Law & Social Inquiry
Journal of the American Bar Foundation

Law & Social Inquiry
Volume 37, Issue 1, 119–145, Winter 2012

Privacy Codes and Institutional Record Keeping: Procedural versus Strategic Approaches

James B. Rule

Privacy codes aim at protecting individuals' interests in the treatment of data on themselves held by institutions. One can distinguish between procedural *and* strategic *principles underlying these codes. The former aim at shaping treatment of personal information, once compiled within data systems; the latter aim at limiting and dispersing personal information from the start. A historical view of the workings of these two principles gives more reasons for optimism in the case of strategic measures. In contrast, procedural restrictions on access to personal information are evidently subject to erosion and reversal with changes in larger political climates.*

INTRODUCTION

In 2003, superstar Alex Rodriguez agreed to take part in a "survey" of performance-enhancing drug use among professional baseball players. According to a *New York Times* account:

> No names were to be revealed. Instead, the results were supposed to be used in aggregation—to determine if more than 5 percent of players were cheating—and the samples were then to be destroyed. (Cohen 2009, B3)

Imagine the unpleasant surprise to Rodriguez and those around him in 2009 on learning that his identity had been preserved along with the test results. Federal investigators seized those results in 2004 in connection with wide-ranging investigations of steroid use in baseball. After first denying any such use, Rodriguez later generated a stream of mea culpas.

In a far lower profile case in 1996, a muscular dystrophy patient in Syracuse, NY, sued Metropolitan Nursing Services for $10 million in pain and suffering. A health aide employed by the service to care for her in her home raped her, and her lawsuit held that the employer did not fully investigate the perpetrator's criminal record (Wright 1996).

In juxtaposition, these two accounts frame the tension central to this study: the tension between the seemingly ever-increasing *supply* of documented personal

James B. Rule is at the Center for the Study of Law and Society, University of California, Berkeley. He writes widely on information and privacy issues. He expresses particular thanks to Evan Hendricks, Paul Schwartz, Peter Swire, and Lee Tien, as well as to a number of conscientious, anonymous reviewers, for help in preparation of this article. He may be contacted at jbrule@berkeley.edu.

information and the commensurately growing *demand* for use of such data to shape institutional action toward the people so depicted.

Since the middle of the twentieth century, Americans and members of other "advanced" societies have come to live in a world where nearly everyone expects dealings with major institutions to be based on one's "record." Such records govern the treatment one receives from the most diverse government and private-sector institutions, ranging from credit card companies to medical care providers to law enforcement and state security agencies. Nearly everyone now appreciates how consequential such record keeping is for one's life chances—that is, how much it matters who compiles records, what information can be included, who can share access to such data, and what kinds of decisions can be made on their basis. Given the gravity of the consequences, it is no surprise that conflict and controversy have come to surround these processes and that legislation and policy have grown up in response.

Let me call these bodies of legislation and policy "privacy codes." "Privacy" is, in fact, less exact than the technical term "personal data protection," but it highlights the complex of sensitive values that the codes seek to uphold. Privacy codes in this sense seek to regulate collection and use of personal data held on file by government and private institutions. Over the last four decades, virtually all the world's liberal societies have adopted some such measures. Adoption began in the 1970s with the democracies of North America and Western Europe and has continued in liberal societies outside these regions, such as Australia (1988), Iceland (1989), South Korea (1994), and Argentina (2000) (EPIC 2005). Details of the codes inevitably vary from one country to the next, but a stable core of principles for the handling of personal information underlies nearly all of them.

Evolving in parallel with diffusion of privacy codes are the possibilities and practices of organizations for creating, collecting, and using personal data. Few aspects of social life have changed more dramatically in the last few decades than the social role of information, with personal information among the most consequential. Conventional wisdom characterizes such changes as direct effects of "technology," but, in fact, they involve both new capabilities in computing and other information technologies and new strategies and institutional relationships among data-using organizations. The net result is that demand for personal data from government and private institutions and the possibilities for exploiting personal information compiled in response to such demands yield ever-unfolding surprises like those confronting Alex Rodriguez.

I argue here that the broad principles of global consensus underlying privacy codes have not done well in upholding privacy values against countervailing forces and trends. Notwithstanding some significant protections for individuals afforded by these measures, it is hard to affirm that privacy interests in the institutional handling of personal data are better served today than at the onset of these debates. Yet, some legal and policy responses to the evident public concern over institutional use and misuse of personal data have produced more effective results than others. I hold that laws and policies constraining when and how personal information should be recorded or retained in the first place and what parties can know about where to look for such data—strategic approaches, as I call them—are more promising than procedural measures governing how personal data should be handled once captured and centralized.

I argue that procedural measures, the mainstay of most privacy codes, are less suited to withstand pressures for sharing and reuse of personal information that predictably arise after its original compilation. Strategic approaches, on the other hand, have the virtue of simply curtailing the availability of such data for such later appropriation.

A number of commentators have noted the limitations of procedural approaches and envisaged alternate programs for protecting personal data. Some of the most acute of these suggestions have focused on changing the designs of Internet data transmission.

Joel Reidenberg, for example, proposes that policy makers rely on what he terms *lex informatica*, "the set of rules for information flows imposed by technology and communication networks" (1998, 554). Such reliance, he holds, would enable various government jurisdictions to customize their own policies as to what information may or may not be shared, making it possible "to achieve objectives that otherwise challenge conventional laws and attempts by government to regulate across jurisdictional lines" (1998, 555). Protection for personal data is, of course, one such objective.

Lawrence Lessig develops a similar argument in *Code; and Other Laws of Cyberspace* (1999), applying it to the development of cyberspace more generally. "*Code is law*" (1999, 6) might be his mantra: "the software and hardware that make cyberspace what it is *regulate* cyberspace as it is" (1999, 6). He urges active shaping of what he calls the *architectures* of cyberspace "to restore in the individual . . . control over . . . personal data" (1999, 156). One example of such architecture given by Lessig is "a machine-to-machine protocol for negotiating privacy protections" (1999, 160), such that a user's computer interacts with Web sites to determine how much and what kind of personal information will be collected. "Only if the machines can agree will the site be able to obtain her personal data," he writes (1999, 160).

Daniel Solove also appeals for change in what he terms "architecture" in treatment of personal data (2004). "The internet itself has a design," he writes, citing Reidenberg and Lessig, "one that affects the way people communicate, the way data is transferred, and the extent to which people can be anonymous" (2004, 98). What he means by "architecture" is very inclusive, and his suggestions go well beyond design of the Internet. They include minimization of data collection by government institutions (2004, 211), enhanced options for consumers to respond to apparent instances of identity theft (2004, 121), and stricter requirements for court orders before government investigators can access personal data held by third parties (2004, 219).

My suggestions here focus much less on Internet design and much more on the vulnerability of personal data to pressures for access once such data are known to be compiled centrally. Much of my argument has to do with change over time. I hold that procedural strictures for treatment of personal information may well protect privacy interests for as long as the political climates prevail under which the strictures are framed. But the sheer knowledge that personal information useful to powerful interests has been compiled centrally itself generates pressure that can undermine such strictures as years pass. By contrast, arrangements that leave personal data either unrecorded or dispersed obviate such pressures.

Thus, my argument is both empirical and normative. Empirically, I aim to show that procedural measures have had mixed success, at best, in stemming individuals' incremental loss of control over "their" information to data-keeping institutions. The role of these measures resembles what students of gender discrimination have

characterized as "managerialization" of the law, with the resulting "protections" to privacy interests often more formal than substantive (Edelman, Fuller, and Mara-Drita 2001). These shortcomings are understandable given the forces driving institutional practice. Much more promising in upholding the values that originally triggered privacy controversies, I hold, are strategies for personal data keeping that simply keep such information beyond the reach of powerful institutions from the outset.

PRIVACY VALUES

Philip Selznick, in a noted statement, characterized law as "a realm of value" (Selznick 1969, 8). His view suggests that law making and enforcing represent efforts to uphold commonly held visions of the good society. This notion fits gracefully in the tradition of Durkheim—particularly, his idea that the law involves not just ground rules for pursuit of *individual* interests but also an expression of *collective* interests. Any shrewd observer will quickly note that the law also plays many other, not necessarily consistent, roles, for example, as a tool for purely sectoral claims or as a way of finessing otherwise troublesome social conflicts. But no one could deny that legislators and courts turn to law making and interpreting in response to public outcries that "something must be done" to uphold widely held sentiments of right and wrong.

Less obvious, but no less important, is the fact that the values to be upheld in these enactments of public righteousness may be far from clear-cut in their implications for action. There is nothing about public opinion that requires that it be consistent; nor is there any rule mandating that the public agree on what practical measures would suffice to uphold values that people consider endangered. Examples to the opposite effect are abundant. Widespread convictions that the state should act to protect the environment—or defend freedom of religion, or uphold family solidarity, or protect the country from foreign dangers—normally mask profound clashes of public sentiment as to what policies in fact would serve such broad values. It is always much easier to agree that "something must be done" to protect widely regarded values than it is to recognize what practices authentically serve those ends. Legislators and other policy makers charged with upholding endangered values often find themselves only too eager to be seen doing something, even when confused or divided about what would constitute success.

Privacy protection provides a salient case in point. Only since the 1960s has institutional use of personal data files been defined as a public issue, that is, as a matter requiring action in legislation and policy. Propelling its emergence in the United States was a steady stream of "horror stories": accounts of lives shattered, reputations trashed, financial well-being undone, and so forth and so on because of high-handed, incompetent, or irresponsible institutional uses of personal data files. Public anxiety over such accounts reached a high point in the Watergate era, with its stories of attempted manipulation of federally held personal data under the Nixon administration. Elected officials felt themselves under strong pressure to "protect privacy" without any unambiguous mandate as to what steps would suffice to this end.

At a minimum, there seems to have been consensus that individuals ought not simply to lose all say over the fate of "their" data once the latter fell into institutional

hands. Beyond this minimalist precept, implications for action were subject to much dispute. As in environmental protection, regulation of financial markets, or defense of family values, measures counted as successful for some sectors of the public may have been tantamount to disaster for others.

Divergences are just as apparent in the realm of theory. Philosophers and legal theorists have struggled over the proper delineation of public and private information since long before institutional appropriation of personal data became a public issue. In the most noted legal statement ever recorded on the subject, Warren and Brandeis famously described privacy as "the right to be let alone" (Warren and Brandeis 1890, 76). They likened invasion of privacy to other forms of assault—hurtful actions that ought to have tort status. But this formulation is enormously problematic. As Diane Zimmerman (1983) and many other commentators have noted, what appears as gratuitous or prurient curiosity to some will predictably appear to others as expression of normal and healthy interest in subjects of wide and legitimate public interest. Thus, legend has it that the original inspiration for the Warren and Brandeis article was Warren's indignation at the intrusive coverage by the popular press into what he considered private social gatherings hosted by his upper-class family. Yet, who can say that public airing of the lifestyles of the wealthy has no legitimate value in civic life?

As Richard Posner and others have argued (Posner 1978), the desire to be left alone—that is, to withhold information about one's self—always competes with the desires of others to inform themselves about those with whom they must deal, live, or entrust their affairs. One's desire to maintain a measure of privacy from, say, one's neighbors is part of endemic tensions with their desire to know whether we are interesting, law abiding, reliable, and cooperative. One's preference for privacy over one's medical history runs in collision with others' interests, ranging from idle curiosity to desire to protect themselves from communicable diseases. The desire of employees and employment applicants to keep certain personal information to themselves is juxtaposed against inevitable interests of employers in knowing whether their staff are reliable, honest, healthy, dependable, and the like.

Communities, groups, and governments universally erect laws and other norms to delineate such claims, but it would be absurd to imagine that the resulting norms follow any unambiguous, bright-line, a priori demarcation between public and private realms. Privacy is, thus, one of what philosophers term "essentially contested concepts" whose implications for practice are bound to be disputed in any real-world setting.

Nowhere are such disputes more charged than in the setting of key interest here: appropriation and use of personal data by government and private institutions as bases for decision making about those concerned. Dealings between individuals and organizations mediated by record systems represent strategic interactions—settings where both parties seek to maximize advantage by controlling what personal data can be mobilized for decision making. Both parties inevitably seek to shape what should be considered germane and legitimate information for collection and use and what should be held private. Even where the decision making in question aims at improving the well-being of individuals, institutions feel constrained to make tough-minded determinations based on personal data. Administrators of Social Security or health insurance benefits, for example, still take recourse to critical decision making, based on details of the "record," to distinguish between those who deserve the benefits they claim and the rest.

In this light, sweeping affirmations of the need "to protect privacy" in institutional use of personal data by themselves afford little practical guidance. How much and what kinds of personal information should an institution be able to collect and use in dealing with any individual? What specific domains of life or forms of data should individuals be able to shield from institutional attention? Not even the most forceful of privacy advocates assert unlimited individual rights to control any and all data about one's self, and, perhaps, not even the most committed defenders of institutional prerogatives would claim that any and all personal information should be grist for the mills of institutional decision making. The emerging law on privacy of institutionally held personal data may indeed be part of what Selznick terms a "realm of value," but affirming the validity of values in such broad terms does not help much in adjudicating specific claims and counterclaims that make up the flux of privacy controversies.

PERSONAL DATA PROTECTION: A GLOBAL CONSENSUS

Privacy protection regarding institutionally held personal data first emerged as a public issue in the United States in the 1960s. Disturbing public revelations of ordinary people's losses of reputation, convenience, and peace of mind through misuse of their records triggered demands for government action. One of the earliest of these controversies focused on consumer credit reporting, culminating in passage of the Fair Credit Reporting Act of 1970. Shortly thereafter, the Watergate controversies brought what appears to have been the high-water mark of public anxiety on the subject to date. One direct result was passage of the Privacy Act of 1974. This law still represents America's broadest national legislation, establishing rights over a wide variety of personal records held by federal agencies. Subsequent privacy legislation in the United States applies to more limited subsets of personal records, for example, those on Americans' video rentals, medical records, or accounts with financial institutions.

Immediately following the first US legislation, nations of northern and western Europe began enacting their own privacy codes. Sweden's first national law came in 1973, West Germany's in 1977, France's in 1978. In a key development in 1995, the European Union adopted its Data Protection Directive, aimed at ensuring standard protections for personal information among all member countries and, not incidentally, at avoiding protectionist restrictions on the flow of such data within Europe. These principles are now binding on all member countries of the European Union, which have been required to "transpose" them into their national codes. The EU Directive has since helped shape privacy codes throughout the globe.

The United States remains an outlier in the content of its privacy codes, notwithstanding its early role. It provides no broad individual rights extending over personal data files held in all private-sector institutions, for example, in contrast to the European Union and most other nations with privacy codes. Nor has the United States ever created a national privacy ombudsman or commissioner, an office mandated in EU law and in nearly all other national privacy codes. Responsibility for enforcement of the Privacy Act of 1974, still America's only legislation establishing rights valid across many different institutional settings, is vested in the Office of Management of Budget.

TABLE 1.
Consensus "Fair Information Principles" for Privacy Codes

An organization (public or private):

1. Must be *accountable* for all the personal information in its possession;
2. Should *identify the purposes* for which the information is processed or before the time of collection;
3. Should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances);
4. Should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes;
5. Should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the *finality* principle);
6. Should *retain* information only as long as necessary;
7. Should ensure the personal information is kept *accurate, complete, and up-to-date*;
8. Should protect personal information with appropriate *security safeguards*;
9. Should be *open* about its policies and practices and maintain no secret information system;
10. Should allow data subjects *access* to their personal information with an ability to amend it if it is inaccurate, incomplete, or obsolete.

Source: Bennett and Raab (2003, 19) (numbers added).

This agency is, of course, an arm of the executive branch, predictably the least privacy-friendly part of government.

Despite this US exceptionalism and other important national differences, privacy codes around the world share a remarkably consistent core of common precepts. One can trace these principles as far back as the "Fair Information Practices" put forward in an influential US government report in 1973 (US Department of Health, Education, and Welfare) and embodied in the Fair Credit Reporting Act of 1970 and Privacy Act of 1974. This rough global consensus has been summarized in a number of writings, including the version by Colin Bennett and Charles Raab (2003) set out in Table 1. The authors identified principles applying both to government and private-sector data keeping.

What essential goods and bads in the use of personal information do these precepts adumbrate? And what specific steps do they suggest as adequate to protect privacy in the institutional use of personal data?

We can start by noting what these principles do *not* intend. Clearly, they do not treat institutional appropriation and use of personal information as activities that simply should never occur, as many codes treat commerce in sex, bodily organs, or recreational drugs. True, the EU Directive does restrain organizations from processing certain forms of data deemed particularly sensitive—namely, those on "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . health or sex life"—but this proscription is immediately undercut by a long list of exceptions and derogations designed to satisfy the interests of many established government and private institutions (EU Directive 95/46/EC: Article 8).

The logic of these principles is overwhelmingly procedural. They take it for granted that organizations have legitimate purposes that make personal data keeping

necessary. They proscribe such data keeping only when it is not truly necessary for the organizations concerned. For data collected consistent with professed institutional purposes, the principles dictate basic ground rules to govern its safekeeping and use, and they aim to secure for individuals some limited access to, and some role in, the uses of data on themselves.

To do this, the principles seek a certain openness in institutional practice. They require government and private record keepers to declare publicly the existence of record systems; they establish people's rights to access and challenge the content and uses made of "their" information. They seek to establish institutional responsibility for the secure, accurate, and lawful operation of the systems, and they aim to curtail uses of personal information that go beyond what is necessary for institutions to accomplish their aims, eliminating uses of personal data that are capricious, unnecessary, or otherwise unrelated to institutional purposes.

All in all, the underlying model is an essentially liberal vision of discerning individual choice. As in other domains of civil society, the individual is pictured as having the right to adjust his or her participation in institutional data-keeping practices, according to judgment of the advantages or disadvantages presented by such participation. One might compare these precepts with measures adopted in response to demands by environmental or nutritional activists to afford consumers more informed choice on the implications of their decisions. Some optimistic observers consider that these fair information practices, as they are often called, resolve the essential value dilemmas posed by institutional record keeping on individuals. If only these principles could be conscientiously applied, they seem to believe, the essential ethical and policy issues would be resolved.

I hold such views myopic. Indeed, they fail to address many of the most compelling and intractable value dilemmas raised by the practices in question.

For one thing, the principles are rarely applied to key personal record-keeping activities carried out by agencies devoted to investigation, law enforcement, espionage, or counterespionage. The organizations involved—including some private-sector bodies, such as insurance investigators—enjoy wide latitude for their work, and they certainly do not expect to make their investigative systems open, accountable to those depicted in them, or limited to publicly stated purposes. The rising importance attributed to the dangers of international terrorism over the last ten years and the increased ease with which state agencies access data held by private-sector institutions make this gap in the applicability of privacy codes hard to ignore. No doubt most informed observers would wish to grant certain investigative agencies the right to work without disclosing their activities fully, at least over certain periods of time. Nevertheless, the idea that these investigative appropriations of personal data should be totally free of constraint from privacy concerns ought to give pause.

The second issue left unaddressed in the consensus principles for fair information practices is even more serious: What personal data should be compiled in the first place? How far should monitoring of individuals' "private" lives through institutional record keeping be expected to reach? What areas of life should we regard as fair game for tracking by government and private-sector organizations? What domains, if any, should be regarded as too intimate, too personal, or too sensitive to permit such scrutiny?

When and how, if ever, should individuals have meaningful options to avoid the attentions of data-gathering institutions? The consensus principles provide no guidance on these points; instead, they take the existence of the systems for granted, focusing instead on establishing ground rules for individuals in their dealings with such systems once they are established.

Yet, if one thing is certain about institutional information gathering on private citizens, it is that this process has long been, and remains, in headlong change. The capacities of organizations of all kinds to create, share, maintain, and use personal information are growing in ways that never cease to astound. Surely, no privacy code can address the values at stake without providing some basis for judgment on how far the underlying social processes should go.

THE EVOLUTION OF INSTITUTIONAL MONITORING

Any such response requires some diagnosis of the origins and long-term directions of such change. Many observers seem to bracket these things simply as the "effects" of "technology," as though computing somehow acted in its own right, independent of human interest or intent. In fact, the beginnings of large-scale institutional monitoring of individual lives and of the privacy controversies surrounding them predate the role of computing. US observers were raising the alarm about consumer credit reporting, for example, well before credit records were widely computerized. Moreover, ongoing innovation fomenting institutional demand for personal information is often as much managerial and strategic as it is strictly technological. Government and private organizations continue to identify new strategies and possibilities for obtaining and exploiting personal data that have long been "there." Overall, the forces propelling such innovation involve complex interactions between new possibilities offered by information technology and the emerging interests of organizations. These interactions take place not just within organizations but also in a kind of information ecology arising out of mutual needs *among* them.

As I have argued elsewhere, institutional exploitation of personal data "*feeds on itself*. The more of it there is, the more there can be" (Rule 2007, 158). Systems and sources that generate bureaucratically usable personal data provide support for other systems that rely on such data, in turn, to make new and valuable determinations about the people depicted in the data. The more independent sources of corroborating data there are on individuals, the less institutions need depend on individuals themselves to supply "their" data.

Thus, institutional monitoring of individuals grows both vertically and horizontally (Rule 2007, 159). In the first sense, personal data systems sprout like plants. They grow in the sheer amount of personal data they embody on each individual. Direct marketing systems accumulate more data, for example, on consumers' choices, or the IRS stores more information on circumstances bearing on individuals' tax liabilities. To extend the metaphor, new shoots are sprouting all the time; that is, repositories of qualitatively new information are coming into existence and they, too, are growing. The last couple of decades have seen the emergence of systems of personal data derived from cell phone use, Web searches, and electronically registered traffic over toll roads,

bridges, and the like—that is, forms of information, and often activities themselves, that formerly did not exist.

No less important are the horizontal processes by which such systems reinforce one another and encourage each other's growth. Government and private organizations are constantly discovering and perfecting new symbioses, by which they exchange crucial personal data to further each other's purposes. Since the 1980s, for example, insurance companies have come to rely on consumer credit ratings as bases for setting rates for insurance coverage. Agencies involved in counterespionage have come to rely on telecommunications records, as further revealed in the exposure of NSA monitoring in December 2005. Social Security records have been mobilized to identify and arrest those working in the United States without the legal right to do so. This list of creative and forceful symbioses among institutions engaged in large-scale tracking and monitoring of individuals could be extended at great length.

Sometimes, the appeal of these symbioses stems from the desire to benefit from the huge sunk costs involved in securing strategic and sensitive information on very large numbers of people. Consider the enormous expense and effort involved over many decades in developing today's systems for reckoning Social Security contributions and Internal Revenue Service (IRS) deductions. From systems that originally touched only a minority of workers, these have grown into vast bureaucratic operations collecting data on virtually every legally employed person. Because it is all but impossible to be legally employed without identifying one's self, one's workplace, and one's income to federal authorities, the capabilities of this combined system are much sought after by other institutional interests. An example is the Federal Parent Locator Service (FPLS), a tracking system dedicated to locating parents who abscond from court-ordered child support obligations. This system mobilizes the resources of the Social Security Administration (SSA) and other federal agencies to determine the whereabouts of absconding parents and enforce child-support requirements. Should someone in this position seek to flee the country to avoid such obligations, the FPLS also makes it possible to withdraw the would-be fugitive's passport.

The attractiveness of the symbiosis supporting the FPLS ultimately depends on the systematic legal compulsion requiring individuals and employers to submit to SSA and IRS reporting. Other symbioses derive their appeal to institutions from new capabilities to compile personal data whose dispersion and obscurity formerly made such data practically inaccessible. The rise of mobile telephony, for example, has created vast personal data resources that simply did not exist before, not only identifying the parties users communicate with but also fixing their whereabouts. Such data are of intense interest to prosecutors, national security investigators, and litigants in divorce actions and other civil cases. All providers of mobile phone services must devote significant resources to responding to the predictable flow of demands for access to such data. The net result is to extend the gaze of institutional record keeping to new domains of hitherto-private life.

Consider the recent evolution in the structuring of personal data held by US courts and public record offices. Potentially volatile personal information on matters ranging from court actions to tax liens, property transactions, marriage and divorce, and residential addresses has long been held in countless dispersed locations, most of

it officially public but difficult to track down and assemble. In the past, seekers of such information had to bear the considerable costs of guessing where such data might be held and sending representatives to obtain them. But in recent decades, record offices have increasingly computerized their operations, triggering a new industry devoted to harvesting the data en masse and retailing it in reports to litigators, prosecutors, or those with other bases for curiosity about others. Recent display ads in major newspapers advertise such reports, for example, to parents anxious about the backgrounds of their daughters' live-in boyfriends. Among the major purchasers of such reports are government agencies, according to privacy researcher Evan Hendricks (Hendricks 2006).

These horizontal exchanges of personal data between often quite different kinds of institutions ultimately have a single rationale. They enable institutions engaged in strategic interactions with individuals to develop strategically useful personal data from sources independent of the persons concerned. That is, they make it possible for the institutions to forestall censorship, editing, or other shaping of the information in question by individuals acting in their own strategic interests.

The logic of such symbioses runs in collision against some of the consensus privacy principles distilled by Bennett and Raab—notably, the importance of collecting and using personal data only with the knowledge and consent of the individual concerned and of identifying the purposes of such collection at or before the time of collection. Such precepts, if followed, would certainly be privacy friendly. But in fact, that very respect for the interest of individuals in controlling the flow of information about themselves flies in the face of the institutional interests driving expansion of institutional record keeping.

Some institutional efforts to bypass individuals in order to assemble strategically crucial personal information could well be called conspiratorial. But no conspiracy theory is necessary to explain the pervasive trend toward symbiosis and mutual support across virtually all domains of personal record keeping. The need for independent, credible, outside sources of personal data stems from structural constraints on the organizations in question. They see their missions, after all, as making and enforcing the "best" possible decisions about the millions of people with whom they deal. In their strategic assessment, by far the best way of accomplishing this is to avoid, as much as possible, relying directly on the persons concerned for information about themselves, and in the changeful information environment of the last few decades, every year seems to yield new sources of personal information on which to rely. The knitting together of such data sources across institutional lines multiplies the effects of such innovations and gives the entire process a life of its own, independent of any individual's choice as to whether or not to participate.

The net effect is to render operations of the institutions in question more efficient—more profitable in the case of businesses, more cost effective or authoritative in the case of government agencies—but no one can claim that these trends are friendly to privacy. The logic—more precisely, sociologic—behind the evolution of these practices over recent decades has been to remove more and more personal information from the direct control of those whose lives are depicted by it. Instead, institutions increasingly share crucial personal data among themselves, often without the permission or even awareness of the individuals concerned.

PRIVACY CODES IN COLLISION WITH DEMAND FOR PERSONAL DATA

The consensus precepts that have shaped global privacy codes reflect, I have argued, an essentially liberal model of individual choice and informed discretion. Law and policy should ensure that people are informed of the workings of institutional record systems, in this view, and people should exercise informed choice over release of information about themselves. Perhaps the strongest expression of this view comes in the "finality principle"—the fifth of the precepts enumerated by Bennett and Raab—holding that organizations "should not use or disclose personal information for purposes other than those identified, except with the consent of the individual."

But I have argued that it is always attractive to organizations, and ever more feasible, to draw personal information that they feel they require from institutional sources independent of the individual. Thus, we need to inquire into the results of direct confrontations between procedural limits on such access and the force of institutional demands.

The brief answer is that procedural guarantees often do not fare well in such confrontations.

Consider an early and telling case, America's Privacy Act of 1974. This legislation, passed during the Watergate period at the height of privacy anxiety, had among its aims to restrict the flow of personal information provided to one federal agency from automatic release to other agencies without permission from the individual. In the language of the law, disclosure of such records is proscribed without the written request of "the individual to whom the record pertains." But the Act contains an exception permitting disclosure for what it terms "routine uses," a loophole widely exploited by federal agencies so as to allow sharing of personal data virtually whenever bureaucratically expedient. As Paul Schwartz has pointed out, the Privacy Act "places definite statutory limitation on the application of the exemption" including "'compatibility'" of the use in question, understood as "a significant degree of convergence and a concrete relationship between the purpose for which the information was gathered and its application." "This language," Schwartz continues, "places an important substantive limitation on the notion of a routine use, which, unfortunately, agencies have generally ignored" (1995, 16).

Nearly every country that has framed a strong privacy code can report examples of such slippage. Restrictions on access to personal data are particularly vulnerable when they appear to stand in the way of state revenue collection or cost-cutting measures. In France, legislation in 1978 established a particularly strong privacy code and created that country's privacy commission, the National Committee on Information-Processing and Liberty (CNIL). For years, the CNIL successfully opposed attempts by the tax administration to obtain, for tax-enforcement purposes, data provided by citizens to other state agencies, including medical services. But in the 1990s, new legislation and court decisions began to erode these manifestations of what Bennett and Raab term "the finality principle." These changes have made it possible, since 1998, for tax authorities to obtain citizens' current addresses from the national medical care system, an invaluable advantage in that most people are more interested in staying in touch with the sources of their medical care than with tax collectors. In 2004, Parliament stripped the CNIL of powers established in 1978 to block legislation that it deemed to infringe on privacy.

In virtually every country, changed political climates following the September 11 attacks have set the stage for undermining or eliminating privacy guarantees. A salient case in point is telecommunications data—notably, the records of telephone and e-mail connections, identifying both the parties to communications, their durations, and, with the advent of mobile telephony, the locations of the parties. Prior to 9/11, largely out of privacy concerns, the European Union mandated relatively short retention periods for such data. But under pressure from the United States and the United Kingdom, the European Union in 2006 adopted a directive extending these limits to as much as two years (Brown 2009, 48; see also http://en.wikipedia.org/wiki/Telecommunications_data_retention). The terrorist attacks of 2001 provided the impetus for this extension, but data so retained are also available for investigative uses unrelated to terrorism.

The leveraging of palpable public anxieties over potential terrorist attack as a means for undoing limitations on investigative access to personal data unrelated to terrorism is widespread. Canada's Public Safety Act (passed in 2004) amended that country's private-sector privacy act to authorize a range of private-sector institutions to collect and retain personal data for disclosure for national security purposes. This same legislation enabled government investigators to obtain passenger data from airlines without court warrant. Privacy Commissioner Jennifer Stoddard might have been speaking for her counterparts around the world, when she objected.

> It may well be that few people would question [such measures] . . . given the risks that terrorists pose to air transport. But the use of this information is not confined to the purposes of anti-terrorism and transportation safety. The Public Safety Act also allows the information to be used to identify passengers for whom there are outstanding warrants for a wide range of ordinary criminal offenses. In other words, the machinery of anti-terrorism is used to nourish the needs of ordinary law enforcement, lowering the standard ordinarily demanded of law-enforcement authorities. (2005)

In Canada, as in most countries, such objections have not prevailed.

Far from being driven by technology, government interests in this country have successfully intervened to shape technological change so as to maximize their access to personal information. Consider the advent of fiber optics transmission as a medium for telecommunications lines. Like other recent innovations in information technology, this one is in one sense inherently more privacy friendly than the ones it replaces. The FBI has accordingly required telecommunications companies—a highly regulated industry—to build in wiretap-friendly capabilities, at their own expense, so as to preserve the ease of FBI eavesdropping.

Similar patterns have prevailed regarding cell phone technologies. As communications analyst David Phillips has written:

> [The FBI] required specific change to the telecommunications system. These changes were justified in part by the claim that since the address of wired telephones had always been available under similar orders, then, in order to maintain the status quo, the location of wireless phones should also be available. But in fact the legal availability of the address of wired lines was initially justified by the technical "accessibility" to the phone company of its own service records. . . . Because the

> location of wired phones was legally accessible to police, then the location of wireless phones should be available, as well, even if that meant changing the phone system in order to make that information "readily available." (2004, 57)

In short, when political forces favoring appropriation of personal data are in the ascent, they may alter the course of technological change itself to achieve their ends.

In the private sector, privacy codes often stress individual consent to institutional collection and use of personal data. But notions of consent can be extremely elastic, especially where relations between individual and institutional parties are markedly unequal. If providing one's "consent" to having one's data collected represents an indispensable condition for having a bank account, credit card, or insurance coverage, the term loses much of its meaning.

Here, legal interpretations of consent requirements are all-important. EU law is widely understood to block "secondary release" of personal information that businesses collect in commercial transactions. Thus, magazines, for example, may not sell, trade, or give away their subscribers' names and addresses without the latter's consent. In many EU countries, businesses are prohibited from sharing account data with credit-reporting agencies on this same principle. In the United Kingdom, however, aggressive, US-style credit reporting was established before the EU Privacy Directive came into effect. Actually granting consumers meaningful choice as to whether data from their accounts should be released to credit-reporting agencies would represent a blow to the vital interests of this industry. Accordingly, British consumers are required to sign consent statements as conditions for opening credit accounts, authorizing future reporting of data from the accounts that they are seeking to open.

Here and there, policy makers have acknowledged the flimsiness of consent secured under such circumstances. Canada's private-sector privacy law adopted in 2000, for example, contains a potentially forceful stipulation that Canadian companies may not require consumers to yield their personal information in exchange for any transaction or service, except where necessary to "fulfill the explicitly specified, and legitimate purposes" for which it is collected. Thus, credit grantors could reasonably require credit applicants to allow reports to be drawn on their *past* credit histories. But the law should enable consumers to decline to have reports of their subsequent credit use automatically routed to credit-reporting agencies, along the US model followed by the Canadian industry.

This privacy-friendly implication of the law has never been enforced. Canadian consumers continue to sign statements when applying for credit that are interpreted as permitting such downstream reporting. These routine privacy incursions entailed in "positive reporting"—to use the industry euphemism for automatic monitoring of all consumers' accounts without their consent—are of course a gold mine for the industry. They guarantee that the key "raw material" of this industry will continue to be made available without cost and without any danger of interruption from the people whose lives are being monitored. No doubt aware of the pressures that any interference with these practices would generate, Canada's Information and Privacy Commission has not challenged them.

More generally, procedural guarantees embodied in privacy codes depend for their efficacy on the larger political climate of their operation. Consider the US Patriot Act.

Fueling its passage in the immediate wake of the September 11 attacks, of course, was vast public anxiety about potential further attacks and other forms of possible subversion. According to a number of informed commentators, the detail of the changes that it afforded in government access to institutional records on individuals had been in preparation long before those attacks. Crucial among its many complex provisions is the access it affords state investigators to personal information held in private-sector sources without court warrant or indeed any form of public notification. Those served with demands for personal data need not be the persons suspected of subversive actions or thoughts but, instead, others who hold data on such people. In the cases that have attracted most comment, these may be librarians and booksellers holding records of patrons' choices of reading matter. But the sources may also include landlords, service providers, or any individual or institution that accumulates data or documents on the person concerned. In the environment we increasingly inhabit, this amounts to a lot of different sources.

Not only did the original Patriot Act free investigators from court supervision, it also enjoined those required to produce personal information under National Security Letters from disclosing the requirement. This stipulation shields the workings of the Act, and the invasions of privacy it fosters, from public attention and debate. A few recipients of the letters risked prosecution by going public with their objections to what they have been required to do. A salient case is George Christian, the Connecticut librarian who in 2005 refused to cooperate with government demands for readers' records and publicly disclosed receipt of the National Security Letter containing these demands. But, apart from a few such exemplary cases, we do not know the true extent of data gathering carried out under Patriot Act provisions.

I do not hold that procedural guarantees, such as those embodied in the consensus principles, are without value. When conscientiously followed, they can make it much easier for individuals to understand the existence and uses of institutional records about themselves and, at best, to challenge uses proscribed by the principles. What these principles do *not* afford, however, is any convincing long-term check on the growth of the monitoring of everyday life by government and private institutions. The problem is not just that they provide no guidance as to what forms of monitoring of once-private domains of life should be held excessive, even when they are expedient. It is that procedural limitations on what institutions may do with personal data compilations are subject to change, and the secular trend of historic change in this connection appears to be toward erosion of privacy guarantees.

True, the examples of such erosion given above are just that, examples. They do not represent results of any sort of representative sampling of instances of change in once-protected systems of personal data collection. As far as I know, no such sampling universe exists, but the force of these examples lies in the apparent absence of counterexamples. It is simply hard to think of major cases where privacy concerns have led to curtailment of established systems of compiling and using personal data, once such systems are up and running. One exception here is data systems maintained by authoritarian regimes that actually fell, as in the cases of Hungary and South Korea (Szekely 2008; Park 2008). But short of such changes in basic social constitutions, systems of institutional record keeping on individuals seem to enjoy something akin to eternal life. The result is what privacy advocates often refer to as a "ratchet effect" in the growth of

such systems. From the standpoint of privacy values, change in the scope of their use rarely appears to be change for the better.

THE LIMITS OF PROCEDURAL SAFEGUARDS

Consider a proposed procedural solution to privacy dilemmas of much interest in the 1990s. This was the controversy over US government plans for "key escrow" access to encrypted telephone and e-mail communications. In a privacy-friendly technology innovation, cryptographers had developed programs for encrypting such messages that proved highly effective and inexpensive. Private individuals and companies could thus readily shield their communications from wiretapping. This development triggered alarm among law-enforcement and state security agencies, which feared that eavesdropping on all sorts of criminal and subversive activity could become impossible. In response, the US government proposed to make encryption widely available to private users but to retain an "escrow key" that would enable state agencies to monitor such communications when they deemed it necessary. Proponents claimed that this system would ensure all users that they had nothing to fear, if they had nothing to hide, while ensuring government agencies the prerogative of accessing communications that they felt it necessary to monitor.

To the predictable complaints that such a step would grant government excessive privacy eroding power, proponents of key escrow advanced essentially procedural arguments. The prerogatives of surveillance conferred by such an arrangement would be constrained by rigorous institutional safeguards. The escrow "key"—that is, the technology required to decode private messages at government behest—would be devolved into two parts, each held by a separate and highly trustworthy party. To mobilize the key, in the words of communitarian privacy critic Amitai Etzioni, very special steps would be necessary:

> this step would be activated only after independent judicial approval. The government would have to make a specific case that there was sufficient reason to suspect that criminal activities had taken place, and that evidence was likely to be found in encrypted communications. Once a judge was convinced of the validity of these claims, he or she would authorize the issuance of a warrant to decipher a specific set or flow of communications. In short, decryption would be governed by the same procedural safeguards as wiretaps. (1999, 91–92)

Then he adds:

> There are some exceptional conditions—for instance, a national emergency—under which warrants are not required and other judicial procedures are used for the tapping of telephones. These exceptions might apply to decryption as well, but because they are just that—very exceptional—they are not discussed here. (1999, 92)

In the end, the US government concluded that it would not be possible to stop private parties in this country from availing themselves of encryption software, and the

ambitious key escrow scheme was abandoned. Nevertheless, it is instructive to consider the logic of the proposal and the larger political forces that would have shaped its implementation had it lived.

Etzioni wrote the above remarks in the late 1990s, about three years before the September 11 attacks that upended the US political climate and led to the hasty passage of the Patriot Act. This mentality of the post-9/11 period exemplified what Etzioni describes above as "a national emergency . . . very exceptional" that would justify abandonment of the warrant requirement that he envisaged. As noted above, one broad effect of the Patriot Act was to sweep away restraints on collection of personal information in the private sector.

The trouble is that the "national emergency" that Patriot Act supporters invoked for its justification has proved to be open-ended. The Act, slightly modified, remains in effect. Had key escrow been enacted in the 1990s, it would most likely have had its warrant requirements bypassed by the Patriot Act. Given the 2005 revelations of large-scale warrantless monitoring of Americans' telecommunications by the National Security Agency, it is hard to doubt that state authorities would have stopped at decrypting telephone and e-mail content.

We still do not know, at the time of this writing, the extent of the NSA surveillance, but we do know something about the mindset of those shaping US policies at the time—to wit, that virtually any available resource for waging the "war on terror" declared by the Bush administration was fair game. In this light, it would have been unwise to place much faith in the durability of the procedural guarantees proposed by Etzioni to restrict indiscriminate access to Americans' communications.

The aim here is not to recapitulate old debates on the virtues of the now-defunct key escrow plan or of efforts to ensure private interests the ability to keep communications secret. My point instead is to insist that the most earnest of bona fides in creating procedural protections for personal data systems do not necessarily withstand changes in political climate.

In Congressional testimony in 1931, long before his rise to the status of national law enforcement icon, J. Edgar Hoover chose strong words to express his objections to wiretapping.

> We have a very definite rule in the bureau that any employee engaged in wiretapping will be dismissed from the services of the bureau . . . While it may not be illegal, I think it is unethical, and it is not permitted under the regulations by the Attorney General. (Quoted in Seipp 1978, 108)

But political times change, whereas capabilities conferred by the amassing of personal information represent enduring temptations. The considerable sunk costs required to bring such systems into existence greatly undermine efforts to dismantle them when political climates moderate. It will thus be instructive to see what fate the Obama administration has in store for the domestic wiretapping capabilities mobilized during the George W. Bush years. Even if the warrantless uses of NSA surveillance capabilities revealed in December 2005 are stopped, it is hard to imagine that the capabilities involved will be scrapped.

PRIVACY-FRIENDLY STRATEGIES

Reviewing the evolution of institutional use of personal information over recent decades, privacy advocates often find it difficult to remain optimistic. Too many earnest efforts to place legal and other procedural limits on the use of such data, once collected, have come to grief. But not all approaches to privacy protection run the same risks of being undermined by changing political climates. Stronger strategies target patterns of distribution and retention of personal information—that is, constraints over what information is retained in the first place and what interested parties can discover about its existence and whereabouts.

Consider some significant cross-national differences in the privacy friendliness of consumer credit reporting. Virtually all prosperous market societies have developed business practices enabling consumers to make purchases on the promise of subsequent payment, through credit cards, mortgages, charge accounts with retailers, or consumer loans. In virtually every case, retailers and financial institutions have developed mechanisms to flag consumers who are failing to meet concomitant repayment obligations. The strategies of personal information compilation embodied by these systems vary widely. Often, the systems begin as simple sharing of data on "bad" accounts among creditors in an effort to protect businesses from taking on new debt from those who have failed to repay elsewhere. But over recent decades, especially in the United States, many systems have grown much more sophisticated and aggressive in their use of personal data.

Beginning in the first half of the twentieth century, the US credit-reporting industry developed what it has subsequently marketed as "positive credit reporting." This is the practice of collecting and reporting data not only on "bad" credit accounts but also on *all* accounts held by any given consumer. This practice, subsequently exported by the US industry to Canada, the United Kingdom, and other countries, provides an invaluable advantage to prospective creditors: it enables them to identify credit applicants who are "loaded up," in the jargon of the industry—that is, so heavily indebted as to be likely to experience difficulty in making new payments. Such knowledge makes it possible for would-be creditors to decline new business from applicants who appear excessively risky or to charge higher interest rates and fees to these applicants. In recent US practice, the most sophisticated versions of these policies enable credit card companies and other credit grantors to raise interest rates charged on long-established accounts simply on the report of mounting credit use on other accounts, even when *none* of a given consumer's accounts is delinquent.

The industry's publicly stated rationale for such practices is that higher levels of indebtedness in any one of a consumer's accounts signals heightened risk for all that individual's creditors—risk that is properly compensated by charging the consumer more on his or her other accounts. A more skeptical interpretation is that consumers, reaching the limits of their ability to borrow on one or more account, will be less able to take their business elsewhere when faced with a rise in the rates they are paying.

This system cannot be described as privacy friendly. The fact that any recipient of credit reports can know the full state of any consumer's credit use in *all* his or her accounts, regardless of whether any account is in default, places individual consumers at a disadvantage. Were the consumer in control of his or her information in this strategic

interaction, he or she would certainly choose to supply to credit grantors only that information that appeared advantageous to share. Credit grantors resist such arrangements in that they prevent the credit grantors from shaping the terms offered to customers in light of the latter's total credit use.

In some consumer societies, prevailing arrangements for sharing consumer credit information are far more favorable to the consumer. In France and Australia, for example, the balance of strategic advantage between credit grantors and consumers is distinctly different. Laws in these countries generally do not permit central compilation of data from consumers' accounts, except for accounts that have gone delinquent. The result in both countries is that consumers accumulate little or no "credit record," so long as no one account goes unpaid beyond a certain legally specified period. At that point, record of the delinquency becomes available to any credit grantor. In France, one repercussion of such listing is that credit grantors contracting new debt with consumers already listed can expect great difficulty from the authorities in enforcing payment for subsequent delinquencies.

By any standard, the arrangements governing credit information prevailing in France and Australia are far more privacy friendly than in countries following the US model. In the former two countries, organizations considering consumers' applications for credit must regard no news as good news or, at least, as the best news available, under the circumstances. It is not just that the US system involves compiling more personal information in more centralized locations; perhaps even more important, in Australia and France consumers are normally the only parties who know the location of personal information on themselves that might be sought by creditors. No aggressive loan company or retail merchant can demand that they grant "consent" to checking data that the consumer may prefer not to provide, as there is no way of knowing where to look for such data unless, of course, the consumer is in default. There is nothing to prevent consumers from furnishing data that they may consider favorable in their applications—evidence of other credit accounts paid on time, for example, or data on income sources or assets—but the sheer dispersion of such information leaves the consumer considerable discretion over when and where such data are shared. Such discretion is a key element of privacy.

Such strategies for compiling personal information matter enormously, then, because of their effects on the balance of advantage and disadvantage in strategic interactions between individual and institutional parties. No one should be surprised that sophisticated actors go to great lengths to manipulate such arrangements to their advantage.

Consider life insurance. Sellers of any form of insurance would, of course, prefer to sell only to buyers who will never make claims, just as buyers would prefer never to take out insurance except when certain that someone would collect. Life insurance companies accordingly require applicants for large policies to undergo medical examinations, some of which turn up information that leads companies to deny coverage or require higher premiums. Under these circumstances, those seeking coverage are inevitably tempted to shop for coverage with other companies, perhaps undergoing other medical exams in hopes that subsequent reports will be more favorable. The industry, for its part, is eager to ensure that unfavorable information uncovered in one application not be lost to other companies that may later consider the same applicant.

To this end, the US life insurance industry created MIB, an organization dedicated to centralizing reports on results of insurance-related medical examinations. Its purpose is to support strategies in compilation of personal information favorable to industry interests. In this instance, the aim is to ensure that information revealing risks to life expectancy, once available to any company, remains available to others. Participating companies forward information on risk-related conditions, ranging from diseases to life-style matters like homosexuality, obtained in the course of insurance applications to MIB. Much as in "positive" credit reporting, MIB in turn disseminates these data on request to other companies considering life insurance applications. The wisdom of the arrangements, from the standpoint of the industry, is obvious as is the privacy interest of insurance applicants in securing for themselves a "second chance" after having had their applications denied or being quoted high premiums in earlier efforts to obtain coverage.

As in consumer credit reporting, the strategy pursued by MIB is a purposeful creation, but elsewhere the balance of advantage between disclosure and withholding of personal information is shaped by circumstances that seem to have emerged through unplanned interactions of self-interested parties. Consider another "trunk line" of personal information on Americans that today is widely accessed by many public and private interests—IRS returns. These compilations of strategically valuable personal data obviously came into existence as a means of enforcing federal government claims for payment of tax on income. The original rationale was to verify the taxpayer's obligations—documentation that, with the growing complexity of tax eligibility, has come to afford an increasingly comprehensive view of individual taxpayers' lives. Enhancing the value of this information is the fact that it is compiled under legal compulsion, with strong disincentives against individual censorship. It was all but inevitable that such compilations would draw attention from resourceful institutions for use in managing their dealings with the persons concerned.

Within the state, additional claims for access to these data—that is, claims from agencies having nothing directly to do with taxation—come from many sources. An example is the Federal Parent Locator Service, discussed above, which mobilizes IRS files and accounts to help custodial parents enforce child-support obligations.

In the private sector, we see a superficially different, but no more privacy-friendly, dynamic at work. For the most part, Americans are not legally required to supply their tax returns to private-sector organizations, but one may choose to do so and the strategic position of the data subject renders such choice little more than a formality. "Requests" for provision of tax returns are routinely made to applicants for services and relationships ranging from home loans to college students' financial aid applications to employment. One may decline in any of these cases, but the result is predictable.

Think how different the situation would be had the US tax system evolved differently: if income taxation had never been instituted or if tax calculation required less detailed personal data. The array of information now reflecting taxpayers' total obligations would remain dispersed and extremely difficult to locate. But US tax law has the potent effect of requiring taxpayers to assemble such information and attest to its accuracy under legal compulsion. For most adults in the United States, denying the existence of one's return is simply not plausible. The net result is to create a kind of comprehensive self-portrait, comparable in form to every other

taxpayer's, that is irresistibly attractive to countless public and private interests. Refusing to provide the data compiled in tax returns may be legal, but it is apt to be strategically impossible.

A quite different chain of events recently shifted the equation of strategic advantage in one rather less important form of personal data use in a more privacy-friendly direction. In 2008, ETS revised its policies so as to allow high school students to take the crucial SAT examinations a number of times, while withholding the results from transmission to colleges at their discretion. This resulting change in information availability obviously enhances the strategic position of students. College admissions officers generally express dissatisfaction with the change, preferring to see all results of all tests taken by each applicant when making their decisions (Rimer 2008).

The ETS policy change apparently stemmed from its desire to sell more testing services. Whatever the reasons, the decision spelled a shift in advantage from institutions to students able to retake the tests a number of times. In the larger privacy assessment, one should remember that while multiple test results may now be concealed from college admissions officers, they are still widely understood to be compiled in a single place. Should these results come under subpoena, for example, the fact that all such scores are held under the test taker's name by ETS would make it impossible to resist granting access.

Knowing where crucial data are to be found is decisive in strategic interactions, such as those depicted here. The fact that personal information exists *someplace* in itself has little bearing on the privacy interests of the individual concerned. What matters most is the knowledge that such data are compiled in predictable and accessible locations. Such knowledge, once available to institutions, is apt to leave individuals with no choice but to grant "consent" to such in exchange for valued services. Government agencies, facing what they consider overriding considerations of preventing terrorist attack, maximizing tax revenues, or enforcing justice, will not find it easy to uphold the "finality" principle by restricting their uses of personal data to purposes for which they were originally provided.

FUTURE DEVELOPMENTS

What new pressures on privacy can we expect to arise from strategies of personal data management likely to emerge in the near future?

One salient case in point is US efforts to reorganize medical data. It has long been noted that Americans' medical histories—their encounters with health care providers, tests done and their results, diagnoses received, treatments administered, and so forth—are currently as dispersed and disorganized as US medical care itself. Many unfortunate consequences ensue. Patients requiring urgent attention, and often not only these patients, receive inappropriate interventions, with resulting costs in terms of money, time, suffering, and life itself. Centralizing *all* medical data on *all* medical encounters for *all* patients, observers have long noted, could potentially result in vast simplification and savings. An added attraction of such centralization would be vast new research possibilities for tracing the origins of diseases and the effectiveness of treatments—a database of proportions that would make any researcher envious.

Thus, one of the rare policy innovations advocated by both the Bush and Obama administrations is creation of such a fully centralized, comprehensive compilation. Every American would have all his or her medical data available in a single place, within a single, comprehensive, centralized system. Inevitably, such a project has spurred a good deal of concern about privacy, understood mainly as the danger of unauthorized access to the system. Elaborate assurances have been provided that patient data would be released only to those parties legally authorized to have them and not to the casually curious, potential marketers of products and services, and the like.

The more compelling questions are who will be considered an "authorized" interest, and whether any system of this new form will afford meaningful individual choice over the fate of medical data.

Presumably, any medical care provider will ipso facto have the right to access the data held in patients' files as a matter of course—at least if the provider is willing to attest that the patient is presently or potentially under its care. This fact in itself has a bearing on privacy values. Today, patients have the effective option of keeping certain information "off the record" by seeking care, testing, or advice from a source other than their ordinary caregiver. Thus, someone who suspects that he or she might be at risk of infection from HIV or some other sexually transmitted disease may not even want to have it on record that he or she had had the test done, regardless of the outcome. Presumably, it will be far more difficult, if possible at all, to keep such information off one's records in a centralized system.

Then there are the predictable demands for official sharing of these rich data sources. Within the federal government, many agencies administer policies that are predicated in some degree on the health of the individuals with whom they deal. Those claiming deductions from their federal income taxes because of extraordinary medical expenses, to take one example, will certainly be expected to allow verification of these expenses via a centralized system. The same would hold for those claiming disability support from Social Security. Agencies responsible for security clearances, antiterrorist operations, and a host of other state-sponsored investigations would certainly want to claim legitimate and routine access to the centralized medical files.

Further, the contents of centralized medical records would presumably be as subject to subpoena as conventional records of the same kind but far more easily located. Since they would at a very minimum establish patients' whereabouts at the times they seek medical care, they will presumably be sought in civil and criminal cases for this reason alone. Like records of cell phone use, they would be much sought after in divorce actions. Criminal investigators would want to troll data that yield DNA identifications and, of course, medical records will detail where such data—in the form of lab samples, for example—are apt to be found. It is hard to imagine that government investigators in the national security arena will be denied access in any case where they are willing to attest that their need to know is part of their interest in protecting national security. Then there will be a vast array of nongovernment interests unlikely to gain access to the vital data held in these records through court order but, nonetheless, forceful in their demands. Prospective or current employers, insurers, credit grantors, and many other private-sector interests will feel themselves vitally concerned with the future health of Americans and hence entitled to know about their medical pasts. Individual Americans will surely be asked to "choose" to release their comprehensive medical files to these

interests, much as Americans are now asked to release their IRS returns for similar purposes. Refusal of such requests will presumably endanger consideration of whatever application triggers the inquiry.

Some planners may propose to circumvent these privacy invading possibilities by prohibiting release of patients' records to private parties, except under a court order, but the promise of any such strategy is apt to be deceptive. Individual patients presumably would retain the option of obtaining copies of their own records. Failing to provide this option would appear to violate a principle held dear by privacy advocates—that of ensuring a degree of control over one's own information. Nevertheless, so long as it is established that *all* of *any* patient's medical information is compiled in a single place, patient control over such data would simply shift the focus of pressure from the institution keeping the data to the patient. Individuals would face the same sorts of dilemmas they now encounter with their IRS returns. The very fact of their existence would generate pressure for their disclosure. Resistance to such pressure would be formally possible but likely to stop any application to an interested institution in its tracks.

One could imagine tinkering with patients' control over the composition of their medical files in an effort to strengthen their privacy interests. One could, in principle, offer patients the right to censor their records, that is, to keep what they might imagine to be especially sensitive data "off the record," but such a prerogative would presumably be opposed by the institutional interests backing the centralization. After all, for them the idea of compiling *all* patient data is a basic element of the appeal of the project.

A variation on this idea would enable patients somehow to censor the data released to outside institutions, for example, would-be providers of medical or life insurance. But for these interests, engaged as they are in strategic interactions with the subjects of the data, such censorship possibilities would deprive the data in question of the very appeal that draw the institutions to them. Then there would be the question of whether outside "consumers" of the potentially censored reports would be able to inform themselves as to whether the patient had exercised his or her hypothetical rights of censorship. Any record of the exercise of such rights would obviously vitiate the value of access for outside institutions and sharpen their demands for direct and uncensored access.

Medical histories are just one form of personal data that, once known to be compiled centrally, generate vast pressures for access. Another is DNA profiles. In Britain, the Home Office and police are orchestrating efforts to create a massive DNA database to aid in crime fighting. Some 4.5 million genetic samples are already included. Under one proposal, collection of DNA signatures should begin in school, at least for children deemed at high risk for future criminal activity (Townsend and Asthana 2008).

The British policy of collecting DNA samples from those arrested but not convicted has recently been ruled a human rights violation by the European Court of Human Rights (Greene 2008). Nevertheless, law-enforcement officials in the United States are pursuing similar plans; the FBI's DNA database currently contains some 6.7 million profiles, not all from convicted criminals (Moore 2009). If successful, projects like these could obviously culminate in situations where law-enforcement authorities retain DNA profiles on virtually all residents of their countries. No doubt many people

would draw comfort from such a development, which after all would increase likelihood of clearing many unsolved crimes and of tracing and identifying missing persons. But the prospect of DNA banking alarms privacy advocates, not least because of the powers it would confer on whoever controls DNA compendia in the future.

Such control would make it possible, for example, for investigators to identify those present at any site of interest where there were traces of blood, saliva, dandruff, or other bodily products left at the scene. Further anxieties focus on potential uses of DNA information to predict diseases and other medical conditions, including those not known even to the individual, at least at the moment when DNA is sampled. Insights and advantages afforded by such knowledge apply not only to those whose DNA is sampled but also to their descendants and blood relatives. Here, as elsewhere, bringing many people's personal data together in a single place is bound to generate pressures to share and exploit such data that cannot necessarily be anticipated when the fateful decisions are first made.

Still another form of personal information that is a candidate for centralized compilation is that on search engine requests. Indeed, one can think of the comprehensive record of any Internet user's search engine requests as a cognitive analogue to his or her DNA. It is widely acknowledged that many institutions now collect records of users' search requests, presumably with purely commercial purposes in mind. But these same databases could also serve many other interests—most notably, government interests in identifying and tracking lawbreakers or subversives.

For any institutional user, whether governmental or private, the value of search engine profiles is apt to lie simply in their associations. If it is shown that users with specific patterns of Internet use are particularly susceptible to appeals to specific products or services—or that they are especially likely to be sympathetic to what are considered subversive or illegal activities—the bases of these associations matter little. Advertisers have long sought such associations among consumption habits in the hopes of converting known consumers of certain items into future consumers of other things. Such thinking could have underlain the (still unknown) rationale for the warrantless NSA surveillance of Americans' telecommunications uses as revealed in December 2005. Perhaps the aim was to identify patterns of communication among ordinary Americans that paralleled the established patterns of known terrorists.

In all these cases, the sheer compilation of personal data in sites whose existence is widely known creates intense pressures to access such data. Such pressures are bound to grow as institutions become more and more adept at associating key data on individuals with decisions that the institutions wish to implement regarding those individuals.

CONCLUSION

A much-noted essay in technology studies bears the title "Do Artifacts Have Politics?" (Winner 1980). The author answers his own question emphatically in the affirmative. Tools and other instrumentalities created to manipulate the world to human ends always bear the mark of some *particular* ends, values, or interests over others.

Winner dwells on the career of Robert Moses, the mid-twentieth-century master planner of transport and urban spaces in greater New York. Moses's car-friendly vision famously included a parkway system radiating from New York City into the surrounding countryside, designed to provide city dwellers access to the beaches of Long Island and recreation spots of the Hudson Valley.

As Robert Caro's biography points out, Moses intended these parkways exclusively for travelers with their own cars, not for the less affluent New Yorkers who might seek to reach leisure destinations by bus. To settle the point, Moses ensured that the overpasses on his parkways were designed with clearances too low to permit buses to pass. These aesthetically pleasing low bridges continue to grace New York's parkway system to this day, just as they continue to preclude use by buses. As Winner underlines, the politics "congealed" in the parkway system were and remain decidedly antipopulist, reflecting those of their key creator and his supporters.

Strategies for institutional use of personal data, like those for public transit, embody the values—or the politics, in Winner's terms—of those who sponsor them. They reflect assumptions not only about immediate needs, uses, and abuses of personal information, but also about contingencies and interests that might shape future uses.

Seen in this light, strategies that stress long-term preservation of data, its effective centralization or networking, or its ease of access favor potentially privacy-unfriendly interests. As in Amitai Etzioni's exhortation to incorporate encryption-breaking tools in personal and corporate communications systems, they protect institutional interests just in case expedient measures should be necessary in the future. Similar values are "congealed" (to use Winner's term) in FBI-mandated requirements to alter technologies of fiber-optic telecommunications systems to facilitate wiretapping. The resulting "artifacts" are bound to remain forcefully in place, even as procedural strictures for treatment of personal data change.

By contrast, strategies to accomplish similar ends while minimizing, anonymizing, or dispersing personal data reflect quite different political values. Such strategies favor privacy, even at the cost of limiting options for future institutional users to implement forceful decisions concerning those depicted in the data.

Systems of institutionally compiled personal information, or systems capable of easily accomplishing such compilation, represent enormous sunk costs and are very reluctantly abandoned. The political climates prevailing over policies governing use of such data, by contrast, are subject to change. Moreover, the constant evolution of new formulae for connecting known or knowable information about individuals with specific determinations that institutions seek to make—for example, identification of people who share crucial characteristics with known terrorists—sharpen demands for access to personal data, often dramatically. The mere knowledge that a given form of personal information is compiled in a given location can generate intense pressures for access that no one may have anticipated when the data were first compiled.

By contrast, the politics or values implicit in privacy-friendly strategies for personal data management do not admit of such easy subversion. Simply not creating, retaining, or centralizing personal data has the simple virtue of not leaving it for future times to determine how such data will be used, and where potentially valuable personal information does exist, dispersion of such information, coupled with institutional ignorance of its location, is a potent privacy-friendly "artifact."

My aim here is not to argue categorically against institutional prerogatives over and against individual privacy claims. Privacy—that is, individual control over creation, storage, and use of information on one's self—can never be the only value guiding law and policy. Even those sincerely committed to privacy values readily identify points at which institutional interests in such data deserve to prevail.

Nevertheless, the forces that have shaped institutional treatment of personal information over recent decades show no signs of relenting. Consequently, it is hard to be optimistic about the long-term prospects for procedural restraint in reducing or even containing the spread of unauthorized institutional monitoring of the lives of ordinary individuals. The better hope, if privacy values are taken seriously, lies in reducing the amount of personal information retained by institutions and ensuring that remaining data are dispersed in ways known only to the individual.

REFERENCES

Bennett, Colin, and Charles Raab. 2003. *The Governance of Privacy; Policy Instruments in Global Perspective*. Aldershot, UK: Ashgate Publishing.

Brown, Ian. 2009. Regulation of Converged Communications Surveillance. In *New Directions in Surveillance and Privacy*, ed. Benjamin J. Goold and Daniel Neyland. Collompton, UK: Willan Publishing.

Cohen, Noam. 2009. As Data Collection Grows, Privacy Erodes. *New York Times*, February 16, B3.

Edelman, Lauren, Sally Riggs Fuller, and Iona Mara-Drita. 2001. Diversity Rhetoric and the Managerialization of Law. *American Journal of Sociology* 106:1589–1641.

Electronic Privacy Information Center and Privacy International (EPIC). 2005. *Privacy and Human Rights; An International Survey of Privacy Laws and Developments*. Washington, DC: Electronic Privacy Information Center.

Etzioni, Amitai. 1999. *The Limits of Privacy*. New York: Basic Books.

European Union. 1995. Data Protection Directive 95/46/EC. *Journal of the European Communities* L281:31.

Greene, Richard Allen. 2008. UK Police DNA Bank a "Human Rights Violation." CNN.com. http://edition.cnn.com/2008/WORLD/europe/12/04/uk.dna.database/index.html (accessed March 9, 2011)

Hendricks, Evan. 2006. GAO: Feds Pay $30 Million to Information Brokers. *Privacy Times* 26 (8): 1.

Lessig, Lawrence. 1999. *Code; and Other Laws of Cyberspace*. New York: Basic Books.

Moore, Solomon. 2009. F.B.I. and States Vastly Expanding Databases of DNA. *New York Times*, April 19, A1.

Park, Whon-Il. 2008. Republic of Korea. In *Global Privacy Protection; the First Generation*, ed. James B. Rule and Graham Greenleaf, 207–229. Cheltenham, UK: Edward Elgar Publishers.

Phillips, David J. 2004. Cell Phones, Surveillance and the State. *Dissent* Spring:53–58.

Posner, Richard. 1978. An Economic Theory of Privacy. *Regulation* May/June:19–26.

Reidenberg, Joel. 1998. Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review* 76 (3): 553–94.

Rimer, Sara. 2008. SAT Changes Policy, Opening Rift with Colleges. *New York Times*, December 31, A12.

Rule, James B. 2007. *Privacy in Peril; How We are Sacrificing a Fundamental Right in Exchange for Security and Convenience*. New York: Oxford University Press.

Seipp, David J. 1978. *The Right to Privacy in American History*, Publication P-78-3, Program on Information Resources Policy. Cambridge, MA: Harvard University.

Selznick, Philip. 1969. *Law, Society and Industrial Justice*. New York: Russell Sage Foundation.

Solove, Daniel. 2004. *The Digital Person; Technology and Privacy in the Information Age*. New York: NYU Press.

Stoddard, Jennifer. 2005. Position Statement on the Anti-Terrorism Act, Submission of the Office of the Privacy Commissioner of Canada to the Senate Special Committee on the Anti-Terrorism Act, May 9.

Szekely, Ivan. 2008. Hungary. In *Global Privacy Protection; The First Generation*, ed. James B. Rule and Graham Greenleaf, 174–206. Cheltenham, UK: Edward Elgar Publishers.

Townsend, Mark, and Anushka Asthana. 2008. Put Young Children on DNA List, Urge Police. *Observer*, Sunday, March 16. http://www.guardian.co.uk/society/2008/mar/16/youthjustice.children (accessed March 9, 2011).

US Department of Health, Education and Welfare. 1973. *Records, Computers and Rights of Citizens; Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. Washington, DC: US Government Printing Office.

Warren, Samuel, and Louis Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4 (5): 193–220.

Winner, Langdon. 1980. Do Artifacts Have Politics? *Daedelus* 109:121–36.

Wright, Gloria. 1996. Victim Relives Rape in Nightmares. *Post-Standard* (Syracuse, New York), October 2, B1.

Zimmerman, Diane L. 1983. Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort. *Cornell Law Review* 68:291–367.