because people often lack sufficient bargaining power over their privacy. As privacy law expert Peter Swire observes, it is difficult for consumers to bargain with large corporations about their privacy because they lack expertise in privacy issues and because it takes substantial time and effort. Information collection is duplicitous, clandestine, and often coerced. The law currently does not provide meaningful ability to refuse to consent to relinquish information. The FCRA, for example, mandates that individuals consent before an employer can obtain their credit report. According to Joel Reidenberg: “Frequently, individuals will be asked to sign blanket consent statements authorizing inquiry into credit reporting agency files and disclosures of information for any purpose. These consents rarely identify the credit reporting agencies or all the uses to which the personal information will be put.” This consent is virtually meaningless. When people seek medical care, among the forms they
sign are general consent forms which permit the disclosure of one's medical records to anyone with a need to see them. Giving people property rights or default contract rules is not sufficient to remedy the problem because it does not address the underlying power inequalities that govern information transactions. Unless these are addressed, any privacy protections will merely be “contracted” around, in ways not meaningful either to the problem or to the contract notions supposedly justifying such a solution. People will be given consent forms with vague fine-print discussions of the contractual default privacy rules that they are waiving, and they will sign them without thought. As Julie Cohen correctly contends, “[f]reedom of choice in markets requires accurate information about choices and other consequences, and enough power—in terms of wealth, numbers, or control over resources—to have choices.” The bargaining process must be made easier. The way things currently stand, most people don’t know even know where to begin if they want to assert their preference for privacy.

The One-Size-Fits-All Problem. Even assuming these problems could be dealt with, a number of additional difficulties remain that prevent individuals from exercising their preferences to protect their privacy. Affording individuals a right to control their personal data improperly assumes that individuals have the ability to exercise meaningful control over their information. Paul Schwartz notes how consent screens on a website asking users to relinquish control over information often do so on a “take-it-or-leave-it basis” resulting in the “fiction” that people have “expressed informed consent to [the website’s] data processing practices.” Individuals are often presented with an all-or-nothing choice: either agree to all forms of information collection and use or to none whatsoever. Such a limited set of choices does not permit individuals to express their preferences accurately. Individuals frequently desire to consent to certain uses of their personal information, but they do not want to relinquish their information for all possible future uses.

For example, a person may want to purchase books from an online bookseller. Suppose that the person’s privacy preferences consist of the information being kept very secure, not being disclosed to the
government, and not being traded or disclosed to other companies (even in the event that the company goes bankrupt). But the online bookseller’s privacy policy is standardized and often does not address these points with any reasonable degree of specificity. And since privacy policies are remarkably similar among many companies, many other online bookstores offer comparable terms. If the person decides to purchase the book in a bricks-and-mortar bookstore, she faces the same difficulties if she pays by credit card. There, the privacy policies are not even readily available to the purchaser.

This state of affairs exists partly because not many choices are available to people regarding their privacy and partly because people are often not aware of the problems, risks, and dangers about how their information is handled. Even if they were, it is doubtful whether a person could create a special deal with a company to provide greater protections for her privacy. Therefore, with regard to the level of privacy protection offered by companies, a person must simply take it or leave it. People are not afforded enough choices to exercise their privacy preferences. A more complete range of choices must permit individuals to express their preferences for how information will be protected, how it will be used in the future, and with whom it will be shared. Moreover, because companies controlling personal information are secretive about its uses and vague about their privacy policies, people lack adequate knowledge to make meaningful choices.

Market proponents might respond that it is not economically feasible for companies to offer customized privacy policies. This would require companies to keep track of each particular customer’s privacy preferences, which could be cumbersome and expensive. However, companies maintain very complex databases, able to handle countless fields of data and multiple variables. Why can’t various privacy preferences be recorded along with various pieces of information?

*Inequalities in Knowledge.* The argument that the market is already providing the optimal level of privacy protection fails because there are vast inequalities in knowledge and much data collection is clandestine. Despite the few instances where information collection initiatives were canceled due to public complaints over privacy, many new,
ambitious information gathering endeavors occur outside of the public eye. At any given time, one of thousands of companies or government agencies could decide on a new use of information or on a new form of collection. People should not always have to be ready to mount a large campaign anytime such an eruption could occur. Many of the activities of the database industry are not well known to the public, and will remain that way under default notions of corporate privacy and trade secrets unless something is changed. Ironically, corporate bureaucracies sometimes have more privacy rights than individuals.

The Value of Personal Information

A key aspect of property rights, observes information law scholar Pamela Samuelson, is that property is alienable—people can readily trade it away. Market solutions, which view information as property that can be traded in the market, depend upon the ability of people to accurately assess the value of information. As legal scholar Katrin Byford aptly notes, assigning property rights in information “values privacy only to the extent it is considered to be of personal worth by the individual who claims it.” The value of personal information is determined by how much it takes for a person to relinquish it. Since people routinely give out their personal information for shopping discount cards, for access to websites, and even for free, some market proponents (especially the self-regulators) argue that the value of the data is very low to the individuals. The market is thus already adequately compensating individuals for the use of their information.

In a well-functioning market, assuming no market failure, the market might work quite well in valuing personal information. But the market in privacy is not a well-functioning market, and thus its valuation determinations are suspect.

The Aggregation Effect. The aggregation effect severely complicates the individual’s ability to ascribe a value to personal information. An individual may give out bits of information in different contexts, each transfer appearing innocuous. However, when aggregated, the information becomes much more revealing. As law professor Julie Cohen
observes, each instance in which we give out personal information may seem “trivial and incremental,” which “tends to minimize its ultimate effect.” It is the totality of information about a person and how it is used that poses the greatest threat to privacy. From the standpoint of each particular information transaction, individuals will not have enough facts to make a truly informed decision.

Uncertain Future Uses. The potential future uses of personal information are too vast and unknown to enable individuals to make the appropriate valuation. The value of much personal information, such as one’s SSN, does not stem from its intimacy, its immediate revelations of selfhood, or the fact that the individual has authored it. Rather, the value is in the ability to prevent others from gaining power and control over an individual; from revealing an individual’s private life; and from making the individual vulnerable to fraud, identity theft, prying, snooping, and the like. Because this value is linked to uncertain future uses, it is difficult, if not impossible, for an individual to adequately value her information. Since the ownership model involves individuals relinquishing full title to the information, they have little idea how such information will be used when in the hands of others.

For example, a person who signs up for a discount supermarket shopper card might have some vague knowledge that her personal information will be collected. In the abstract, this knowledge may not be all that disconcerting. But what if the person were told that information about the contraceptives and over-the-counter medications she buys would be made available to her employer? Or given to the government? Or used to send her advertisements or spam? Without being informed about how the information will be used, the individual lacks the necessary knowledge to assess the implications of surrendering her personal data.

Is Privacy a Property Right? When personal information is understood as a property right, the value of privacy often is translated into the combined monetary value of particular pieces of personal information. Privacy becomes the right to profit from one’s personal data, and the harm to privacy becomes understood as not being adequately paid
for the use of this “property.” But is this really the harm? Can privacy be translated into property concepts without losing some of its meaning?49

An initial difficulty with understanding personal information as a form of property is that it is unclear who really creates the information. Some pro-privacy commentators quickly assume that because information pertains to a person, the person should have a right to own it. However, information is often not created by the individual alone. We often develop personal information through our relationships with others. When a person purchases a product, information is created through the interaction of seller and buyer.

Consider the case of Dwyer v. American Express Co. American Express cardholders sued American Express for renting their names to merchants under both invasion of privacy and appropriation. The court held that by using the credit card, “a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder’s spending habits and shopping preferences.” Thus, there was no invasion of privacy. As for appropriation, the court reasoned:

Undeniably, each cardholder’s name is valuable to defendants. The more names included on a list, the more that list will be worth. However, a single, random cardholder’s name has little or no intrinsic value to defendants (or a merchant). Rather, an individual name has value only when it is associated with one of the defendants’ lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendants’ practices do not deprive any of the cardholders of any value their individual names may possess.50

This case indicates what is omitted when information privacy is reduced to property rights in information. The court only focused on the value of the information to each individual, not on the systemic harms to which American Express’s practices contributed—namely, the powerlessness of the individuals to have any meaningful control over information pertaining to their personal lives. The problem with databases is not that information collectors fail to compensate people
for the proper value of personal information. The problem is people’s lack of control, their lack of knowledge about how data will be used in the future, and their lack of participation in the process. It is not merely sufficient to allow people to sell their information, relinquish all title to it, and allow companies to use it as they see fit. This provides people with an all-or-nothing type of exchange, which they are likely to take when they are unaware of how information can or might be used in the future. Nor is it enough to attach some default contractual rights to information transactions such as nondisclosure obligations or a requirement of notification when a future use of information is employed. These solutions cannot work effectively in a situation where the power relationship between individuals and public and private bureaucracies is so greatly unbalanced. In other words, the problem with market solutions is not merely that it is difficult to commodify information (which it is), but also that a regime of default rules alone (consisting of property rights in information and contractual defaults) will not enable fair and equitable market transactions in personal information. As Julie Cohen warns, giving people property rights in a defective market runs the risk of leading to more trade in personal information, not less.51

Due to the problems with ascribing a value to personal information and because privacy is an issue about societal structure involving our relationships with public and private bureaucracies, some form of regulation is necessary that exceeds the narrow measures proposed by proponents of a market solution. There are certain rights we cannot bargain away because they are not mere individual possessions but are important for the structure of society as a whole.

**Too Much Paternalism?**

Market proponents are wary of government regulation because it threatens to usurp individual choice. They argue that people should be free to contract as they see fit. If people want to give up their privacy, the government shouldn’t paternalistically say that it knows best. Market proponents contend that people are capable of making rational decisions about their personal information and that the law shouldn’t interfere.
This argument is quite compelling, for not all individuals want privacy. For example, people may want their names sold to other companies because they like receiving catalogs. Market proponents thus aim to preserve individual choice.

The problem, however, is that the market currently fails to provide mechanisms to enable individuals to exercise informed meaningful choices. Even market approaches favoring a more pro-privacy regime of contractual default rules neglect to account for the core of the database problem as illustrated by the Kafka metaphor—the power inequalities that pervade the world of information transfers between individuals and bureaucracies.

As a result of these problems, there is little economic incentive for companies to adopt strong privacy protection in the absence of legal regulation. Although the Direct Marketing Association (DMA) maintains standards for self-regulation, polls suggest that less than 25 percent of DMA members adhere to self-regulatory practices. The individual’s lack of knowledge about the use of personal information also makes companies less responsive to privacy concerns. One employee at a bank stated: “We joke about it all the time because we officially say that we don’t reveal information and we treat it with the utmost respect. What a crock. I hear people laughing in the elevator about credit reports they’ve pulled!” Unless people have greater knowledge about the uses of their information and practices within a company, they won’t be able even to raise an outcry.

I am not arguing that the market can’t protect privacy. The market can work well, but not in the absence of structural legal protections. A set of laws and rights is necessary to govern our relationship with bureaucracies. These laws must consist of more than default rules that can be contracted around or property entitlements that can be bartered away. Market-based solutions work within the existing market; the problem with databases is the very way that the market deals with personal information—a problem in the nature of the market itself that prevents fair and voluntary information transactions.

Inalienability rules do not necessarily have to limit a person’s ability to disclose or sell certain information; nor must they limit many forms of information collection. If the problem is understood with the Kafka metaphor, the solution to regulating information flow is not
to radically curtail the collection of information but to regulate uses. For example, Amazon.com’s book recommendation service collects extensive information about a customer’s taste in books. If the problem is surveillance, then the most obvious solution would be to provide strict limits on Amazon.com’s collection of information. This solution, however, would curtail much data gathering that is necessary for business in today’s society and that is put to beneficial uses. Indeed, many Amazon.com customers, myself included, find Amazon.com’s book recommendation service to be very helpful. In contrast, if the problem is understood as I have depicted it, then the problem is not that Amazon is spying on its users or that it can use personal data to induce its customers to buy more books. What is troubling is the unfettered ability of Amazon.com to do whatever it wants with this information. This problem was underscored when Amazon.com abruptly changed its privacy policy to allow the transfer of personal information to third parties in the event Amazon.com sold any of its assets or went bankrupt. As a customer, I had no say in this change of policy; no ability to change it or bargain for additional privacy protection; and no sense about whether it would apply retroactively to the purchases I already made. And what’s to prevent Amazon.com in the future from changing its policy once again, perhaps retroactively?

Therefore, privacy regulations should focus on our relationships with bureaucracies, for unless these relationships are restructured, markets in information will not consist of fair, voluntary, and informed information transactions. Markets can certainly work to protect privacy, but a precondition of a successful market is establishing rules governing our relationships with bureaucracies.