The following two articles were extracted from the report:

Engaging Privacy and Information Technology in a Digital Age
James Waldo, Herbert S. Lin, and Lynette I. Millett, Editors,
Committee on Privacy in the Information Age, National Research Council
Published by the National Academies Press, Washington, D.C., 2007.

Committee on Privacy in the Information Age, National Research Council

William H. Webster
Milbank, Tweed, Hadley & McCloy,
Chair

James Waldo
Sun Microsystems,
Vice Chair

Julie E. Cohen
Georgetown University

Robert W. Crandall
Brookings Institution (resigned April 2006)

Oscar Gandy, Jr.
University of Pennsylvania

James Horning
Network Associates Laboratories

Gary King
Harvard University

Lin E. Knapp, Independent Consultant
Ponte Vedra Beach, Florida

Brent Lowensohn, Independent Consultant
Encino, California

Gary T. Marx
Massachusetts Institute of Technology
(emeritus)

Helen Nissenbaum
New York University

Robert M. O'Neil
University of Virginia

Janey Place
Digital Thinking

Ronald L. Rivest
Massachusetts Institute of Technology

Teresa Schwartz
George Washington University

Lloyd N. Cutler
Wilmer, Cutler, Pickering, Hale & Dorr LLP,
served as co-chair until his passing in May
2005.

Staff

Herbert S. Lin, Senior Scientist

Lynnette I. Millett, Senior Staff Officer

Kristen Batch, Associate Program Officer

Jennifer M. Bishop, Program Associate

David Padgham, Associate Program Officer

Janice M. Sabuda, Senior Program Assistant

Journal of Privacy and Confidentiality (2010) **2**, Number 1, pp. 5–18

Engaging Privacy and Information Technology in a Digital Age: Executive Summary

Committee on Privacy in the Information Age, National Research Council,
Editors, James Waldo*, Herbert S. Lin†, and Lynette I. Millett‡

1 Introduction

Privacy has many connotations—control over information, access to one's person and property, and the right to be left alone have all been included under this rubric. In political discourse, the term "privacy" has been used to refer to physical privacy in the home or office, the ability to make personal reproductive decisions without interference from government, freedom from surveillance, or the ability to keep electronic communications and personal information confidential. For many, privacy is regarded as a fundamental value and right, tied to ideals of autonomy, personal worth, and independence. Privacy is often seen as a necessary condition for keeping personal and public lives separate, for individuals being treated fairly by governments and in the marketplace, and for guaranteeing spaces where individuals can think and discuss their views without interference or censure.

Philosophical approaches to the study of privacy have centered on the elucidation of the basic concept and the normative questions around whether privacy is a right, a good in itself, or an instrumental good. Economic approaches to the question have centered around the value, in economic terms, of privacy, both in its role in the information needed for efficient markets and in the value of information as a piece of property. Sociological approaches to the study of privacy have emphasized the ways in which the collection and use of personal information have reflected and reinforced the relationships of power and influence between individuals, groups, and institutions within society.

Key to any discussion of privacy is a clear specification of what is at stake (what is being kept private) and the parties against which privacy is being invoked (who should not be privy to the information being kept private). For example, one notion of privacy involves confidentiality or secrecy of some specific information, such as preventing disclosure of an individual's library records to the government or to ones employer or parents. A second notion of privacy involves anonymity, as reflected in, for example, the unattributed publication of an article or an unattributable chat room discussion that is critical of the government or of an employer, or an unidentified financial contribution to an organization or a political campaign.

These two simple examples illustrate a number of essential points regarding pri-

*Sun Microsystems, Mountain View, CA, mailto:jim.waldo@east.sun.com
†Computer Science and Telecommunications Board, National Research Council of the National Academies, Washington, DC, mailto:hlin@nas.edu
‡Computer Science and Telecommunications Board, National Research Council of the National Academies, Washington, DC, mailto:lmillett@nas.edu

vacy. First, the party against which privacy is being invoked may have some reason for wanting access to the information being denied. A government conducting a terrorist investigation may want to know what a potential suspect is reading; an employer may be concerned that an article contains trade secrets or company-proprietary information and want to identify the source of that information. Privacy rights are invoked to prevent the disclosure of such information. Second, some kind of balancing of competing interests may be necessary. Third, balancing is a task that is essentially political—and thus the political and societal power of various interest groups is critical to understanding how tradeoffs and compromises on privacy develop.

2 Drivers of Change in Notions of Privacy

This report focuses on three major drivers of the vast changes affecting notions, perceptions, and expectations of privacy: *technological change*, *societal shifts*, and *discontinuities in circumstance*.

- *Technological change* refers to major differences in the technological environment of today as compared to that existing many decades ago (and which has a major influence on today's social and legal regime governing privacy). The hardware underlying information technology has become vastly more powerful; advances in processor speed, memory sizes, disk storage capacity, and networking bandwidth allow data to be collected, stored, and analyzed in ways that were barely imaginable a decade ago. Other technology drivers are just emerging, including sensor networks that capture data and connect that data to the real world. Increasingly ubiquitous networking means that more and more information is online. Data stores are increasingly available in electronic form for analysis. New algorithms have been developed that allow extraction of information from a sea of collected data. The net result is that new kinds of data are being collected and stored in vast quantities and over long periods of time, and obscurity or difficulty of access are increasingly less practical as ways of protecting privacy. Finally, because information technologies are continually dropping in cost, technologies for collecting and analyzing personal information from multiple, disparate sources are increasingly available to individuals, corporations, and governments.

- *Societal shifts* refer to evolutionary changes in the institutions of society—the organizations and the activities and practices that make use of the technological systems described above—and to the transformation of social institutions, practices, and behavior through their routine use. To an unprecedented degree, making personal information available to institutions and organizations has become essential for individual participation in everyday life. These information demands have increasingly appeared in licensing; administration and conferring of government or private sector benefits to particular classes of people (e.g., veterans, the unemployed, those with low income, homeowners); providing of services; employment; and retailing.

- *Discontinuities in circumstance* refer to events and emergent concerns that utterly transform the national debate about privacy in a very short time (and thus do not allow for gradual adjustment to a new set of circumstances). The most salient example in recent years concerns the events of September 11, 2001, which transformed the national environment and catapulted counterterrorism and national security to the very top of the public policy agenda. But the SARS outbreak in 2003 hinted at the potential for global pandemic on a very short time scale with some other disease, and measures to prevent pandemic outbreaks are receiving greater attention today. In the past, the Watergate scandals of 1972-1973, the Church Committee Hearings of 1976 (also known as the Hearings of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities), and the attack on Pearl Harbor in 1941 could also be seen as watershed events with dramatic changes in the environment for privacy.

These multiple drivers suggest how our attitudes toward privacy are context dependent. It is difficult to hold a precise view of what privacy is, absent consideration of what kind of information is sought, who seeks it, and how it is to be collected, protected, and used. There are, for example, some things one might not mind the government knowing that one would object to an employer knowing (and vice versa). And there are other things that one would not object to either of them knowing, but would not want passed on to aunts and uncles, just as there are things that one would like to keep within the family. Determining what should (1) be left to the realm of ethics and common courtesy, (2) be incentivized or discouraged, or (3) be formalized in regulation or law is yet another balancing question that comes up when contemplating privacy.

Taken together, these drivers point to an environment for privacy that is quite different from what existed in the era that led to the formation of many of today's expectations and assumptions about the nature of privacy and the role that privacy plays in individual lives and in society. As the environment changes, it is easy to see how understandings and a status quo developed prior to those changes can be upended. Thus, there is no immutable standard for what degree of privacy can be expected suggesting that battles once fought and settled in one era may need to be refought and settled anew in another.

3 Understanding Privacy Tradeoffs

Privacy is a complex issue because multiple interests are at stake. Indeed, if the information had no value to anyone (either at the moment of collection or in the future), the protection of privacy would be a nonissue; the information would not be gathered in the first place.

But this is not the case. In many ways, both large and small, benefits do accrue from the collection of some kinds of information. These benefits lead to pressures against privacy measures that might impede the collection of such information. In some cases, these pressures are the result of *specific uses* for the information collected—

that is, privacy concerns sometimes emanate from specific uses of information rather than the fact of collection itself. From a privacy protection standpoint, this in turn highlights a major problem for individuals—knowing those ultimate uses can be difficult or impossible.

Some of the most complex tradeoffs—and the ones most controversial or difficult to manage—involve a tradeoff of the interests of many individuals against the interests of a collective society. An individual's interest in keeping his or her medical records private—an interest shared by many individuals—may pose a tradeoff when community needs for epidemiological information are concerned or when emergency care for the individual is necessary without explicit consent. Video surveillance may deter crime but also poses a privacy risk if male camera operators use the cameras to focus on private parts of women's bodies. While law enforcement authorities believe that it is helpful to know the identities of individuals interested in reading about terrorism or bomb making, librarians and many state legislatures are concerned about ensuring a free, unfettered, and unmonitored flow of information to all library patrons that could be jeopardized if individuals reading habits are potentially the subject of government investigation or even monitoring. Surveillance by government authorities can inhibit legal and legitimate social and political gatherings.

However, the fact that tradeoffs are sometimes necessary should not be taken to mean that tradeoffs are always necessary. In some cases, careful design and planning will minimize the tradeoffs that are needed to attend to societal needs without compromising personal information. An example might be a design decision for a system to discard data immediately after it has been used for the purpose at hand—in many instances, privacy concerns are strongly mitigated by the non-retention of data.

This perspective makes clear that the social context in which privacy is experienced has shifted in recent years. Identifying balances that people are comfortable with in legal affairs, security provisions, behavioral norms, and relationships will require an ongoing dialogue involving numerous stakeholders and constituencies. Expectations of privacy formed in the preindustrial age were not sufficient after the industrial revolution, and it should not be surprising that notions of privacy developed during the industrial age should show signs of stress in the new information age. It is at just such times of changing capabilities and expectations that we need to examine the core of our notions of privacy to ensure that what is most important survives the transitions.

4 Tools for Protecting Privacy

There are many pressures to diminish privacy, regardless of how the term is defined, but there are also a number of tools available to help protect privacy. These tools fall into three generic categories:

- *Personal unilateral actions (self-help).* When information collectors rely on individuals themselves to provide personal information, these individuals can take action to withhold that information. They can refuse to provide it at all, or they

can provide false, misleading, or incomplete information. A common example is an affinity card, which entitles the holder to a discount on store products. Affinity cards are typically provided to an individual upon receipt of a completed application, which usually involves a questionnaire about income, demographics, and spending habits. There is often no verification of the information provided or sanction applied for inaccurate information, and so many individuals simply provide inaccurate information. Withholding information also works to protect privacy, although it may also deny one certain benefits, such as a license or a job. Neither of these approaches is well advised, of course, when there are excessively negative and severe consequences to withholding or providing false information.

- *Technology.* Technical measures can protect privacy as well, although a relevant question is who decides to implement any given technical measure. From an individual standpoint, encryption and anonymizers are today the primary privacy-protecting technologies. That is, encryption of personal information can be used to ensure that such information can only be accessed with the express permission of the subject of that information, and that communications cannot be seen by others than those taking part in the communication. Anonymizers (e.g., anti-spyware tools, anonymous browsers) allow an individual to explore cyberspace (e.g., using e-mail, viewing Web sites) with a high degree of anonymity. In addition, antispam and anti-phishing technologies help individuals to be left alone and reduce the leakage of personal information. Technical safeguards to protect privacy are also available to the collectors of personal information, who may wish to protect such information to make individuals more willing or more comfortable about sharing information with them. For example, technologies are being developed that can screen out individuating characteristics in large-scale public data-gathering systems such as video cameras, and some statistical methods and data-mining algorithms have been developed that facilitate the anonymization of information without changing the important statistical properties of the information taken in the aggregate.

- *Policy.* Policy measures, by which are meant actions that information collectors can or must take, are arguably the most important privacy protection tool. That is, privacy is much more an issue of who is permitted to see an individual's personal information than of technologically restricting access to that information. People may be concerned about personal health and medical information being improperly disclosed, but this problem may arise at least as much as a result of policy decisions to make such information broadly accessible to relevant parties as from the activities of hackers breaking into medical databases. Policy measures fall into five generic categories:

  - *Limits on the information collected and stored (data minimization).* For example, often the most "obvious" efforts to enhance public safety or security are highly privacy-invasive (e.g., collect all possible data about individuals and mine it extensively). However, it may be possible, with some thoughtfulness early on, to collect a much more limited set of information that will

still satisfy a given purpose. Collected information, once used, can also be deleted to prevent further use. Of course, such limits will be strongly resisted by information collectors who do not know in advance of collection the specific purposes for which they need information, and who see information as an opportunity to develop a resource that might be useful for an extended time. Note also that limits need not be formulated in all-or-nothing terms. Limits may be imposed in the form of differential levels of access for different individuals, varying time windows for access (both when data are made available and for how long), or access for certain purposes but not for others.

- *Limits on outsider access.* By definition, an outsider is a party external to the organization that collects the information in question. Outsiders can be denied access through both technical and procedural means. Technical means include measures such as encryption and access control mechanisms that prevent unauthorized access; procedural means include regulation-based restrictions on who receives information.
- *Prevention of internal abuse.* Even organizations with the best of intentions may have insiders (e.g., employees) who do not use the information collected in accordance with organizationally approved purposes. For example, a law enforcement agent may use a national criminal database to investigate an individual for personal reasons, in violation of departmental policy. In such instances, frequent audits to uncover improper access and penalties for improper access are essential elements of preventing such use.
- *Notification.* It is generally believed that violations of privacy are in some sense worse when they occur without the knowledge of the individual in question; thus, notification when unauthorized access occurs can be regarded as a privacy protection measure.
- *Correction.* The opportunity to review information collected and to ensure that it is at least correct protects the individual against decisions being made on the basis of incorrect information.

5 A Basic Analytical Framework for Understanding Privacy

The notion of privacy is a basic starting point for this framework, and as suggested in the introduction, three essential questions arise:

- What is the information that is being kept private (and with whom is that information associated)?
- From whom is the information being withheld?
- What purposes would be served by withholding or not withholding the information, and whose interests do those purposes serve?

5.1 A Worked Example of Privacy Tradeoffs

To illustrate how basic privacy tradeoffs arise, this report considers privacy and the U.S. library community. The issue of privacy in libraries is considered not because it is more important than privacy in other domains (e.g., in health care or law enforcement), but because it provides an opportunity to introduce in a concrete manner some of the basic tradeoffs.

The library community has a long historical commitment to protecting the privacy of its patrons, formalized more than five decades ago and integrated into a core set of shared beliefs. This community was also an early adopter of information technology as a way of furthering its mission of offering full access to all information to libraries' patrons. Since many libraries are publicly funded in one way or another, this community is also directly subject to shifts in the political landscape. This combination makes this community one of the most active, articulate, and thoughtful of the various factions taking part in the debates about privacy.

The framework of questions posed above provides a starting point for the discussion of library privacy.

- What is the information that is being kept private (and with whom is that information associated)? The information that is being kept private is the borrowing history of reading materials of library patrons who are identifiable by name or the names of all individuals who have had access to specific reading materials. (Such information is protected under the laws of many states.) "Borrowing history" can include computer access to information as well.

- From whom is the information being withheld? According to the librarians' code of ethics, borrowing records should be kept private from all parties except as necessary to provide fiscal accountability for materials borrowed (you fail to return a book, you pay for it).

- What purposes would be served by withholding or not withholding the information, and whose interests do those purposes serve? The rationale underlying the withholding of borrowing information is the belief that citizens are served best when they can obtain information and access to society's scientific, cultural, and historical legacy without interference or observation from other parties, and disclosure of that information might subject patrons to pressure and outside influence. Moreover, because there is no general social consensus about information that is or is not desirable for people to have (the primary exceptions being materials judged to constitute child pornography), librarians believe that leaving the choice of subjects to the individuals own choosing maximizes the benefit to society as a whole. As for disclosure of information on borrowing, the interests served depend on who has access and for what reasons access is being sought. For example, parents may wish to know if a teenage daughter is reading about sex, or law enforcement authorities may wish to know if a person of interest is reading about guns or radical politics.

From this example, several themes emerge.

First, the direct interests of the individual differ from those of the parties seeking the information.

Second, a long history of privacy concerns in the library community provides the basic context against which today's current concerns about privacy are judged and assessed.

Third, technological advances in the library domain—coupled with change in the social and political milieu in which libraries operate—reopen once-settled arguments and compromises that have historically been made between privacy and other values. Law enforcement authorities have sought information about reading habits of patrons in the past, but debates over library privacy have been reopened as records of Internet access in libraries become important to criminal or intelligence investigations.

In order to compare how these issues play out in other domains, the next section illustrates three other important scenarios.

5.2 Elaboration of the Issues

Although other parties have many reasons for using personal information of individuals, four stand out as being of particular significance. One reason is economic—by using personal information about individuals, various profit-making enterprises can enhance their revenue streams, sometimes quite substantially. A second is medical—detailed information about patients enables higher-quality and less expensive health care than would otherwise be possible. A third is public safety and national security—collection of information about criminals, criminal activities, and terrorists enables law enforcement and national security authorities to protect the public more effectively. A fourth is research—statistical trends derived from collections of personal information are often of importance to public policy makers. Privacy tradeoffs related to each of these reasons are explored below.

5.2.1 Economic Drivers

A good example of how economic drivers affect privacy can be found in the area of the definition, protection, and enforcement of intellectual property rights in the networked digital environment. Deep privacy issues arise in this domain because digital rights management technologies (DRMTs)—originally intended to help limit illegal distribution of copyrighted digital materials—also enable very-fine-grained control over what legitimate users may do with materials in their possession (e.g., how many times a document can be read, or whether it can be forwarded). Of particular concern from a privacy perspective, DRMTs could also be used to monitor what intellectual property and information an individual uses and how. Information can be collected about how many times you read a document, how long you spend listening to a piece of music, how often you visit a particular place on the Internet, or what kinds of changes you

make to information and when—among many other things. Such finegrained information collection and monitoring of what many perceive to be critical components of their intellectual and emotional selves (the books we read, the music we listen to, the movies that we watch) might have a dramatic impact on people's perceptions of their individual privacy.

In the case of DRMTs, the economic benefit today arises not from the collection of this information about user behavior per se, but from the primary applications of DRMTs to charge fees for various services for access to protected materials (printing, storage, multiple simultaneous access, and so on). That is, publishers have found that DRMTs are enablers for a different and more profitable business model, although in the future certain parties might also find significant economic interest in what could be gleaned from such information such as from targeted marketing based on user interests). Privacy concerns arise because of the potential for these DRMTs to collect detailed information on user behavior regarding the digital content they consume and thus all of the consequences that could result if DRMTs were in fact used in this way.

5.2.2 Medical Drivers

Health and medical privacy has traditionally been considered a core privacy right. The experience of policy makers in implementing the privacy regulations of the Health Insurance Portability and Accountability Act (HIPAA) serves as a case study in some of the subtleties of privacy, showing the difficulty of determining the line between what should be private and what can be disclosed (and with whom and for what purposes such sharing can take place); the difficulties of placing the appropriate procedures and technologies in place to ensure the required levels of privacy; and the various costs of such privacy regulations. The health and medical communities are also on the leading edge of several possible future privacy issues, having to do with the appropriate use of information that can be gathered from sources such as DNA analysis. These issues call into question even the notion of whose privacy is involved, since the information contained in a person's DNA concerns not only that person but also the set of people who share that person's genetic lineage. The same may be true to a lesser extent for health habits and infectious diseases, the presence of which often correlates with family membership.

Privacy issues arise in the health and medical domain primarily as the result of a concern about the consequences should personal health and medical information be disclosed or disclosable. One source of concern is social—there is stigma associated with certain medical conditions, and disclosure of those conditions potentially subjects individuals with them to discrimination and to being socially ostracized. A second is economic—disclosure of information about an individual's health to insurance companies can be used to deny him or her health insurance (or increase the price of such insurance), and disclosure of such information to an employer may affect his or her employment prospects with that employer. And underlying these social and economic concerns is the fact that candor between a patient and his or her health care provider is essential for good care.

An interesting middle ground is the disclosure of personal health information for research purposes (e.g., to determine effective courses of medical treatment). For such purposes, individual names need not be associated with the information being collected, although unique identifiers may be needed to track individuals longitudinally. In this context, some people may regard collection of information as benign from a privacy standpoint, while others may regard it as intrusive.

More generally, this example illustrates that concerns about privacy in many domains —often relate to the stated reasons for which the information is gathered, the intention of the gatherers, and the subsequent uses to which the information is put. Something can be seen either as an invasion of privacy or as an attempt to give better service, depending on the motives, results, explanations offered, safeguards provided, and trust relationships that hold between the individuals and the companies that are gathering and using the information.

5.2.3 Law Enforcement and National Security Drivers

Law enforcement and national security authorities need information about criminals, criminal activities, and terrorists if these authorities are to carry out their missions. And if collection of information could be precisely limited to these targets there would be little controversy.

But criminals and terrorists do not wear brightly colored shirts announcing that they are actual or potential criminals and terrorists. As a rule, criminals and terrorists wish to blend in with the law-abiding population so that they do not come under suspicion and thus have a freer hand to plan and operate. Thus, any information collection directed at criminals and terrorists potentially gathers information about law-abiding citizens, and striking the appropriate balance between acknowledging the law enforcement/national security need for collecting information and protecting the privacy of law-abiding citizens has been an especially copious source of public policy controversy since September 11, 2001. Of course, this is not a new tension; indeed, it has existed far longer than this country. What makes this subject of particular importance for this study is the confluence of the technology that makes it possible for privacy to be eroded far more extensively than ever before with the historical context that makes the claims for security more persuasive.

There are many reasons that law-abiding individuals might be concerned about the collection of their personal information, but three are worthy of particular mention. First, these individuals may be concerned that such information might be abused. By giving government officials the ability to collect personal information, citizens must take on faith that such abilities will be exercised only for proper reasons, such as the investigation of a crime, and not for improper ones, such as the settling of personal vendettas. Second, government knowledge about certain activities often has a chilling effect on such activities, even if such activities are entirely legal—an example might be planning a public protest about government action. Third, many individuals do not want government authorities to collect personal information simply on the theory

that such collection raises their profile and makes it more likely that they might be erroneously singled out in some manner to their detriment even if they have done nothing illegal.

6 Findings and Recommendations

Argumentation for the findings and recommendations is provided in Chapter 10 of the report. Recommendations are presented in boldface below.

The committee found that the meaning of privacy is highly contextual, and it can vary depending on the specific circumstances at hand, such as the situation and relationships at issue, the intentions of the parties involved, and the historical context, technology, and political environment. Despite this contextual meaning, privacy is an important value to be maintained and protected, because the loss of privacy often results in significant tangible and intangible harm to individuals and to groups. Privacy is most important to people when they believe the entity receiving their personal information is not trustworthy and that they may be harmed by sharing that information.

At the same time, privacy is not an absolute good in itself. Tradeoffs against other desirable societal values or goods are sometimes inevitable. Privacy-invasive solutions to public policy problems may be warranted under some circumstances. However, when they are implemented as measures of first rather than last resort, they generate resistance that might otherwise be avoided if other alternatives were tried first.

Businesses, researchers, and government agencies find value in the exploitation of personal information, and they have further developed many mechanisms—both voluntary and intrusive—for obtaining personal information. Moreover, because these entities often develop new ways of using personal information in pursuit of their organizational goals and missions, there emerge many pressures for the repurposing of data that have already been collected. Changing social trends and sentinel events such as the 9/11 attacks put additional strong pressures on privacy.

The changing information technology environment has also helped to compromise privacy, although some developments in information technology and other technologies do have considerable potential to enhance it. In addition, technology-based privacy enhancement rests on firmer ground to the extent that technologists attend to privacy considerations throughout the life cycle of personal information that is collected rather than just at the beginning of the collection process.

The committee is concerned about the nature of public debates about privacy and its relationship to other societal interests. For example, the committee found that there is often a lack of clarity about the privacy interests involved and too often a tendency to downplay and to be dismissive of the privacy issues at stake. When privacy is at issue, the committee found that bland assurances that privacy will not be harmed offered by policy makers can do more to raise skepticism than honest presentation and assessment of tradeoffs.

To facilitate a more thoughtful public debate, the committee articulated a number of principles. The first was that the debate should avoid demonization. Most threats to privacy do not come from fundamentally bad people with bad intentions. Demonization tends to make compromise and thoughtful deliberation difficult. Second, the debate should account for context and nuance; taking nuance and context into account will often be necessary if common ground is to be found. Third, the debate should respect the complexity inherent in the problem. Privacy is a complicated issue, and it is a moving target, as the numerous social and technical factors with which it is intertwined change over time. Thus, initiatives that have policy implications and solutions to identified privacy problems are more likely to be successful if they can begin with modest and simple steps that provide feedback to guide and shape further actions. Fourth, decision makers must be aware of long-term costs and risks. In particular, it is costly to retrofit privacy features into a system (such as the addition of query audit trails to deter inappropriate use by employees), and such fixes are often necessary when inadvertent violations of privacy occur that might have been prevented if those features had been available in the first place. (There are also the costs associated with unfavorable publicity and possible economic liability.) Thus, it often makes sense to ensure that adequate technology-based enforcement of privacy policies is a part of a system's initial design.

In order to enhance privacy, individual, organizational, and public policy actors have roles to play.

Individuals can take a number of steps to enhance the privacy of their personal information and to become better informed about the extent to which their privacy has been compromised, although the effectiveness of these measures is bound to be limited. The committee thus recommends that **if policy choices require that individuals shoulder the burden of protecting their own privacy, law and regulation should support the individual in doing so.**

Firms and other organizations can design and implement self-regulatory regimes for protecting the privacy of the personal information they collect. Self-regulation is limited as a method for ensuring privacy, although it nevertheless offers protections that would not otherwise be available to the public. The committee offers a number of concrete recommendations to enhance the effectiveness of privacy policies. Specifically, **organizations with self-regulatory privacy policies should take both technical and administrative measures to ensure their enforcement, routinely test whether their stated privacy policies are being fully implemented, produce privacy impact assessments when they are appropriate, strengthen their privacy policy by establishing a mechanism for recourse if an individual or a group believes that they have been treated in a manner inconsistent with an organization's stated policy, and establish an institutional advocate for privacy.**

The committee found that governmental bodies have important roles to play in protecting the privacy of individuals and/or groups and in ensuring that decisions concerning privacy are made in an informed fashion. However, the U.S. legal and regulatory

framework surrounding privacy is a patchwork that lacks consistent principles or unifying themes. Accordingly, the committee concluded that a less decentralized and more integrated approach to privacy policy in the United States could bring a greater degree of coherence to the subject of privacy. Two recommendations follow from this conclusion. First, the committee recommends that **the U.S. government should undertake a broad systematic review of national privacy laws and regulations. Second, the committee recommends that government policy makers should respect the spirit of privacy-related law.**

The principles of fair information practice for the protection of personal information were first enunciated in a 1973 report of the U.S. Department of Health, Education, and Welfare. In reviewing the privacy landscape, the committee found that these principles are as relevant and important today as they were in 1973. Thus, the committee recommends **that principles of fair information practice should be extended as far as reasonably feasible to apply to private sector organizations that collect and use personal information.** Given the growing importance of repurposing collected personal information, the committee also recommends that **to support greater transparency into the decision-making process regarding repurposing, guidelines should be established for informing individuals that repurposing of their personal information might occur, and also what the nature of such repurposing would be, and what factors would be taken into account in making any such decision.** In addition, the committee recommends that **the principle of choice and consent should be implemented so that individual choices and consent are genuinely informed and so that its implementation accounts fairly for demonstrated human tendencies to accept without change choices made by default.**

Furthermore, although a number of laws do protect the privacy of personal information in government hands, the use of private sector data aggregators is a gray area, and the committee recommends that **the U.S. Congress should pay special attention to and provide special oversight regarding the government use of private sector organizations to obtain personal information about individuals.**

As for the government use of personal information, the committee found that because the benefits of privacy often are less tangible and immediate than the perceived benefits of other interests such as public security and economic efficiency, privacy is at an inherent disadvantage when decision makers weigh privacy against these other interests. The committee concluded that, to reduce this inherent disadvantage, governments at federal, state, and local levels should establish mechanisms for the institutional advocacy of privacy within government. Accordingly, the committee recommends that **governments at various levels should establish formal mechanisms for the institutional advocacy of privacy within government, and furthermore that a national privacy commissioner or standing privacy commission should be established to provide ongoing and periodic assessments of privacy developments.**

Finally, the committee found that the availability of individual recourse for recog-

nized violations of privacy is an essential element of public policy regarding privacy. Accordingly, it recommends that **governments at all levels should take action to establish the availability of appropriate individual recourse for recognized violations of privacy.**