Principles for Protecting Privacy

Fred H. Cate

The past five years have witnessed an explosion in legislation, regulation, and litigation designed to protect the privacy of personal information. Congress alone has adopted comprehensive federal financial privacy legislation, online privacy protection for children, and the first federal prohibition on access to historically open public records without individual "opt-in" consent, among other privacy laws. Rather than preventing harmful uses of personal information or invasions of privacy by the government, these laws grant individuals broad rights to control innocuous and even beneficial uses of information about them by the private sector.

At the state level, legislators have considered hundreds of their own privacy bills in the past two years alone. State attorneys general have initiated aggressive privacy investigations and litigation. State insurance commissioners have been busy trying to implement the insurance provisions of the Gramm-Leach-Bliley Financial Services Modernization Act of 1999.

On the judicial side, the Supreme Court has decided two cases upholding privacy laws from constitutional attack,[1] while at the same time holding that the First Amendment protected the broadcast of an illegally intercepted cellular telephone conversation.[2] Federal appellate courts, meanwhile, have been busy alternately upholding and striking down privacy laws.[3]

Outside of the United States, Europe has brought its sweeping data protection directive into force, while other industrialized countries

---

Cato Journal, Vol. 22, No. 1 (Spring/Summer 2002).

Fred H. Cate is Professor of Law at the Indiana University School of Law-Bloomington.

[1]Reno v. Condon, 528 U.S. 141 (2000); Los Angeles Police Department v. United Reporting, 528 U.S. 32 (1999).

[2]Bartnicki v. Vopper (2001).

[3]See, e.g., U.S. West, Inc. v. Federal Communications Commission, 182 F.3d 1224, 1235 (10th Cir. 1999), Cert. Denied, 528 U.S. 1188 (2000); Trans Union Corp. v. Federal Trade Commission, 245 F.3d 809 (2001).

have either adopted or are in the process of considering new privacy laws.

In sum, there is no shortage of sources to which we might look for experience in enacting and enforcing privacy laws.

The most recent federal privacy enactment involves the rules adopted by the Department of Health and Human Services in December 2000, and amended in March 2002, to implement the health privacy provisions of the 1996 Health Insurance Portability and Accountability Act. While weakening protection for privacy against government intrusion, they impose substantial new restrictions on the use of personal health information by the private sector. Under the amended rules, such information can generally be used for health care treatment, payment, or operations only after an individual is provided with a detailed disclosure of privacy practices by covered health care providers. Providers with a direct treatment relationship also must make a good faith effort to receive a written acknowledgement of receipt of that notice. Information may be used for other health-related purposes only with the explicit, opt-in "authorization" of the individual concerned.

These rules ignore much of the evidence about the cost and burden to consumers of providing notices and securing consent, and the undesirability (and likely unconstitutionality) of conditioning medical service on compliance with bureaucratic notice and acknowledgement or consent requirements, especially when that service cannot be provided without the information or access to the information yields broad societal benefits. The rules demonstrate how little we have learned from our past experience with privacy laws and regulations.

This article, therefore, addresses health privacy in the broader context of other areas of recent privacy activity, in an effort to discover what we should have learned in trying to identify those principles that should undergird regulatory efforts to protect privacy.

The Privacy Debate

The recent debate over privacy, and the role of law in protecting it, is unlike many other political debates for a variety of reasons.

Privacy is an unusually broad term, encompassing both fundamental constitutional rights (such as freedom from government intrusions into our homes and other forms of search and seizure, as well as the right of citizens to make decisions about marriage, contraception, and abortion) and less well-defined and arguably less critical issues (such

as the desire to be free from annoying direct marketing calls and mailings).

"Privacy" has always been susceptible to many meanings. The Supreme Court has interpreted the Constitution to protect, under the rubric of "privacy," an individual's right to be free from unreasonable searches and seizures by the government; the right to make decisions about contraception, abortion, and other "fundamental" issues such as marriage, child rearing, and education; the right not to disclose certain information to the government; the right to associate freely; and the right to enjoy one's own home free from intrusion by the government, sexually explicit mail or radio broadcasts, or other intrusions. Interestingly, none of these understandings of privacy, based on protection against government actions, is at issue in the current privacy debate.

However, the term "privacy" has been stretched in common parlance to suggest even more meanings, including individual autonomy (the right to make decisions without undue interference), self-definition (the right to define one's self to others), solitude and intimacy (the desire to limit access to a place or to oneself), confidentiality (trade secrets and information disclosed subject to a promise of confidentiality), anonymity (the desire not to be identified), security (for oneself or one's information), freedom from intrusion (whether physical—a trespasser, or technological—a hidden camera or microphone), freedom from annoyance (such as the distraction or harassment of unsolicited mail or telephone calls), freedom from crime (such as identity theft or financial fraud), freedom from embarrassing disclosures, freedom from discrimination (whether legal or illegal), profit (the desire to share in the proceeds from disclosing or using valuable information), trust (protect against breaches of fiduciary and other professional duties), and countless other concepts.

Moreover, the breadth and malleability of the term "privacy" has had a remarkable effect on the political debate over the role of law in protecting it. Because "privacy" can mean almost anything to anybody, and because the term carries such emotional weight (conjuring up, as it does, images of the sanctity of the body and the home), legislators can generate broad support for so-called privacy laws just by invoking the word. Yet without any specificity as to what privacy interest a proposed law or regulation is intended to serve, neither legislators nor the public can determine whether a need exists, whether the law in fact meets that need, and whether there are less expensive or burdensome ways of accomplishing the same end.

Privacy is important for all individuals in a wide variety of settings. Because it involves restrictions on the information flows that are

essential to consumer products and services, commerce, and government, the debate over how to protect privacy affects all citizens, consumers, most businesses, government agencies, and other institutions. Few people think they understand bankruptcy or Medicare reform, but almost everyone has an opinion about privacy.

Those opinions about privacy are inherently subjective. People who respond to public opinion polls that they worry about privacy or support laws to protect it mean *their* privacy, not anyone else's. Most surveys ask about privacy in a vacuum, not how much consumers are willing to pay or endure for more privacy protection. Accordingly, privacy tends to be a one-sided issue. Who is against it? Most people regard privacy, or at least their own privacy, as deserving of as much protection as possible. If a little is good, more is even better.

It is frankly difficult to find the "other" side of the privacy debate in large part because the benefits that result from open information flows (and may be placed at risk when privacy protections interfere with those flows) are so integral a part of our lives that they are seldom explicitly recognized or fully understood. In a society dominated by the First Amendment and a history of open information flows, most American citizens and companies have little experience with the cost and burden of privacy restrictions and missing information.

The rhetoric of the privacy debate further runs the risk of distorting its outcome. As Kent Walker (2001) has written: "Just as no one is 'pro-abortion' or 'anti-life,' no one can be 'anti-privacy,' yet that's the only label left by the rhetoric."

Finally, privacy as an issue is not only popular and difficult to oppose, but it costs the government little to regulate the information flows of the private sector. It suits perfectly an era of feel-good legislation and budget cutting.

Collectively, these and other factors have contributed to diminishing the rationality of the current privacy debate, while escalating the pressure on legislators to support privacy bills.

The Transformation of Privacy Law

The result has been a transformation of privacy law. Historically, U.S. privacy law focused on two broad themes. The first and most visible was preventing intrusion by the *government*. Virtually all constitutional privacy rights reflect the reality that only the government exercises the power to compel disclosure of information and to impose civil and criminal penalties for noncompliance, and only the

government collects and uses information free from market competition and consumer preferences.

The second theme reflected in U.S. privacy law throughout the last century was preventing uses of information that *harm* consumers. When privacy laws did address private-sector behavior, they were designed to prevent specific, identified harms. For example, the Fair Credit Reporting Act, one of earliest privacy laws applicable to the private sector, focuses primarily on correcting inaccuracies and assuring that credit information is not used in ways likely to harm consumers.

Increasingly, however, the dominant trend in recent and pending privacy legislation is to invest consumers with near absolute *control over information* in the marketplace—irrespective of whether the information is, or could be, used to cause harm. Alan Westin (1967: 7) describes this as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Public officials and privacy advocates argue that we must assure consumers that they have full control over their personal information and that privacy is "an issue that will not go away until every single American has the right to control how their personal information is or isn't used" (LaFalce 2000). The National Association of Attorneys General's December 2000 draft statement on Privacy Principles and Background sets forth as its core principle: "Put simply, consumers should have the right to know and control what data is being collected about them and how it is being used, whether it is offline or online" (NAAG 2000: 7). Virtually all of the privacy bills pending before Congress reflect the goal of strengthening control by individual consumers.

William Safire (1999) summed up this trend when he wrote in the *New York Times*:

> Your bank account, your health record, your genetic code, your personal and shopping habits and sexual interests are your own business. That information has value. If anybody wants to pay for an intimate look inside your life, let them make you an offer and you'll think about it. . . . [E]xcepting legitimate needs of law enforcement and public interest, control of information must rest with the person himself.

This focus on control ignores the extent to which many uses of personal information pose no risk of harm to individuals, while creating significant benefits for data subjects and society more broadly. Laws that facilitate that control, therefore, often create significant costs, without yielding net benefits.

The Limits of Notice and Consent

The focus on control also ignores that fact that most consumers, in practice, do not exercise that control—by either consenting or withholding consent—over the information they disclose and generate.

Consumers are typically presented with meaningful opportunities to make choices concerning the collection and use of their personal information in two settings. The first occurs when a consumer seeks a service, and the business responds by disclosing its intent and seeking consent to collect and use the personal information necessary to provide the requested service. The business and the individual already are in contact and focused on the transaction for which the information is necessary.

In this situation, individuals tend to ignore privacy policies and consent requests if they can, or to simply click through or sign them without reading them if they are not permitted to ignore them completely. When online, most consumers click through pop-up screens with terms and conditions, and rarely if ever click on privacy notices. In fact, the chief privacy officer of Excite@Home, Ted Wham, told a Federal Trade Commission (FTC) workshop on profiling that the day after *60 Minutes* featured his company in a segment on Internet privacy, only 100 out of 20 million unique visitors accessed that company's privacy pages (Federal Trade Commission 2001).

We also see this same behavior offline, where most people flip through disclosure notices and sign consent forms, when being admitted to the hospital or applying for a mortgage or loan, without ever reading them. Because the terms contained in those documents are not optional—individuals must accede to them if they want the requested service or product—and because most consumers are so focused on the ultimate goal (being treated or obtaining the loan), they rarely take time to consider what they are being told. In this situation, a privacy law based on notice and choice imposes costs but does little to enhance privacy protection. The only real choice that individuals have is to go elsewhere, which is the same choice they had prior to enactment of such privacy protection.

The second setting in which notices are provided and consent may be sought is when the business wishes to use information about a consumer who is not at that moment seeking a service or product. The need for such consent may arise because the consumer is not a customer of the business, the business wishes to make a new use of information about an existing customer that goes beyond the uses described in the original privacy notice, or the business wishes to use information that it has observed or collected from a third party.

The major problem here is the difficulty of reaching the customer who is not currently in direct contact with the business. Most requests for consumer consent never reach their intended recipient. The U.S. Postal Service reports that 52 percent of unsolicited mail in this country is discarded without ever being read. Unsolicited e-mail, even when sent by a company with which the recipient has a relationship, is left unopened at about the same rate. No matter how great the potential benefit resulting from the information use might be, if the request is not read or heard, a consumer cannot act on it.

Consider the experience of U.S. West, one of the few U.S. companies to test an "opt-in" system. To provide individualized notices to customers and obtain their permission to use information about their calling patterns (e.g., volume of calls and time and duration of calls), the company found that it required an average of 4.8 calls to each customer household before it reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. Consequently, many U.S. West customers received more calls, and one-third of their customers were denied opportunities to receive information about valuable new products and services (Brief for Petitioner and Interveners 1999: 15–16).

The difficulties of reaching consumers are greatly exacerbated where the party wishing to use the information has no (and may not have ever had) direct contact with the consumer. For example, most mailing lists are obtained from third parties, not the people whose names are on the list. Requiring a secondary user to have to contact every person individually to provide a notice and/or obtain consent to use the information would cause delay, require additional contacts with consumers, and almost certainly prove prohibitively expensive. This is an especially acute concern in the area of medical research, where researchers performing chart review will likely have no contact with the patient, and the patient will likely no longer be present in the health care system. To require that the researcher provide the patient with notice and/or obtain the patient's consent means that the researcher will face not only all of the burdens normally associated with reaching individuals and getting them to pay attention to a notice and/or respond to a consent request, but the additional burden of having to do so without the benefit of an existing relationship with them or a ready mechanism for communicating with them.

The Experience of Gramm-Leach-Bliley

The Gramm-Leach-Bliley Financial Services Modernization Act provided that by July 1, 2001, and annually thereafter, every financial

institution is required to send to every one of its customers a notice outlining how the financial institution collects and uses personal information, and offering the customer an opportunity to opt out of certain third-party information-sharing. By July 1, 40,000 financial institutions had mailed approximately 4 billion notices.

If ever consumers would respond, this would appear to be the occasion. The notices came in an avalanche. The notices were based on model terms drafted by federal regulators to communicate clearly and effectively. The press carried a wave of stories about the notices. Privacy advocates trumpeted the opt-out opportunity and offered online services that would write opt-out requests for consumers. The information at issue—financial information—is among the most sensitive and personal to most individuals.

Yet the response rate was negligible. By mid-August 2001, only about five percent of consumers had opted out of having their financial information shared with third parties. This is consistent with the experience with company- and industry-specific opt-out lists: Less than 10 percent of the U.S. population ever opts out of a mailing list, and often the figure is less than three percent.[4] More surprising were the results of a late September 2001 survey revealing that 35 percent of the 1001 respondents could not recall even receiving a financial privacy notice, even though the average American had received 20 (Star Systems 2002: 9).

This suggests that recent privacy mandates that condition the collection and use of information on providing notices and obtaining consumer consent impose costs without generating meaningful benefits. As FTC chairman Timothy Muris (FTC 2001) has noted,

> The recent experience with Gramm-Leach-Bliley privacy notices should give everyone pause about whether we know enough to implement effectively broad-based legislation based on notices. Acres of trees died to produce a blizzard of barely comprehensible privacy notices. Indeed, this is a statute that only lawyers could love—until they found out it applied to them.

The Special Problem of Opt-In

The burden of privacy laws is even greater when their rules forbid the use of information without affirmative, opt-in consent. The traditional standard for privacy protection in the United States is opt-out. It allows personal information about an individual to be freely used

[4]Less than 3 percent of the U.S. population takes advantage of the Direct Marketing Association's Mail and Telephone Preference Services (U.S. Congress 1999). Financial institutions, retailers, and other businesses report similar or lower figures for their opt-out programs.

within defined legal limits so long as the individual does not expressly prohibit such use (i.e., "opts out"). Under *opt-in*, the collection and use of personal information is prohibited unless the individual expressly consents (i.e., "opts in").

While both opt-in and opt-out give consumers the same legal control about how their information is used, the two systems differ in the consequences they impose when consumers fail to act. Under opt-out, consumers like those under Gramm-Leach-Bliley who failed to read or respond to a privacy notice still received services. Under opt-in, consumers who did not respond could not have their information used. By virtue of not responding—whatever the reason—those subject to opt-in are excluded from receiving services.

Our experience with any system that tries to put control over how information is used into the hands of consumers suggests that there are not only many obstacles to consumers actually receiving and reading the notices but also a clear reluctance to respond to them at all—whether by opting out or opting in. Opt-in rates are virtually identical to opt-out rates, if not lower. In one 2000 test, a major U.S. online service provider sent e-mail messages to two groups of approximately 90,000 randomly selected customers each, describing its desire to use personal information to market to them. One e-mail message said that the information would be used unless the customer *opted out* within 14 days. The other said the information would likely not be used unless the customer *opted in* within 14 days. Both e-mails included a link to the notification preferences section of the user profile. The response rates were nearly identical for both groups: 4.41 percent for the opt-out group and 4.55 percent for the opt-in group. More than 95 percent of both groups did not respond at all.

In any case, the two systems diverge significantly in the burdens and costs they impose. Opt-in imposes considerable costs on consumers, because every consumer must be contacted individually to obtain consent to collect information, and again every time a new use for the information is proposed. U.S. West found that an opt-in system was significantly more expensive to administer, costing almost $30 per customer contacted (Brief for Petitioner and Interveners 1999: 15–16).

An Ernst & Young (2000: 16) study of financial institutions representing 30 percent of financial services industry revenues found that financial services companies would send out three to six times more direct marketing material if they could not use shared personal information to target their mailings, at an additional cost of about $1 billion per year. The study concluded that the total annual cost to consumers of opt-in restrictions on existing information flows was

$17 billion for the companies studied, or $56 billion if extrapolated to include the customers of all financial institutions. Those figures do not include the additional costs resulting from restricting information flows, such as fewer and less effective efforts to reduce fraud, increase the availability and lower the cost of credit, provide co-branded credit cards and nationwide automated teller machine networks, and develop future innovative services and products. Opt-in is more costly precisely because it fails to harness the efficiency of having customers reveal their own preferences as opposed to having to explicitly ask them.

Opt-In Restricts Competition, Entry into New Markets, Innovation, and E-Commerce

According to Robert Litan, director of economic studies at the Brookings Institution and a former Deputy Assistant Attorney General of the United States, switching from an opt-out system to an opt-in system would "raise barriers to entry by smaller, and often more innovative, firms and organizations" (Litan 1999: 11). Information sharing allows new businesses to break into markets and smaller businesses to compete more effectively with larger ones. New and smaller businesses lack extensive customer lists of their own or the resources to engage in mass marketing to reach consumers likely to be interested in their products or services.

Today, if a company wishes to expand into a new geographic area or product line, it may seek a list of potential customers from a third party. Under opt-out, a third party is free to provide the company with such a list, provided that it excludes consumers who have already opted out of receiving such communications. The company can then use the list to contact people with a special offer or introductory discount. After receiving the offer, consumers are free to opt out of receiving future offers from that company. The only "harm" suffered by the individual is receiving an offer in which he or she ultimately was not interested.

Under opt-in, every person on that list will need to be contacted for consent. The company cannot contact them, because it does not have explicit consent to make such a use of their names or addresses. The third party supplying the list is unlikely to bear the expense and inconvenience of contacting every person on the list. The promise of explicit consent in the opt-in requirement thus results in nothing to consent to at all.

Because of the difficulty of businesses contacting consumers individually, many consumers may miss out on opportunities that they

would value, not because they chose not to receive them, but because they never had the opportunity to choose. When that happens, opt-in creates only the illusion, not the reality, of consent.

Moreover, if the cost of obtaining consent becomes too great to make the proposed use of information economically feasible, then there will be nothing to which the consumer can consent. Many beneficial uses of information that consumers now enjoy depend on spreading the cost of collecting and maintaining the information across a variety of uses. If an opt-in law makes obtaining consent for those other uses difficult or prohibitively expensive, then the data and systems that they help fund might no longer be available for *any* use—including the ones that the public values most.

The Limits of Consent and Consent

In some cases, consent may be not only illusory but undesirable as well. There are many beneficial uses of personal information where the benefit is derived from the fact that the consumer has *not* had control over, or perhaps even notice about, the use of the information. For example, this is true of credit information. Its value derives from the fact that the information is obtained routinely, over time, from sources other than an individual consumer. FTC chairman Muris (FTC 2001) observes that the credit reporting system "works because, without anybody's consent, every sensitive information about a person's credit history is given to the credit reporting agencies. If consent were required, and consumers could decide—on a creditor-by-creditor basis—whether they wanted their information reported, the system would collapse." Requiring contact with the consumer before the information could be collected or used, or allowing the consumer to block use of unfavorable information, would likely make such records useless.

This is especially true in medical research and treatment. Even when information is not particularly "positive" or "negative," its value often depends on its being complete. Identifying unusual patterns or abnormal behavior or reactions requires access to a complete set of data.

Finally, there are some uses of information so valuable, or the risk of harm so little, that it would seem to make sense to permit use in any event. This is also important in the context of health privacy, both because of the extent to which the development of new treatments and drugs depends on the widespread availability of information, and because of the important distinction between privacy of the body—the right to refuse treatment or to choose among medically appropriate treatments—and privacy of information *about* the body.

Helena Gail Rubenstein (1999: 203) observes:

> Privacy, which is intertwined with the concept of control over what is disseminated about oneself, is an expression of autonomy. . . . [W]hile autonomy is an appropriate framework for evaluating questions concerning the treatment of one's body, it is not the appropriate framework for evaluating rules to regulate the use of health data.

Those who wish to condition the collection and use of health-related information on consent—without regard for the value of its other uses or its potential for causing harm—refuse to recognize "in exchange for the vast improvements in medical care, a correlative responsibility on the part of the individual, as a consumer of health care services, toward the community," notes Rubenstein. "As individuals rely on their right to be let alone, they shift the burden for providing the data needed to advance medical and health policy information. Their individualist vision threatens the entire community."

These considerations and the experience gained from recent privacy laws suggest the real limits of a notice-and-consent-based approach to protecting privacy. Most consumers ignore notices entirely. If consent is sought, they either provide it unthinkingly, just to get on with the transaction at hand, or, if contacted later for consent, they tend not to receive, read, or act on the request. Even in the rare instances where the consumer does respond, there may be good reasons why consent is nevertheless inappropriate.

Privacy and the First Amendment

Because privacy laws control the collection and use of expression, and inevitably restrict expression, they are subject to constitutional attack under the First Amendment. When presented with those challenges, the Supreme Court has consistently upheld the right to speak or publish or otherwise use information under the First Amendment, to the detriment of the privacy interest.

For example, the Court has rejected privacy claims by unwilling viewers or listeners in the context of broadcasts of radio programs in city streetcars and R-rated movies at a drive-in theater. It has consistently dismissed claims that unsolicited commercial mail or telephone calls constitute an invasion of privacy: Individuals need only "avert[] their eyes" or "terminate the call. Invasion of privacy is not a significant concern" (Edenfield v. Fane 1993).

The Supreme Court has struck down many ordinances that would require affirmative, opt-in consent before receiving door-to-door solicitations, before receiving communist literature, and even before

receiving "patently offensive" cable programming. The Court's opinion in *Martin v. Struthers* (1943: 141)—involving a local ordinance that banned door-to-door solicitations without explicit (opt-in) householder consent—is particularly apt:

> Whether such visiting shall be permitted has in general been deemed to depend upon the will of the individual master of each household, and not upon the determination of the community. In the instant case, the City of Struthers, Ohio, has attempted to make this decision for all its inhabitants.

Plaintiffs rarely win suits brought against speakers or publishers for disclosing private information. When information is true and obtained lawfully, the Supreme Court has virtually eliminated restrictions on its disclosure. Punishing the publication of true expression, the Court has written, is "antithetical to the First Amendment's protection" (Philadelphia Newspaper, Inc. v. Hepps 1986). The Court has struck down laws restricting the publication of confidential government reports and of the names of judges under investigation, juvenile suspects, and rape victims.

The Supreme Court reaffirmed the dominance of free expression interests in the recent case of *Bartnicki v. Vopper* (2001: 534). The Court explicitly balanced the constitutional interests in privacy and expression, and it held that the broadcast of an illegally intercepted cellular telephone conversation was protected by the First Amendment:

> Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society that places a primary value on freedom of speech and of press. Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period.

This suggests that laws that give individuals legal rights to restrict the use of accurate information about them will be upheld only if the government can show that the laws effectively alleviate a demonstrable harm.

This was certainly the view of the U.S. Court of Appeals for the Tenth Circuit when it was presented with a First Amendment challenge to Federal Communications Commission rules. The rules required U.S. West and other telephone companies to obtain opt-in consent from customers before using data about their calling patterns to determine which customers to contact or what offer to make to them. The appellate court found that the FCC's rules, by

limiting the use of personal information when communicating with customers, restricted U.S. West's speech and therefore were subject to First Amendment review. The court determined that under the First Amendment, the rules were presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were necessary to prevent a *"specific and significant harm"* on individuals, and that the rules were "no more extensive than necessary to serve [the stated] interests" (U.S. West 1999: 1235, emphasis added).

> Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial state interest under *Central Hudson* [the test applicable to commercial speech] for it is not based on an identified harm.

The court found that for the rules to be constitutional, the Commission first must demonstrate that less restrictive rules, such as opt-out, would not offer sufficient privacy protection. The appellate court found that the FCC could not do so, and it therefore struck down the rules as unconstitutional. The Supreme Court declined to review the case.

HIPAA Health Privacy Rules

In December 2000, HHS, as required by the 1996 HIPAA legislation, adopted rules protecting the privacy of personal health information. The rules proved so complex and so controversial that, in July 2001, the Department issued a "Guidance" to provide additional clarification, and then, in March 2002, it issued amendments to reduce the rules' unintended negative consequences and cost.

As amended, the rules regulate the use of information that identifies, or reasonably could be used to identify, an individual, and that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care. The rules apply to "covered entities," namely, anyone who provides or pays for health care in the normal course of business.

The rules permit a covered entity to use personal health information to provide, or obtain payment for, health care only if it provides a detailed notice about the intended collection and use of information, and makes a "good faith effort to obtain an individual's written acknowledgement of receipt of the provider's notice of privacy prac-

tices."[5] Those privacy notices must meet the specific requirements set forth in the amended rules, and the acknowledgement forms must be retained for six years after the date on which service is last provided. The notice need not be provided under limited circumstances, such as when the health care provider has an "indirect treatment relationship" with the patient or in medical emergencies.

A covered entity may use personal health information for purposes other than treatment or payment only with an individual's opt-in "authorization." An authorization must be an independent document that specifically identifies the information to be used or disclosed, the purposes of the use or disclosure, the person or entity to whom a disclosure may be made, and other information. A covered entity may not require an individual to sign an authorization as a condition of receiving treatment or participating in a health plan.

However, a covered entity may use or disclose personal health information for directories and to notify and involve other individuals in the care of a patient if the covered entity obtains the "agreement" of the individual. An agreement need not be written, provided that the individual is informed in advance of the use or disclosure and has the opportunity to opt out of the disclosure. This is the only consent requirement under the amended rules for which opt-out (rather than opt-in) consent is sufficient.

The HIPAA rules contain a number of exceptions, under which personal health information may be used without any form of consent. They include information used for public health activities; to report victims of abuse, neglect, or domestic violence; in judicial and administrative proceedings; for certain law enforcement activities; for certain research purposes; and for certain specialized governmental functions. The rules actually *lower* the protection afforded personal health information from government collection and use. A covered entity is required to release personal health information to the individual it concerns, and to the Secretary of HHS to investigate compliance with the privacy rules.

Under the rules, individuals have the right to access and copy their own personal health information from a covered entity or a business associate. They also have the right to amend information possessed by a covered entity. If the covered entity denies the request to amend the personal health information, the individual may file a statement that must then be included in any future use or disclosure of the information. Individuals also have the right to be informed of any

[5]67 *Fed. Reg.* 14,776.

disclosures a covered entity makes of personal health information about them.

Covered entities must make reasonable efforts to limit the use and disclosure of personal health information to the minimum necessary to accomplish the intended purpose. They may disclose personal health information to a business associate (such as a billing company, third-party administrator, attorney, or consultant) only if the covered entity has a contract ensuring that the business associate will be bound by all of the obligations applicable to the covered entity, and that, at the termination of the contract, the business associate with destroy or return all personal health information.

The rules do not apply to information that has been "de-identified," which the rules define as information that does not identify an individual and with respect to which there is no reasonable basis to belief that the information can be used to identify an individual. The December 2000 rules contained 18 identifying data elements that must be removed from personal health information before it can be considered "de-identified."

Health Privacy and the Public

The HIPAA privacy rules ignore many of the lessons we have learned from prior experience with privacy laws in the United States and elsewhere. For example, the rules ignore everything we have learned about the importance of using clear, narrow definitions to focus restrictions only on those information flows that could reasonably cause harm. The rules (45 C.F.R. § 160.103) define "health information" as:

> any information, whether oral or recorded in any form or medium, that:
> (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

This sweeping definition ensures that the rules will have effects far beyond what is necessary or intended to protect private health information, and exacerbates the cost and burden of compliance.

Similarly, for information to be considered "de-identified," and therefore no longer subject to the rules, it must not reveal "geographic subdivisions smaller than a State," except for certain circumstances where it is permissible to reveal "the initial three digits of a zip

code" (§ 164.514(b)(2)(i)(B)). The de-identified information must not reveal dates relating to individuals (such as birth date or treatment date) with any more precision than the year (§ 164.514(b)(2)(i)(C)).

These requirements are so broad and go so far beyond what is necessary to meaningfully de-identify personal information that they make the information useless as a basis for medical research. How would one study drug interactions without being able to specify the date of administration more closely than just the year, or identify the area in which an infectious disease has spread more precisely than just the state? In short, these requirements impose costs without achieving benefits.

Last March, in response to widespread criticism of these provisions, HHS sought public comment on whether some identifying elements might be retained if the information were to be used solely for research purposes. But the proposal on which the Department sought comment would only allow the inclusion of "admission, discharge, and service dates; date of death; age (including age 90 or over); and five-digit zip code."[6] Even if HHS were to adopt this modification, it seems unlikely to alleviate researchers' concerns.

The HIPAA privacy rules also wholly ignore the concept of harm and the constitutional requirement of targeting restrictions on information flows to specific harms. These and other examples of the shortcomings of the rules are well documented elsewhere.

The rules' greatest fault is their continued focus on notice and consent, and their reliance on opt-in as the means for manifesting consent. Despite all that we have learned about the costs and burdens of providing notices and obtaining consent, even in opt-out settings, the rules create a system of bureaucratic "acknowledgement" and "authorization" forms that promise little in the way of privacy protection, but considerable inconvenience and cost for consumers. The rules then further exacerbate the burden and expense that they impose by requiring, in those situations where consent is necessary, that consent be manifest by opting in.

The effect of the rules is that when patients visit a physician or other health care provider, they will face—before being seen—not only the existing range of forms concerning payment authorization, assignment of benefits, past medical conditions, and the like, but also a detailed privacy notice and acknowledgement form. To be certain, this is an improvement over the situation created by the December 2000 version of the rules, which would have required individuals to

[6]67 *Fed. Reg.* 14,776

sign actual consent forms before they could be treated. The rules provide exceptions for emergency conditions and health care providers who are consulting with, or providing services to, another health care provider that has already obtained consent

But experience tells us—and should have told the regulators—that these new, expanded privacy notices will be treated with the same neglect as current privacy notices and other legally required health forms. Individuals will flip through them quickly, looking for a place to sign, so that they can obtain the services they seek as soon as possible. Yet the health care provider is subject to a fine if it fails to provide the forms, or seeks or uses personal information without providing the required notice and acknowledgement form, or does not retain the form in storage for *six years* after the date on which service is last provided (§ 164.530(j)(2)). Individuals will encounter these notices and acknowledgement forms not only when they visit their physicians, but also when they deal with hospitals, pharmacists, laboratories, physical therapists, insurance companies, and anyone who uses personal information for treatment, payment, or other health care operations.

Should it later prove necessary to use information in a manner not covered by the initial notice, the entity covered by the rules presumably will have to track down the individuals concerned and provide new notice and acknowledgement forms. Given the experience to date of companies trying to comply with such requirements, it seems likely that few individuals will even be aware of the new notices and that fewer still will actually read them. Consumers will pay the price—both in dollar costs and inconvenience—of HIPAA's notice and acknowledgement requirements, but it seems unlikely that they will receive any benefit. Most will ignore the notices, and those few who do read them will have no opportunity to express disagreement other than by seeking service elsewhere—which they could have done prior to the enactment of the rules in any case.

To use information for any purpose not directly relating to treatment, payment, or "health care operations," entities covered by HIPAA must obtain a separate, explicit, opt-in authorization from individuals (§ 164.508(a)(1)). Authorizations are required for marketing, fund-raising, pre-enrollment underwriting, and employment-related related determinations, among other uses. This authorization is different from the notice and acknowledgement process described above. It must be contained in a separate document and provide far more detailed information (§ 164.508(b)(3), (c)–(f)). Moreover, HIPAA prohibits covered entities from conditioning service on individuals' willingness to authorize the requested use of personal infor-

mation (§ 164.508(a)(4)). The HIPAA rules, therefore, appear to prohibit health care providers and payors from offering discounts to individuals who contribute to lower health care costs and more efficient operations by consenting to the responsible use of information about them. Instead, everyone must subsidize the privacy, or the simple failure to act, of every other person.

How the public will respond to a new wave of authorization requests is difficult to predict. For those individuals who do review the authorization forms, the real question is whether individuals simply will sign them routinely along with the stack of other forms presented when they visit a health care provider. Or will media stories and the activities of privacy advocates scare them into not signing any authorizations at all?

It seems most likely that, as is the case for similar long and cumbersome opt-in requirements elsewhere, most people will not even read them. That's particularly true for authorization requests that are mailed *after* service is provided. Current trends suggest that half will be discarded without being read, and the rest will provoke a handful of people, a few percent at most, to provide the requested authorization.

As a result, it appears certain that there will be less information available to help remind individuals to take prescribed medications, to inform them of alternatives, and to offer discounts and bulk-buying programs. Yet it remains unlikely that it will appear to most consumers that their privacy is better protected. Businesses will still be free to use the information they extrapolate from grocery purchases, online browsing habits, and other activities—alternative sources of information that appear to reveal something about the health condition of individuals. The end result may be that, while few consumers perceive any significant increase in their health privacy, they may miss the discounts, information, and other benefits they used to receive in return for broader health information sharing.

The cost for this flood of forms, together with the other requirements of the HIPAA rules, will be great. In economic terms, HHS calculates the compliance cost at $3.2 billion for the first year, and $17.6 billion for the first 10 years.[7] Health care consulting companies predict that the cost will be much higher—between $25 and $43 billion (or three to five times more than the industry spent on Y2K) for the first five years for compliance alone, not including the rules impact on medical research and care or liability payments (Nolan 1999; Fitch IBCA 2000; Kirchheimer 2000: 48).

[7]65 *Fed. Reg.* 82,761, Table 1.

In noneconomic terms, the cost also will include the annoyance and wasted time of more forms that individuals are told they *should* read at the time of service; more follow-up contacts from covered entities seeking to get them to read and acknowledge privacy notices and sign authorization forms that were sent *after* service; the confusion of facing one set of forms for notice and acknowledgement and an entirely different set for authorization; and the greater consequences of not acting than they face today under opt-out rules.

While the HIPAA rules impose new restraints on private-sector collection and use of personal information, they actually reduce the standard by which the government may obtain access to health information. The rules lower the legal requirement for government access to medical records from a court-issued warrant to an administrative subpoena, despite the fact that it is freedom from government intrusion that is the only "right to privacy" protected in the U.S. Constitution.[8]

Ironically, HIPAA's federal health privacy rules originally developed as a reaction to HIPAA's other push for more uniform electronic data standards. The legislation's "administrative simplification" provisions were aimed at reducing costs and making health benefits more portable, by smoothing and accelerating the flow of health and health insurance information. But political demands for greater individual control of personal health information pushed HIPAA privacy rules in the opposite direction. Indeed, federal regulators declined to preempt more restrictive state privacy rules, inviting states to go beyond the minimum federal privacy standards set under HIPAA.[9] Depending upon how many states take advantage of that opportunity, the HIPAA rules may well force covered entities to provide, and individuals to decipher, inconsistent notice, authorization, and even consent forms.

The costs of the HIPAA privacy rules will be borne not just by patients and covered entities, but by all people who benefit from medical research and innovation. Medical researchers rely on personal information to conduct "chart reviews" and perform other research critical to evaluating medical treatments, detecting harmful drug interactions, uncovering dangerous side effects of medical treatments and products, and developing new therapies. Such research cannot be undertaken with wholly anonymous information, because the detailed data that researchers require will always include infor-

[8]45 C.F.R. § 164.512(f)(1)(ii).
[9]See § 160.203(b).

mation that could be used to identify a specific person. Moreover, when that information indicates that a given therapy or drug poses a significant health risk, researchers are required by law to notify the affected individuals.

While it is clear that the March 2002 amendments reduce the negative effect of the health privacy rules, the impact of those changes is likely to prove small. Even HHS calculates that the amendments will reduce the cost of complying with the rules by only $100 million over 10 years, less than one-half of one percent of the original estimated price tag of $17.6 billion.[10]

The revised rules continue to rely on a bureaucratic system of notices and acknowledgements for health care treatment and payment, despite all of the evidence indicating how little value such notices provide most consumers and how inefficient individualized notice systems are. And the rules continue to condition most other uses of health information, including much medical research, on notices and opt-in authorizations, despite the inherent limits of opt-in consent systems.

Principles for Health Privacy Protection

There is no question but that health privacy is important and should be protected as a matter of law. However, the issue raised by the HIPAA rules is whether health privacy can be protected as well, or even better, at lower cost. I believe that our growing experience with privacy laws and regulations in other sectors tells us that the answer is "yes." That experience suggests five principles that regulators would do well to consider. They should focus on harm, not control; use narrow, precise definitions; employ appropriate consent requirements; apply regulations consistently; and evaluate the constitutionality of rules.

Focus on Harm, Not Control

The consistently low consumer response rates to either opt-in or opt-out requests suggest that most consumers do not want to bother with trying to exercise legal control over their information. They want to be protected from the harmful use of that information. This approach is more consistent with past U.S. privacy protections. It has fewer and less burdensome unforeseen consequences. It is more

[10]67 *Fed. Reg.* 14,805.

likely to prove constitutional. We should regulate harmful use, not the open and innocuous collection of information.

Use Narrow, Precise Definitions that Focus on Reasonable Expectations of Privacy

Regulators should use narrow, not expansive definitions. Financial regulators expanded Gramm-Leach-Bliley's definition of "personally identifiable financial information" to require that the information be neither personally identifiable nor financial.[11] HIPAA reflects the same tendency. As written, the health privacy rules apply to gossip, scraps of paper, and information like state of residence and year of treatment. Ironically, the introduction to those rules discusses at length the Fourth Amendment right to be free from "unreasonable searches and seizures." What the introduction fails to mention is that the Supreme Court has found that a search or seizure can be unreasonable only when it invades a "reasonable expectation of privacy." The Court has found that privacy expectations are reasonable only if the individual actually believed the information was private and there is objective support for that expectation.[12] The HIPAA rules are so broad that they apply to information that no one considers private and that is patently unreasonable to treat as such. A narrower focus would be more likely to protect consumers from harm yet avoid burdening all of society with restrictions applicable to information that involves no reasonable privacy interest.

Employ Appropriate Consent Requirements

If there is anything we have learned over the past decade in the realm of privacy, it is that the mechanisms specified for obtaining consent should be appropriate to the information being collected and the setting in which the collection is taking place. By requiring written notices and acknowledgements for the use of information that is necessary if service is to be provided, the HIPAA rules burden patients without yielding commensurate benefits. Why do people go to doctors, if not to provide the information necessary to be treated? Similarly, requiring separate, opt-in consent for what includes wholly innocuous uses of often impersonal information (for example, the use

[11]12 C.F.R. §§ 40.3(o), 216.3(o), 332.3(o), 573.3(o).

[12]Terry v. Ohio, 392 U.S. 1, 9 (1968); Smith v. Maryland, 442 U.S. 735, 740 (1979).

of a name and address to mail a fund-raising letter from a hospital) is difficult to justify, either constitutionally or practically.

Behave Consistently with Legal Requirements Imposed on Others

Regulators should apply legal requirements for privacy consistently. Unfortunately, the government has a well-established habit of seeking to impose privacy requirements on others that it cannot live up to itself. For example, state legislators have taken many steps to restrict unsolicited mail and telephone calls, but they have consistently exempted themselves and their own fund-raising efforts. The FTC appealed to Congress in 2000 to enact online privacy laws, because, as of May 2000, only 88 percent of commercial Web sites (100 percent of the busiest commercial Web sites) had voluntarily posted a privacy policy (FTC 2000). However, six months later the General Accounting Office found that only 85 percent of federal government agency Web sites posted a privacy policy (GAO 2000: 3), despite a directive more than a year earlier from Office of Management and Budget director Jack Lew compelling them to do so (Lew 1999). A September 2000 Brown University study of 1,700 state and local government Web sites found that only seven percent posted a privacy policy (West 2000). If the government is serious about protecting the privacy of medical information, it certainly should not allow HIPAA rules to lower the protection afforded such information from government intrusion, and it should make certain that its own agencies are prepared to comply with the onerous burdens those rules impose.

Evaluate the Constitutionality of Rules

Given that the HIPAA rules require opt-in consent, it seems certain that they will have to pass "strict scrutiny." The government will have to show that the rules serve a compelling interest and that they are the least restrictive method of achieving that interest. While it is likely that protecting personal privacy would constitute a sufficiently important interest, by no stretch of the imagination could the government make, much less support, the claim that these rules are the least restrictive way to do so. Given the extent to which it is already clear that the rules will not even serve the interest of protecting privacy, it is difficult to imagine how they could be the least restrictive way of doing so. A good place to start in constitutional analysis of HIPAA privacy rules, and one required by the Tenth Circuit in *U.S.*

West, is to answer the question: "Why won't opt-out work just as well?"

It is ironic that the introduction to the HIPAA rules discusses at length the Fourth Amendment right of privacy and the right to "informational privacy" recognized by the Supreme Court in *Whalen v. Roe*.[13] Unfortunately, the rules' drafters failed to note that both the Fourth Amendment and the privacy right identified in *Whalen*, as with all constitutional rights, apply only against the *government*. The government may not unreasonably search and seize and the government may not compel disclosure of personal matters in certain circumstances. The private sector, by contrast, is free to do so, at least from a constitutional perspective.

Privacy presents many complex issues to which there are no easy solutions. This is especially true in the case of health privacy, where the availability and control of information inevitably and directly affect the efficiency, cost, and quality of medical treatment and research. The important, but modest, steps taken in the March 2002 amendments demonstrate that the federal government is not incapable of learning from its past mistakes. But the failure to go further and cut through more of the regulatory underbrush and complexity that has come to characterize these rules is disconcerting, especially in a context as critical as health care. A wrong step here will likely prove costly not only in terms of dollars and consumer burdens, but also in reducing access to medical care and compromising its efficacy. The recent avalanche of privacy activity has taught us many important lessons about this critical subject. Ignoring those lessons threatens not only our pocketbooks and convenience, but also our very lives.

References

American Bankers Association (2001) "ABA Survey Shows Nearly One Out of Three Consumers Read Their Banks' Privacy Notices." ABA News Release, 15 June.

Bartnicki v. Vopper (2001) 532 U. S. 514.

Brief for Petitioner and Interveners (2000) U. S. West, Inc. v. Federal Communications Commission: 15-16. 182 F.3d 1224, 1239 (10th Cir. 1999) (No. 98-9518), cert. denied 528 U. S. 1188.

Edenfield v. Fane (1993) 507 U. S. 761.

Ernst & Young LLP (2000) *Customer Benefits from Current Information Sharing by Financial Services Companies* (December). New York.

Federal Trade Commission (2000) *Privacy Online: Fair Information Prac-*

[13]429 U.S. 589 (1977).

tices in the Electronic Marketplace—A Report to Congress. Washington, D.C.
Federal Trade Commission (2001) "Workshop on the Information Marketplace: Merging and Exchanging Consumer Data." Washington, D.C. (31 March).
Fitch IBCA (2000) *HIPAA: Wake-Up Call for Health Care Providers*. New York: FitchRatings.
Kirchheimer, B. (2000) "Report Predicts Huge HIPAA Price Tag." *Modern Healthcare* (2 October): 48.
LaFalce, J. (2000) Statement at Democrat News Conference on Financial Privacy. Washington, D.C. (4 May).
Lew, J. (1999) Memorandum from OMB Director, Memorandum M-99-18 (2 June).
Litan, R. E. (1999) "Balancing Costs and Benefits of new Privacy Mandates." Working Paper 99-3, AEI-Brookings Joint Center for Regulatory Studies.
Martin v. Struthers (1943) 319 U. S. 141.
National Association of Attorneys General (2000) *Draft Statement on Privacy Principles and Background*. Washington, D.C. (11 December).
Robert E. Nolan Company, Inc. (1999) *Common Components of Confidentiality Legislation—Cost and Impact Analysis*. Dallas.
Rubinstein, H. G. (1999) "If I Am Only for Myself, What Am I? A Communitarian Look at the Privacy Stalemate." *American Journal of Law and Medicine* 25: 203–31.
Safire, W. (1999) "Nosy Parker Lives." *New York Times* (23 September): A9.
Smith v. Maryland (1979) 442 U. S. 735.
Star Systems (2001) "Financial Privacy: Beyond Title V of Gramm-Leach-Bliley." Star Systems Industry Research (November). (www.star-systems.com/news-industryresearch.html.)
Terry v. Ohio (1968) 392 U.S. 1.
U. S. Congress (1999) "Financial Privacy." Hearings before the Subcommittee on Financial Institutions and Consumer Credit of the Committee on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (20 July) (statement of Richard A. Barton). (Available at www.house.gov/banking/72099rba.htm.)
U. S. General Accounting Office (2000) "Federal Agencies' Fair Information Practices." GAO/AIMD-00-296R.
U. S. West, Inc. v. Federal Communications Commission (1999) 182 F.3d 1224 (10th Cir.), cert. denied, 528 U.S. 1188 (2000).
Walker, K. (2001) "Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange." *Stanford Technology Law Review*. (http://stlr.stanford.edu/stlr/articles/00_stlr_2.)
West, D. M. (2000) *Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments* (September). (www.brown.edu/Departments/Taubman_Center//polreports/egovtreport00.html#Security.)
Westin, A. (1967) *Privacy and Freedom*. New York: Atheneum.
Whalen v. Roe (1977) 429 U. S. 589.