Privacy in a Free Country: In Search of Reasonable Principles

by

Solveig Singleton
Competitive Enterprise Institute

NCPA Policy Report No. 243
April 2001
ISBN #1-56808-105-7

Web site: www.ncpa.org/studies/s243/s243.html

National Center for Policy Analysis
12655 N. Central Expressway, Suite 720
Dallas, Texas 75243
(972) 386-6272

Executive Summary

"Privacy" has often been thought of as a traditional American value, but the concept has always been difficult to define precisely. With the passage of time and the development of technology, particularly the ability to share information quickly and inexpensively, the issues involved have become increasingly complex.

For example, the use of new electronic surveillance technology by law enforcement officers is raising new questions about the limits of privacy and the reach of the Constitution's protections against search and seizure. Without ever stepping on your property, government agents can:

- Detect heat from a possible marijuana crop in your basement or detect activity in your bedroom, using thermal emissions equipment.
- Use electronic emissions readers to "read" a computer screen in your home.
- Use laser beams trained on a windowpane to "listen" to a conversation inside your home.

The determination by courts that business records, unlike personal records kept in your home, are not protected by the Fourth Amendment has allowed government fishing expeditions for illegal activity. For example, under a "know your customer" program, banks monitor customers' accounts for "suspicious activities" and "voluntarily" report them to regulators:

- The government collected 62 tons of paper covering 77 million currency transactions between 1987 and 1995 in an effort to catch money launderers.
- Yet since only 580 money launderers (most of them "small fry") were caught, the government collected more than 100,000 reports on innocent citizens for every criminal convicted.

In addition to banking, the federal government alone has hundreds of databases, some of which have been criticized for inadequate security, containing information about private citizens, and new government rules will create a centralized health information network and assign unique identifiers — national IDs — to all patients.

Moreover, even if strict rules are applied to government privacy, rogue employees can abuse those rules:

- When more than 500 Internal Revenue Service agents were caught illegally snooping through tax records of thousands of Americans in 1995, only five were fired.
- After the IRS developed new privacy protection measures, hundreds more agents were caught doing the same thing again in 1997.

In two other areas of privacy — consumer protection and employer/employee privacy — technology and innovations over the past few decades have also given rise to uneasiness as information is used in new ways.

Some people see the development of targeted marketing by businesses and the ability to track a customer's activities on a Web site as a threat to consumer privacy.

- One survey found that 86 percent thought Internet companies should ask permission before sharing personal information with third parties.
- Even so, 55 percent of Americans bought something online during the holiday season — and 86 percent reported they tried to buy, although technical problems prevented many from completing their transactions.

Many employers monitor employees' activities electronically or with video cameras, and some use medical or credit information in making hiring and promotion decisions.

- A survey in early 2001 reported that 61 percent of large businesses were monitoring workers' use of the Internet.
- Another survey concluded that 35 percent of Fortune 500 companies use medical information in hiring or promotions.

Despite the perception of a privacy crisis, there is excitement in the air about the potential for enormous gains in business and government administration and in consumer welfare and service from new uses of information. It would be wrong to shape public policy or pass laws based on the perception of a crisis or on the fears by some of technology and innovation.

Human beings rarely make better decisions by having less information about themselves and their fellow human beings. The principle that freedom of information should only rarely give way to privacy concerns is as reliable today as ever.

Introduction

Popular discussions of privacy today are characterized by sweeping generalities. One example is the assertion that people own information about themselves. But if people really owned information about themselves, journalists would never be able to write a story about someone without his or her permission. The idea of "privacy" has not been clearly defined. In casual conversation, "privacy" is a useful umbrella term that refers to all manner of situations where the use of information makes us uneasy. But when used in public policy, the vagueness of the term hinders real problem-solving. Having one's door broken down by police acting without a proper warrant is not like receiving an unwanted advertisement in the mail. Some privacy concerns are serious, but others are spurious.

"We have given the government broader and broader powers to gather information in ways not contemplated in the Constitution."

This paper examines privacy in four different areas — privacy from government, privacy as consumer protection, employer/employee privacy and medical privacy. Only employer privacy and privacy as consumer protection have much in common — both are a matter of contract law where there is no fiduciary relationship between the parties. Privacy from government is a matter of constitutional law, while medical privacy involves the special duties of a doctor to his or her patients.

What each of these areas has in common is a conflict between familiar norms of privacy and the pace of technological and cultural change. Yet we must still distinguish real harms from red herrings. Privacy red herrings will lead only to more red tape for business and higher costs for consumers. Targeted solutions to real harms are far superior. Only the case of government — which enjoys broad, unique powers — calls for omnibus prophylactic measures.

Government Access to Your Information

Discussions of privacy and government access to information customarily begin by noting that privacy is a traditional American value. A more realistic assessment is that privacy is one of many American values and not the most important to most people. One might even say that when it comes to privacy from government, privacy is a lost American value. We have given the government broader and broader powers to gather information in ways that were not contemplated in the Constitution.

Dangers of Government Access to Information

Some see the gradual abandonment of privacy from government as a good thing.[1] After all, how can we expect government to do a good job without information about its citizens? But, given government's unique ability to control the police, the armies and the courts, can we trust government with any broad powers?

The Three Risks of Government Information-Gathering. Essentially, there are three main reasons to worry about government access to our information. These include:

- The Rogue Employee Problem. The danger that "rogue" government employees will use our information for their own personal ends.

  Example: In 1995, more than 500 Internal Revenue Service agents were caught illegally snooping through tax records of thousands of Americans, including personal friends and celebrities. Only five employees were fired for this misconduct. In response, the IRS developed new privacy protection measures. Despite these measures, hundreds of IRS agents were caught in early 1997, again snooping through the tax records of acquaintances and celebrities.

"IRS agents were caught snooping through tax records in 1995 — and again in 1997."

- The Threat to Human Rights. The danger that an entire government may, under color of law, use this information to oppress the population in general or to target an unpopular political, religious or ethnic minority.

  Example: During World War II, U.S. census data were used to identify Japanese-Americans and place them in internment camps.

- Brutal Methods of Collection. The danger that a government may use brutal or unfair methods (such as a warrantless search or torture) to collect information.

  Example: In 1974, United States agents reportedly abducted an Italian citizen from Uruguay by clubbing him with a gun and throwing him into the back seat of a car in front of his pregnant wife; for three weeks he was subjected to torture and denial of food before being illegally taken for trial on narcotics charges in the United States.[2]

Heightening the Risk: Lack of Government Accountability. Exacerbating all three dangers is the problem of holding government agents accountable even for gross violations of human rights. In general, one cannot sue the government, and it is rare for government employees to be fired for misconduct. You have no choice but to deal with the government — you cannot go to a competitor. If a clerk working for a private law firm violates the firm's obligation to keep information confidential, the clerk is likely to be fired, and the law firm stands a good chance of losing its client to another firm. This means that law firms have a cultural atmosphere in which client confidentiality is taken very seriously. It is much more difficult to create such an atmosphere in a government office where, even if "mistakes were made," no heads will roll.

"It is difficult to hold government agents accountable even for gross violations of human rights."

How The U.S. Constitution Addresses the Problem. Only one of these dangers, the risk that brutal methods will be used to collect information, is directly addressed by the U.S. Constitution.

- The Fourth Amendment protects us against overly broad or warrantless searches.[3]
- The Fifth Amendment shields us from self-incrimination, which should prevent us from being tortured into making confessions.

The framers were able to draft effective general principles to prevent these practices because the problems they addressed were familiar to them. They knew of the use of torture even in civilized countries in their recent history. They also had had many unpleasant experiences with the so-called general warrant used in America in colonial times. A general warrant allowed the authorities to randomly shuffle through one's house and papers fishing for evidence of lawbreaking. The Fourth Amendment prevents such random searches by stipulating that the warrant must describe what is to be seized with particularity. It also makes the executive branch of government, including the police, accountable to the judiciary before a search is conducted.

Because of the Fourth and Fifth amendments, U.S. citizens enjoy far more privacy than most people around the world most of the time. That the Constitution has proved durable in this respect is no mean feat. Overall, however, the balance of power between government information-gatherers and private individuals has shifted in favor of government. A partial list of the direct and indirect ways that government now collects information about us is shown in Exhibit I.

"U.S. citizens enjoy far more privacy than most people around the world because of the Fourth and Fifth amendments."

Exhibit I

Ways Government Can Collect Information

Direct	Indirect
Search and seizures	From your employer
Heat images of your home	From your banker
Phone and e-mail taps	From your doctor, hospital or insurance company
Tax forms	From your children's school
Applications for programs like welfare	From your credit card company
	From driver's license applications
The national census	From other government agencies

Government Information Gathering in the Twentieth Century

The federal government alone has literally hundreds of databases containing information about private citizens, some of which have been criticized for inadequate security. This growth in government monitoring has come about despite the Fourth and Fifth amendments because of two important trends.

Trend: New Electronic Surveillance. The first trend that has tended to erode privacy is the development of new communications and surveillance technologies that endow the police with new powers. Take wiretapping. When wiretapping was first invented, it was not illegal. Beginning in the late 19th century, wiretapping became a widespread method of police investigation. Wiretaps were also used by feuding private parties[4] and by criminals. But wiretapping was controversial, and many states passed statutes governing its use. In 1928, the Supreme Court ruled that wiretapping without a warrant did not violate the Fourth Amendment because placing a tap on the telephone company's wire was not a search of the suspect's property.[5] In response, many states amended their constitutions to preclude wiretapping.[6] In 1967, the Supreme Court changed its mind. In *Katz v. United States*[7] the court found that wiretappers must comply with the Fourth Amendment even when a wiretap does not involve a trespass. Indeed, the Court abandoned the rule that a privacy violation can only be a property rights violation. The new rule is that the Fourth Amendment protects us from infringement on a reasonable expectation of privacy.[8]

"Law enforcement agencies outside your home can read your computer screen, listen to your conversations or monitor your activity in a bedroom."

This modern standard is problematic. As several commentators have noted, it is circular.[9] Whether or not one has an expectation of privacy will depend on whether the law says one does. It is hard to see how anyone would have had a reasonable expectation of privacy in a phone call, either in 1928 when wiretapping first came before the Court or in 1967 when the Court's previous determination that the police could place wiretaps without a warrant was still on the books.

Most importantly, the "reasonable expectation" gives courts no help when new communications technologies and surveillance methods are developed. Consider the following methods of surveillance:

- Thermal emissions equipment that records heat (infrared radiation) being radiated from one's home, including activity in a bedroom.[10]
- Electronic emissions readers that allow police to read the screen of one's computer even outside the room.[11]
- Laser beams that can be trained on a windowpane and pick up human speech inside a room.

When devices such as these are introduced, how would anyone have a reasonable expectation as to whether they would be used? On the one hand,

one could presume that no one expects such devices to be used. On the other hand, one might with equal plausibility assume that everyone expects to be subjected to devices that make the formerly invisible visible.

This philosophical weakness in the constitutional law means that the Fourth Amendment has been of little use in protecting privacy against incursions by advanced communications technology. Thus the matter is left to Congress, which has passed federal legislation on electronic interceptions — but usually gives broad power to law enforcement.

Trend: Regulatory Access to Business Records. The second trend is a move toward larger, more regulatory governments at the federal and state level. At first, many of these new regulations were directed against businesses. As the politics of the New Deal became dominant, the idea that businesses had constitutional rights became disfavored in the intellectual and legal community. One outcome was the courts' determination that business records, unlike personal records kept in your home, are not protected by the Fourth Amendment.

This has opened up whole new avenues for the government to collect information. The police need not search your home or your papers. Instead, they can simply ask your employer, or your banker, or any business with which you deal to turn over all of their customer records. They can then fish through the reports looking for illegal activity.

One example is the "know your customer" reporting requirements for banks. A few years back, the Federal Deposit Insurance Corporation proposed to make these reporting requirements into law. Under the "know your customer" program, banks must monitor customers' accounts for "suspicious activities" and report them to bank regulators. Suspicious activities include ordinary acts such as using large amounts of cash or using the night deposit box frequently. The attempt to pass formal "know your customer" rules was defeated when thousands of people wrote to complain. But what many people do not know is that the "know your customer" program already exists as a regulatory program with which banks comply "voluntarily" (under substantial pressure from regulators).

"Under the 'know your customer' program, banks 'voluntarily' report on their customers."

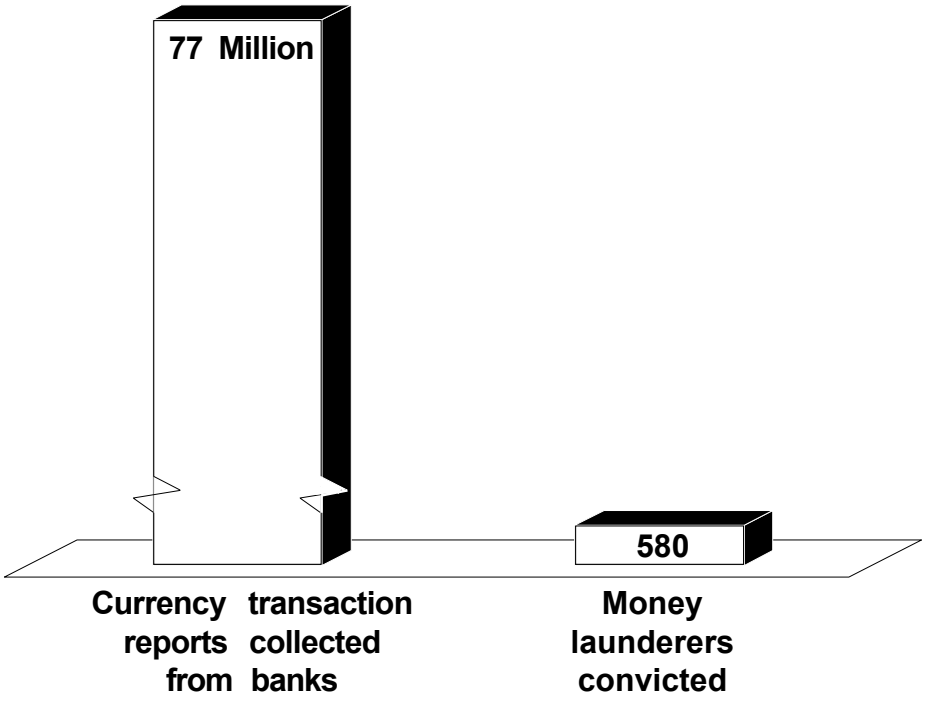
- Between 1987 and 1995, the government collected more than 77 million "currency transaction reports" — 62 tons of paper.
- The collection was intended to help enforce money-laundering laws, but only 580 money launderers were convicted — most of them "small fry."
- More than 100,000 reports on innocent citizens were collected for each conviction.[12] [See Figure I.]

The fact is that businesses, whether acting as your employer or your banker, have in essence no Fourth Amendment leg to stand on when the

"The government collected more than 100,000 reports on innocent people for every money laundering conviction."

FIGURE I

Chasing Money Launderers, 1987-1995



Source: Lawrence Lindsey, "The Money-Laundering Conundrum: Mugging Privacy in the Assault on Crime?" in *The Future of Financial Privacy: Private Choices versus Political Rules* (Washington, D.C.: Competitive Enterprise Institute, 2000).

regulators come calling. In any case, they have no obligation to protect their employees or customers, and even with Fourth Amendment rights, they might be urged to cooperate with authorities voluntarily. But it is unlikely they would do so to the extent of imposing millions of dollars of mandatory reporting costs on themselves.

Other Government Information-Gathering. When the government collects income tax filings, welfare applications, student loan applications and so on from private citizens, there is no physical search and seizure. In these contexts, we cheerfully hand government vast amounts of information without any constitutional limits so as to avoid jail or to obtain benefits such as subsidies, welfare or a driver's license. People who object to such information-gathering are considered quite eccentric. However, many Americans would be surprised by the extent to which information collected by government for one purpose is used by it for another.[13] For example, national Census data are shared with city governments that wish to limit the number of people living in a housing unit. This is a controversial practice because most homes that are

shared among extended families are those of immigrants and other poor people, who are more likely to have difficulty finding other housing once city officials rule that they cannot continue to live together.[14]

Privacy in a Context of Limited Government. Some may not view the erosion of privacy from government as a particularly serious problem. Privacy is not an absolute right. How could government administer an income tax without gathering information about income? A welfare system without tracking fraud? A social security system in a world with millions of people named "Smith"? A regulatory system with none of the information needed to safeguard consumers? How could one fight crime without the means to identify suspects and criminals? Americans have consistently voted for larger governments that are more and more involved in our day-to-day lives. How can the programs and benefits we want be provided efficiently without information? The answer is that for the most part they cannot be. And the U.S. government has not had the history of egregious abuses that some governments in Europe, Africa or South America have had. Privacy is a right relevant to a world in which the concept of a limited government is still important. American voters have long since abandoned such a world.

"Government cannot provide many of the programs and benefits Americans enjoy without information about people."

Why, then, battle to rescue privacy? Because the key concepts of limited government are not outdated at all. Expansive government programs like Social Security and welfare, we are discovering, do not work well. More and more laws are passed that punish mere paperwork offenses rather than real moral wrongs. We may often have given up much of our privacy for no good reason. And the dangers that government information-gathering pose as a whole have not gone away. The fact that the U.S. government has not committed any (or perhaps, been detected committing any) really high-profile abuses since Watergate does not mean that none will happen. If one were to take a survey of 20th-century governments worldwide, one would find that America's apparent respite from abusive surveillance, if we are indeed having one, is a rare historical moment indeed.

It is as difficult to carry on a sustained public debate about privacy from government as to maintain any other aspect of limited government — for example, low taxes. Every new government program adds a few cents to our yearly tax burden — and who cares about a few cents? No one does, so those who object to each program's creation are easily seen as hysterical or petty. But the programs add up, and taken altogether they have led to a massive growth in government power and spending. Privacy is the same way — every new intrusion may seem appropriate in isolation, dressed up as crime prevention or another aspect of the public welfare. Taken altogether, the intrusions represent a significant shift away from our constitution of limited powers.

Principles for Public Policy. In policy debates about government access to information in the future, these principles may be helpful:

- Unless businesses have Fourth Amendment rights, they cannot protect their customers' privacy rights if they choose to do so.
- People should be able to use technology as a counterbalance against new surveillance technology, because there is no effective constitutional protection in that area.
- New institutions within government should be developed so the different branches of government can check one another's practices.
- When new government services or powers are granted, privacy and security should be built into the system.
- Government employees should be held accountable for careless or deliberate abuse of information.

It is important not to cry "privacy wolf" too stridently. When no disasters are immediately forthcoming, the public perceives those who raised the cry as hysterical or paranoid. Privacy as an absolute or isolated value before which all else must give way makes little sense. But privacy does make sense as part of an overall discussion on whether we have moved too far from the government of limited powers the framers envisioned. And it does make sense to limit the systemic dangers of the rogue employee or the oppressive regime.

Privacy as Consumer Protection

In the case of the constitutional limits on government access to information, it is clear what citizens are being protected from: the unique powers of government to control law enforcement and the military, to arrest people for trial, to determine which acts are illegal and which are not, and so on. Businesses gather information about their customers' buying habits, and sometimes trade this information with other businesses. So long as the information is secure from criminals, there is little harm likely to result from this. For a minority of sensitive purchases, it is possible that marketing information could leak out and embarrass the consumer, but embarrassment is just as likely to result from a co-worker's wandering into one's office at the "wrong" time, an e-mail sent to the wrong address, or a neighbor's overhearing a conversation through thin walls. Marketing information is stored in vast, secured arrays that cannot be easily read by any human being; it is rarely, if ever, kept in personal dossiers sorted by name and address.

"Many consumers and privacy advocates see business as a sinister 'Big Brother.'"

Now, many consumers and privacy advocates see business as a sinister "Big Brother." Changing technology and business methods are at the root of this unease. The new technologies can exacerbate real harms that need real solutions. But more often the new information tools are beneficial, and individuals can act to withhold personal information from others. In general,

therefore, consumer unease about business information-gathering requires no broad legislative solution.

New Uses of Information that Affect Consumers

Attitudes to changing technology are at the root of the issue of privacy as consumer protection**.** The following are some examples.

The Development of Targeted Marketing. One relatively recent development that has fed concerns about privacy is the practice of targeted marketing. Especially throughout the '90s, businesses were responding to consumers' hatred of "junk mail." Consumers were unhappy with the number of irrelevant offers piling up in their mailboxes. The business response was to develop more targeted marketing schemes to avoid sending unwanted material. To do that, businesses needed to learn more about customers' preferences and to identify groups or classes of customers with particular interests. This began well before the Internet, and so long as it involved familiar mainframe computer technology and stand-alone networks was not perceived as particularly threatening. Indeed, from the standpoint of consumers, it was a very popular change. Catalog sales grew from $64 billion in 1995 to $104 billion in 2000.[15]

The Internet and the Demonization of Cookies. Next, the Internet came along — a new and thus inherently more scary technology. On the Internet, entrepreneurs trying to commercialize the medium for the first time had a particular problem. Imagine an ordinary shopkeeper with a little store in the corner of a very big mall. As he stands at the counter, he watches customers come in. He can see whether they are regulars or strangers, can get a fair idea whether they are locals or tourists, German or Spanish, young or old, male or female. Are they missing the special display in the back? Is it too dark? Do they look longingly at the stuffed monkeys, but comment that the price is just a little too high? The traditional operator of a Web site has none of this information. None of it. It is as if he is deaf, dumb and blind. He can learn nothing about his visitors. And thus he has little chance of improving his service to customers, unless he hits upon their needs by sheer dumb luck. Thus, cookies were born.

"Cookies are intended to help Web sites become viable commercial enterprises."

What are cookies, and what do they do? Invented by Internet pioneer Lou Montulli in 1994, when he was working for the brand new Netscape, cookies are intended to help Web sites become viable commercial enterprises. Cookies are little data files that are saved to an Internet user's computer, usually temporarily but sometimes permanently. For example, these files record how many times a user has seen a certain banner ad, track purchases loaded into online shopping carts, etc. They help Web sites identify a regular visitor, so the visitor need not reenter identification every time. Cookies tell the server, "this visitor has been here before" or "this visitor has an orange T-

shirt and a pair of jeans in his shopping cart." Cookies cannot access your name or your e-mail address until you type that information into an online form.

However, increasingly the press has treated cookies as some form of sinister surveillance, especially when used by third-party advertisers. Most Web sites today make money from selling advertising. But the advertiser is wasting his money if none of the customers who see his ad are interested in it. So banner ads on the Internet also use cookies to store bits of information such as "this consumer has seen this ad three times already." The advertisers' cookies may continue to store such information as the consumer travels from Web site to Web site. If the Web site owner cooperates — and many do — advertisers can collect name and address information entered into the Web site's forms and combine it with the information stored in the cookies.

Many people have come online only within the past few years, use the Internet without being entirely aware of how it works and are unaware of this practice. That does not exactly make cookies surreptitious: both Internet Explorer and Netscape can easily be set to tell a computer user when a cookie is being placed on his or her machine.[16] And cookies are a way the Internet can show people what they want to see, not intrusions intended to ferret out secrets. A good thing to remember when venturing onto the Internet is that it is like heading out into Disney World — whenever you go out to deal with other people on their turf, you can expect that they will be interested in learning about why you're there and how they can get you to come back.

Identity Theft and Other Security and Crime Problems. Real hazards await consumers on the Internet and in other venues. Identity theft and credit card fraud are reportedly growing. There is no evidence, however, that marketing data play a role in this. And there is no necessary link between technology and identity theft. Many cases of identity theft involve a criminal's dumpster-diving for financial records or bills carelessly thrown into the garbage or a vindictive cousin or schoolmate sneaking documents out of one's purse.

"Identity theft and credit card fraud are better seen as crime problems than as privacy problems."

Identity theft and credit card fraud are better seen as crime problems than as privacy problems. The problem is not that the companies have too much information about their customers. Rather, they often have too little information to be able to detect when another person is pretending to be you. The less information the companies have, the more likely they are to be bamboozled. If, for example, all a company knows is that your name is Betty Smith, it is relatively easy for someone else to call and pretend to be Betty Smith. If the company knows your name and Social Security number and mother's maiden name, it is a little harder — the fake Betty must obtain this extra information before proceeding with her fraud. If the company knows all that plus a PIN number or other password, or has a fingerprint or retinal scan,

it is that much harder for the fake Betty to proceed. In many ways, then, information is our most powerful weapon to detect and identify perpetrators of fraud. The need for security and the desire for privacy often cut in opposite directions.

In any case, the harms to consumers of fraud and identity theft are already illegal. Where consumers need more help is in the area of enforcement. The amounts of money stolen in fraud cases are often too small to interest police and prosecutors.[17] New and more effective enforcement institutions should be developed to address these harms without penalizing the economy.

Consumer Surveys about Privacy as a Basis for Public Policy

The policy debate about privacy as a consumer issue thus seems to be driven more by consumers' perceptions of danger than by actual danger. Nevertheless, these perceptions are powerful.

Survey Results on Consumer Privacy. Consumer surveys purport to show that Americans are very concerned about privacy.

- One commonly cited survey reported that 57 percent of Americans want the government to pass federal privacy laws for the Internet.[18]
- The Pew Internet & American Life Project recently found that 86 percent of those surveyed thought that Internet companies should ask permission before sharing personal information with third parties.
- 54 percent viewed cookies as an invasion of privacy; and only 27 percent agreed that tracking consumers online helps improve content and service.[19]

The question is, do these survey results reveal that the public's perceptions create a crisis of trust demanding new laws? This is doubtful.

Surveys Can Be Misleading. First, responses to consumer surveys about privacy are likely to be misleading. All surveys suffer from what one might call the "talk is cheap" problem. That is, the consumer thinks about a problem (loss of privacy) and a solution (a new law) without being given any accurate information about the costs of that solution.[20] If it were guaranteed free of all harmful consequences, who would oppose a new law addressing any issue? In addition to this, some privacy surveys have not distinguished between the use of information for marketing and its use by criminals — yet these are not the same issue at all. It is noteworthy that in the most accurate and least manipulative form of consumer survey, in which people are asked to list their top concerns without being prompted, privacy does not appear among top concerns.[21]

"The policy debate about privacy as a consumer issue seems to be driven more by consumers' perceptions of danger than by actual danger."

By comparison, actions are a better indicator of true preferences than words, because having to act makes the actor consider the cost of his preference as well as its theoretical benefit. Another colloquial saying, "Put your money where your mouth is," captures this well. Consumers say they are concerned about privacy. Yet their concern does not lead most of them to take action. Only a small percentage opt out of marketing lists, use encryption, regularly change their passwords or turn off cookies.[22] Yet most of those actions require little effort. Apparently, when consumers report a "concern" about privacy, the concern is superseded by a desire to pay bills, watch TV or keep the toddler out of the swimming pool.

Privacy advocates would counter that many people are unaware of things like cookies. This is confirmed by some surveys and contradicted by others,[23] but even among those who do know, the percentage that takes steps is low.[24] Furthermore, privacy advocates cannot have it both ways — the public cannot be simultaneously concerned about privacy and unaware that businesses are interested in learning about their behavior. Many realize that charitable donations are likely to be followed by packets of information from other charities and orders sent to gardening catalogs will bring a new array of gardening catalogs. People are certainly aware of the privacy issue at this general level — and those who really do care deeply about the issue are on notice to seek out more information for themselves. Ignorance is voluntary and is not, in any event, a useful basis for public policy-making.

"The fact that some people question the security of online commerce is not a reason to enact a new law on privacy."

The Future of Consumer Privacy

Despite the above caveats about surveys, however, let us assume that the surveys offer us at least some evidence of people's views on privacy. And at least one survey result purports to show that some have responded to perceived privacy problems online by refusing to engage in electronic commerce (though that survey seems to have counted both concerns about security problems like credit card theft and concerns about marketing information).[25] The possibility remains that a minority of the public questions the security of online commerce. The question may still be asked, is this the proper foundation for a new law on privacy? Surprisingly, the answer to that question is still "no."

Freedom Means Avoiding Unnecessary Legislation to Address Purely Speculative Harms. As a general rule, we will not preserve the freedom to build and plan a new business or any other venture in this country if legislators get into the habit of passing laws when there is only a perception of a problem but no real harm to consumers. The United States has remained one of the world's most innovative economies because legislators generally have acted against known or proven dangers, and only rarely interfered with invention, technical change and business method innovation. In the area of

privacy, however, where the product being produced by business is greater knowledge and understanding of human behavior, state and federal level proposals to regulate this product almost out of existence are increasing.

The real harm in consumer protection debate — a very real harm indeed — is credit card fraud. The perception of security problems, not concerns about marketing, represents consumers' greatest concern with online commerce; one recent survey showed that among online users who do not buy online, 43 percent are concerned about security issues such as entering a credit card number online.[26] (This topped all concerns; consumers were not prompted for their answers, and privacy or concern with marketing did not appear at all.) But credit card fraud is already illegal, and none of the privacy laws proposed by Congress would make enforcement of those laws more effective.

"Trust is largely a market phenomenon; legislation is not enough."

Building Trust as a Market Phenomenon. Broad new laws on the use of consumer information by marketers also would be unlikely to make a difference in the level of consumer trust. Trust is largely a market phenomenon. It comes from brand-building, good customer service and the positive experiences of friends and neighbors. No amount of legislation or legalese would substitute for the hard work of building trust in a new medium. And, slowly, American businesses are doing just that.

- In a study by the National Consumers League in August 2000, 91 percent of American respondents said they trust companies to follow posted privacy policies much of the time (up from 67 percent in 1998).[27]
- Internet users who think the Internet is secure enough for online financial transactions have risen from 34 percent to 45 percent since summer of 2000.[28]
- A recent study by Consumers International shows that U.S. companies are much more likely to reveal their privacy policies online than are European companies, although Europe is committed to broad privacy laws and the U.S. is not.[29]

Why Legislate to Suit the Most Technology-Resistant? The percentage of those refusing to use the Internet because of worries about online privacy no doubt includes a substantial proportion of the just plain technophobic. Research psychologists Larry Rosen and Michelle Weil estimate that about 30 to 40 percent of the population are "resistant" to technology.[30] Of the remainder, 10 to 15 percent are early adopters, while about 60 percent wait for the early adopters to work out any problems before they go online. The massive growth of the Internet shows that it continues to capture the largest group — those who are skeptical at first but not perpetually resistant — at a tremendous pace:

- As Figure II shows, 55 percent of Americans bought something online this holiday season, up from 20 percent in 1998. (Eighty-six percent reported an intention to buy online, but technical problems prevented many from completing their transactions.)
- Experts expect electronic commerce to continue growing at a rate well above 55 percent — some anticipate growth rates of 150 percent.

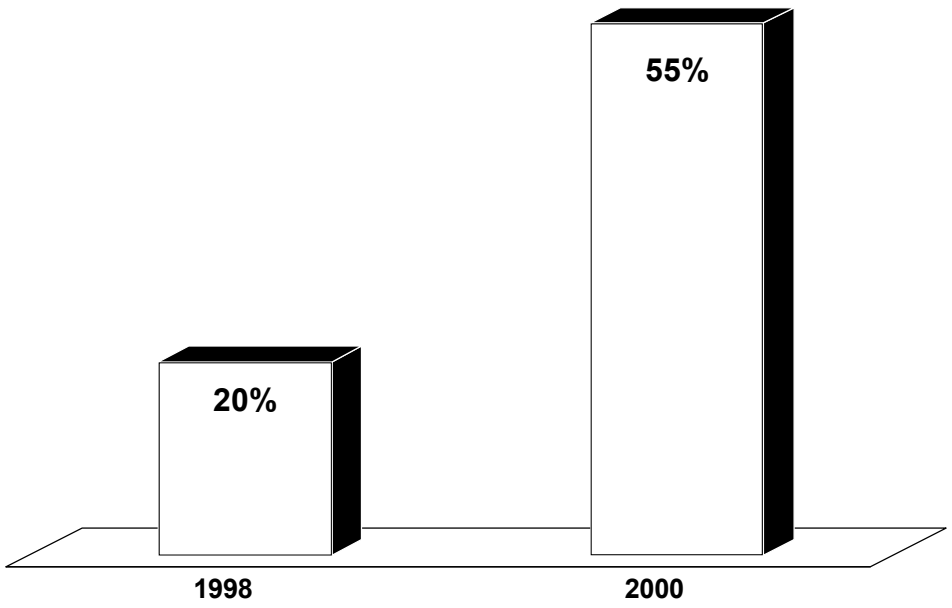
This suggests that the drive to regulate privacy policy is being formulated on the basis of the trepidations of a minority. For example, one survey by online research firm i-Novation found consumers divided into three camps: 37 percent seemed not to care about the issue of privacy; 28 percent liked the idea that businesses could use information about them to improve service or offer them new products they would be interested in if they asked first. On the other hand, 35 percent were "risk-averse" (fearful) when it came to information sharing.[31]

The most fearful among us would not necessarily be soothed by new federal or state privacy laws. Even among Europeans, one survey showed that fewer citizens believe new laws would improve Internet security (15 percent) than believe in technological solutions like passwords or encryption (27 percent).[32] In the U.S., in response to a Jupiter Consumer Survey, only 14

"55 percent of Americans bought something online during the holiday season."

FIGURE II

Percent of Americans Shopping Online during the Holiday Season



Source: Competitive Enterprise Institute.

percent of consumers reported that legislation would make them more likely to trust a Web site with information. Eighty-six percent said they would not trust Web sites even if regulated by the government. In other surveys, levels of support for government action have been very inconsistent.[33]

Several surveys have found (as one would expect) higher distrust of online commerce for security reasons among non-Internet users than among Internet users. Distrust levels are also generally lower among experienced than inexperienced users. It is unclear, however, what this means. It may mean that personal experience with the Internet results in a user more confident that, for example, Amazon.com is not in fact some sinister enterprise that tracks its customers in the hope of embarrassing or humiliating them, but rather is simply another bookseller. On the other hand, the levels of distrust may simply be more indicative of the users' attitudes to technology than any reality about the Internet; those most inclined to technophobia are naturally going to be the last adopters. In any case, this phenomenon decidedly does not prove, given that electronic commerce is still growing at an amazing pace, that the "distrusters" will just stay that way unless there is a new federal law.

Policy Should Do the Right Thing, Not Cater to Unfounded Fears. The idea that public policy should be shaped by the most fearful among us is a very bad one. The truth is that information-sharing among companies trying to learn about consumers' preferences has far more benefits than risks for consumers. In Jack Calfee's book *Fear of Persuasion,* research into marketing and advertising shows that consumers get enormous benefits in lower prices and higher quality when companies compete through advertising.[34] Before consumer reports existed, poor people or strangers in town found it almost impossible to obtain loans or buy on credit. Small and midsize businesses and ventures trying to compete in a market for the first time are more likely to fail or never exist without the ability to use targeted lists of potential customers. The current perception of a crisis in consumer privacy is largely unfounded. Electronic databases have made people uneasy, but they have little true grounds for concern.

"73 percent of employees think their employers have a right to monitor their e-mail."

Privacy and the Employment Agreement

Most people are pretty comfortable with the idea that their boss may check up on them from time to time; a recent study from the Angus Reid group found that 73 percent of workers thought their employers have the right to monitor e-mail and Internet access at the office.[35] We have all had experiences with fellow employees who do not do their fair share of the work, lie to avoid blame for mistakes, carry on disruptive personal affairs or vendettas in the workplace, steal, or use electronic resources inappropriately. Employers monitor and investigate their employees:

- To avoid liability for employees sending racist, sexist and sexually explicit e-mail,[36] for defamation or for violating intellectual property licenses and laws.
- To monitor productivity.
- To prevent losses from employee crimes such as embezzlement or theft from the employer or customers, estimated to cost over $400 billion annually.[37]
- To protect trade secrets and other confidential information.
- To avoid workplace violence, estimated to cost businesses $36 million each year.[38]

Even so, technological changes have raised new concerns about employer monitoring and workplace privacy among some advocates of privacy.

Electronic Monitoring at Work. The advent of computerization and other electronic devices has raised difficult issues in employer/employee privacy. Because e-mail and computer networks are relatively new and many do not understand how they work, some employees seem to expect that their e-mail or Internet access will be confidential. At the same time, e-mail and the Internet offer employees a new distraction during work hours and compel employers to keep an eye on workers' productivity. If a $30,000 employee spends an hour a day browsing online or answering personal e-mail, it costs the company $3,600 per year;[39] for a $50,000 worker this rises to $6,500.[40] One survey reports that half of all employees often surf the Net for personal reasons at work; one in eight men views sex sites at the office, and one-third often download unauthorized software.[41] As a result, one survey reports that large businesses are monitoring more and more of their workers' use of the Internet, up from 54 percent in 2000 to 61 percent in early 2001.[42] [See Figure III.]

"If a $30,000 employee spends an hour a day browsing online or answering personal e-mail, it costs the company $3,600 per year."

The use of video cameras and other electronic devices also is relatively new and still controversial. About two-thirds of employers use some kind of surveillance to monitor employees.[43] Such devices and techniques include:

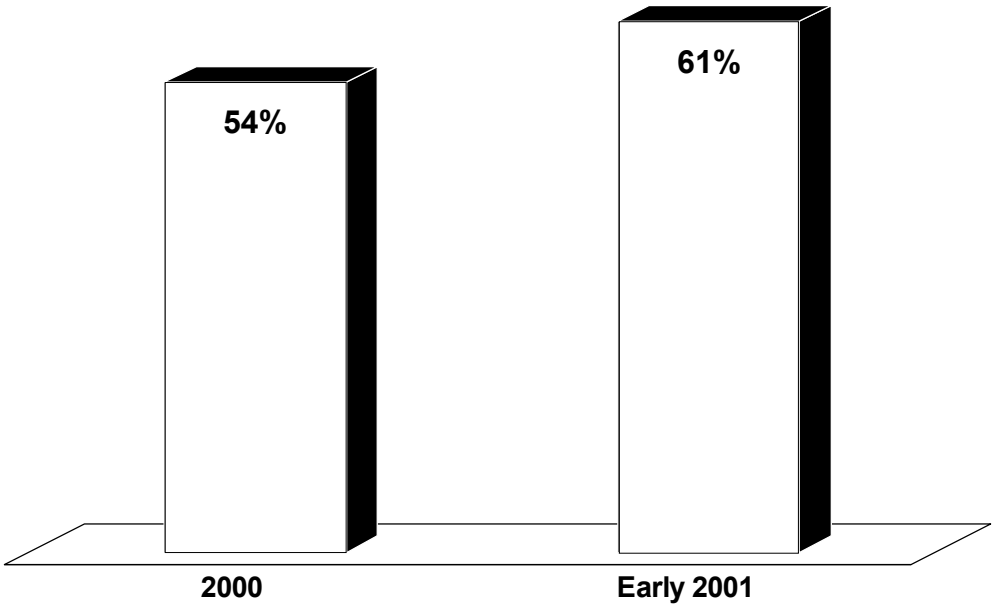
- Keystroke monitors that track the individual's productivity in typing.
- Video cameras monitoring the work area.
- Reading employee e-mail.
- Monitoring employee access to the Internet.
- Monitoring employee telephone conversations.
- Drug testing and other medical tests.

The use of such devices and techniques has arisen not only because it is possible but because over the past decades courts have been ever more willing

"Large businesses are monitoring more and more of their workers' use of the Internet."

FIGURE III

Percent of Large Businesses Monitoring Workers' Internet Use



Source: Kenneth Bredemeier, "Billing Arrangements Are Up to the Employer," *Washington Post*, February 2, 2001.

to hold employers responsible for their employees' behavior, illnesses, injuries, etc. Faced with this threat of expanded liability, employers seek to defend themselves.[44]

Using Medical Information. Another controversial practice is the use of medical information in making hiring and promotion decisions. Employers seek this information because:

- Health issues can affect an employee's ability to perform a job or pose a danger to other employees.[45]
- An employee at risk of developing certain illnesses might sue an employer for placing him or her in conditions that precipitate that illness.
- Because of U.S. tax law, employers often pay for employees' health insurance, and insurance prices go up when an employee uses a lot of expensive medical services.

One survey concluded that 35 percent of Fortune 500 companies use medical information in hiring or promotions.[46] This statistic, standing alone, is quite alarming. It naturally leads one to wonder, "Can my boss just look at my medical records any time he or she wants to?" But the answer is generally "no" unless your employer self-insures. Ordinarily one's employer simply

cannot access one's medical records at any stage of hiring or promotion, sometimes because of federal or state laws, but more commonly because medical care providers are not willing to share them, consistent with their understanding of the obligations of medical ethics. The survey of Fortune 500 companies is thus somewhat misleading. (Under new federal medical privacy rules, this practice among self-insurers is scheduled to become illegal.) Of course, all employers have access to information from any medical tests conducted on the job, such as a drug test. But it is a little hard to perform such tests without the knowledge of the employee.

Using Credit Information. A somewhat less controversial issue is the employer's use of credit information in hiring or promotion decisions. On the one hand, many employers have a justifiable interest in their employee's financial integrity and responsibility. An employee with large debts may have an incentive to steal, and one who does not pay bills may be unreliable in other ways. But credit reports are often perceived as inaccurate and thus their use may be perceived as unfair. However, the hard evidence suggests that, on the whole, rates of error in credit reports are low.[47] Two highly publicized but biased studies misleadingly reported high rates of error in credit reporting (from 30 to 50 percent). A 1991 study by Consumers Union relied on its employees and their acquaintances to review their own credit reports and report "inaccuracies." Consumers Union did not check whether those claims of inaccuracy were true or false, or try to identify the source of the errors.[48] Ralph Nader's Public Interest Research Group also failed to select a random sample, instead estimating an error rate from a sample of consumers who had paid to review their credit reports — people who probably had reason to suspect they would find errors.[49] A more rigorous study of 15,703 consumers, conducted by Arthur Andersen & Co., showed that the true error rate is probably as low as 1 to 3 percent.[50]

"Hard evidence suggests that rates of error in credit reports are as low as 1 to 3 percent."

The Current Law of Employee Privacy. Usually, when a private employer notifies an employee that surveillance is being or may be carried out, it is not particularly controversial as a matter of contract or tort law. A survey by the American Management Association reports that more than 80 percent of companies using electronic monitoring inform their employees of their policies.[51]

Employees are likely to find secret or unexpected surveillance more disturbing; it is in these cases that they are most likely to sue for invasion of privacy or wrongful discharge. But the courts generally hold that employees should be aware that their activities using the employer's property (telephones or computers) or in public places may be observed; the employee has no right to expect privacy under those circumstances. For example, in one case an employee had gotten into the habit of changing her clothes in her cubicle in a large office space after the other employees had gone home. She eventually discovered that there was a video camera monitoring the space and sued her

employer. The court held that because the space was essentially open to the public, she could not reasonably expect privacy there. A camera placed in a restroom or dressing room, would be another matter.[52]

It makes sense to use property rights as a boundary of privacy when the contract between a private employer and employee is silent on the matter of surveillance. It provides a clear, bright line for employers and employees alike. But what if the contract explicitly promises employees that e-mail will remain private? One court has said that the employer may read the e-mail anyway.[53] The result seems wrong and likely to be treated as such in future; the whole purpose of a contract is to rearrange the parties' normal rights and duties. The case would in effect make employees even more distrustful of employers by sending the message that employers' explicit assurances about privacy cannot be trusted.

In any case, it is unwise for businesses to spy on their workers, for when the surveillance inevitably is discovered the employees are likely to suffer a blow to morale even if they do not sue. However, the practice is not indefensible. In some cases, announcing surveillance allows employees bent on wrongdoing (such as embezzlement) to take further steps to evade detection; and employees who know they are under surveillance are likely to be more stressed and suffer physical ailments.[54]

"Limits on what sources employers may consult to learn about employees may have serious unintended consequences."

Several federal and state statutes may also affect privacy on the job. For example, Title III of the Federal Omnibus Crime Control and Safe Streets Act generally prohibits the interception of electronic communications by any device.[55] But the law allows employers to monitor employees in the ordinary course of the employer's business,[56] or with the employee's consent. State wiretap laws may also apply. As a general matter, of course, federal constitutional rights of privacy apply only to government employees.

The Future of Employee Privacy: The Gossip's Revenge. The current direction in legal discussions of state and federal privacy policy is to urge the enactment of more laws that protect workers' privacy. These proposals include enacting federal or state law to require employers to give notice of surveillance[57] (although employers seem to be moving in that direction in any event, as advised by countless attorneys writing on the subject) or supporting judicial activism to apply constitutional rights of privacy to the private sector or to expand privacy torts.[58]

Limits on what sources employers may consult to learn about their employees may have serious unintended consequences. As described above, there are common-sense reasons that employers want this information. Employers who are shut off by law from reading employee e-mail, credit reports or medical information will not stop wanting the information. They will instead step outside of accurate, professional sources like health records or consumer reports. What will the most likely alternative be?

The "Good Ol' Boys' Network." Employers for a long time hired people they or their friends and family knew. Strangers in town were out of luck. People outside the employer's social circle were out of luck. Often this meant women and minorities were out of luck. The irony of privacy laws that restrict the use of professionally developed and run databases is that those laws would backfire. Employers, shut off from legitimate sources, will go back to inaccurate and unfair gossip.

In view of this, it is probably wise to leave cases of privacy invasion on the job to the courts, which seem to be leaving employers the freedom to gather the information they need, while restraining the more untoward cases involving spying on restrooms.

Information Sharing and Health Care

Medical privacy is unlike consumer privacy or employer/employee privacy because of the special relationship between doctor and patient. It is not an arms-length contract, but more like a fiduciary relationship.[59] Medical ethics for centuries have respected patients' need for confidentiality.[60] During the 19th century, state statutes created a doctor/patient privilege requiring a patient's consent before the doctor could reveal medical information in a court of law.[61] Because of this history, patients have some reason to expect that what they tell their doctors will be kept confidential — the normal rule of freedom of information does not apply. On this basis, courts may find that the agreement between doctor and patient implicitly contains an obligation to keep information confidential even when the doctor has not expressly agreed to do so.[62]

"Medical ethics for centuries have respected patients' need for confidentiality."

However, since the Middle Ages authorities have sought the disclosure of certain contagious illnesses to preserve public health.[63] The tension between the public need to separate the sick from the well and private desire to avoid the stigma of illness is obvious.[64]

The Changing Business of Medicine

The last several decades have seen major changes in the practice of medicine. Customary concepts of confidentiality are under siege from several directions.

The Creation of a Federal National Medical Database. One natural and probably inevitable change has been computerization. Increasingly, medical records are stored electronically. This often means that people other than doctors and insurers can obtain access to records for purposes beyond treatment and payment.[65] Electronic databases and medical sites on the Internet raise new security issues, and the press has brought public attention to several leaks from government and private companies.[66] The latest major

development in this area was in 1996, when the Health Insurance Portability and Accountability Act of 1996 (HIPAA) called for the creation of a controversial national medical database, in which each patient would have a unique medical identifier like a Social Security number.[67] To ease concerns about security and privacy, the legislation stipulated that the Department of Health and Human Services protect this health information. Out of this change come the new HIPAA rules for medical privacy, discussed in detail below.

The Use of Health Information in Marketing. Another controversial practice is the use of health care information in marketing. In 1998, the *Washington Post* incorrectly reported that CVS and Giant Food had sold their drug customers' names to drug companies. The *Post* corrected the error the next day; but the public outcry caused CVS and Giant to drop out of the patient treatment compliance program in which they were participating.[68] In response, the National Association of Boards of Pharmacy put together "Guidelines for the Confidentiality of Patient Health Care Information as It Relates to Patient Compliance and Patient Intervention Programs."[69]

The Impact of Third-Party Payments on Confidentiality. Another factor has been the longer trend in America to a third-party-payer system of health care financing. Today, most patients obtain health care from a private insurance plan paid for by their employer, or from Medicare or Medicaid. Because someone else is paying, patients have little or no reason to monitor the costs of their treatments.[70] As a result, costs and fraud have risen drastically in the health care area. To protect themselves, third-party auditors seek access to medical records showing details of treatment and symptoms. And because third parties, not patients, are the source of doctors' incomes, health care institutions have become more attuned to the demands of the auditors than to the demands of patients for privacy. This change is inevitable without significant reforms to restore free markets to medicine.[71] Until then, auditors will delve deeper and deeper into medical records to cut costs and control fraud. The third-party-payer system has tended to erode the traditional promise of confidentiality between doctor and patient.

"The third-party-payer system has tended to erode the traditional promise of confidentiality between doctor and patient."

The Growing Use of Medical Information by Law Enforcement. As noted above, the tension between public health authorities and advocates for medical privacy is not new. What is new is the spread of mandatory reporting requirements to benefit law enforcement rather than public health. For years, hospitals and doctors have turned patient records over to the police virtually upon demand, having little legal right to object should they be served with a subpoena. The intrusion on privacy probably would not bother people if the police were hot on the trail of a serial killer wounded by a victim. But what about a recreational nonviolent drug user trying to kick the habit? The wider the police net, the more willing people will be to hide their condition rather than risk being turned in. This risk is not just theoretical. For example, under South Carolina's mandatory child abuse reporting law, a significant percent-

age of pregnant drug abusers stopped using in-state prenatal care and drug treatment programs for fear of being arrested for child abuse.[72] In areas with mandatory reporting for domestic violence, even seriously injured women have been known to go to battered women's shelters rather than to hospitals to evade reporting.[73] Medical associations resist this type of reporting, which creates an ethical dilemma for physicians and makes it difficult for them to gain patients' trust. Turning doctors into arms of law enforcement seems inappropriate and unnecessary.

Medical Privacy and the New HIPAA Rules. In response to these developments, medical privacy has become a key policy issue. In December 2000, the Department of Health and Human Services issued final privacy rules under HIPAA. These rules will be the first comprehensive federal law on medical privacy. The new rules are effective as of April 14, 2001, with health care providers expected to comply in February of 2003. The Bush administration ultimately decided to keep the rules largely intact despite the controversy, with the likelihood of some minor changes.[74]

"The new medical privacy rules are controversial."

The text of the HIPAA rules is 350 pages long; the rules and commentary together amount to 1,500 pages. In sum, the rules:

- Cover "protected health information" (PHI) in oral, written or electronic form.
- Protect health information that relates to a person's physical or mental health, treatment or payment.
- Require the patient's written consent for use of PHI for treatment, payment or health care operations (defined as activities directly related to treatment and payment, including credentialing, auditing, reinsurance, population studies, fundraising, medical training, quality assurance and peer review).
- Require the patient's explicit written consent for use of PHI for fundraising or other purposes other than treatment, payment or health care operations — that is, marketing.[75]
- Give the patient the right to ask for restrictions on the use of his PHI, to access PHI about himself, to ask for amendments to his PHI and to be notified how his PHI will be used.
- Allow public health officials, law enforcement, judicial and administrative authorities and emergency services to access PHI without consent. Medical researchers may also access information without consent, with the permission of a review board. In this respect, HIPAA will simply formalize what many institutions did before HIPAA.

The new HIPAA rules are controversial. Representatives of the health care industry believe that the government has seriously underestimated the cost

of the new rules.[76] The government's estimate of the cost was $18 billion, with $30 billion in savings expected from standardization. The industry's estimate of the cost is over $40 billion.[77] Advocates for more privacy continue to push for stricter rules, opposing the rules' toleration of the use of medical information in marketing.[78] Privacy advocates are also alarmed at the ease with which law enforcement may access medical records, although the rules do not give the police easier access to data than federal agencies already had.[79]

Even with the new rules, HIPAA gives the government more access to and control of medical information because it creates a centralized health information network and a system of national codes to ease intranetwork communication. It also assigns patients, health plans, employers and health care providers unique identifiers — national IDs for the health care system.[80]

"Under the new rules, every patient will have a national ID."

The Future of Medical Privacy: Will More Openness Bring Health Benefits to Patients? Two key conclusions follow from the analysis above. First, the forces of change are impelling us further from the understanding of doctor/patient communications as inviolable, an understanding which seems to be widespread among the public and which can be partly justified given the history of medicine. Second, the new HIPAA regulations confirm the trend toward more sharing of medical information throughout the medical industry. Issues of medical privacy become particularly complex because the government is involved in some intrusions — bringing in a constitutional element — but not in others.

All of these changes come as something like a glass of cold water in the face — one initially recoils from them. And medicine faces the same problem that it always has; that is, that patients may keep their health problems to themselves if they cannot trust their doctors to keep private communications private.[81] On the basis of this concern alone, there are grounds for sticking to a traditional view of medical privacy. Yet there is a strong counterargument that the medical industry should not be constrained by that tradition.

As Medical Advances Bring New Cures, Some Sensitivity about Medical Information Will Be Reduced. Privacy in medicine has been valued in part because a stigma has been attached to so many illnesses. Most people do not mind others knowing about their arthritis or common cold. And modern medicine has eliminated the stigma attached to other ailments and reduced the shame attached to being ill. For example, when depression and bipolar disorder were virtually untreatable, few wanted to be publicly identified as depressed. If one's mind had been identified as not functioning properly, it would be harder to find friends, potential mates and good jobs. But as more and more illnesses are conquered, hiding vulnerabilities and suffering plays a lesser role in medical policy, although it is unlikely to disappear entirely.

This observation holds even for the highly controversial issue of genetic privacy. In recent years, the privacy of one's genetic information has been a key topic, driving states to adopt legislation regulating the use of such information and prohibiting its use in certain insurance and employment decisions that are deemed "discriminatory." But in another 20 years, the issue of genetic discrimination may become a non-issue. The reason: genetic knowledge will potentially not just identify a risk of illness, but also create new cures and usher in a new age of powerful preventive medicine. In the meantime, the main danger is that the information that researchers will need to develop these cures will be closed off because of well-meaning legislation that sticks to a rigid model of privacy.

"Marketing can help patients compare the virtues of competing medical products."

In this changing world, the medical profession should remain unencumbered by legislation that forces it either to share information (for those areas where continued privacy turns out to be critical) or to keep it private (for those areas where tremendous health benefits could be realized from sharing). Some patient groups will be able to adapt more quickly than others to information sharing that brings wider medical benefits.

The Surprising Benefits of Marketing and Medicine. One of the most potentially beneficial aspects of information will turn up where we least expect it — in marketing. For a long time, we lived in a world of patent medicines, where advertising was the realm of quacks and con artists. But in today's world not only are there effective treatments, but these treatments compete with each other. One medication might relieve all symptoms but have difficult side effects. Another might relieve only some symptoms but have few side effects. In a competitive world, advertising and targeted marketing are enormously valuable to consumers. Consumers are the audience to the ongoing debate about the virtues of comparable products. Stopping the information flow between drug companies and patients means impeding competition among pharmaceuticals. Without marketing, patients have only doctors as information sources, while doctors are pressured to spend less and less time getting to know their patients or may have some non-medical reason for favoring one treatment over another. Finally, there is little danger to patients from the use of medical information in marketing. The most threatening thing likely to happen is that they would be sent coupons or some other unsolicited offer in the mail.

Medicine and Government. This is not to say that all information-sharing should be welcomed with open arms. Both the American constitutional tradition and the lessons of history suggest that privacy is one part of a sensible long-term strategy to control the risks associated with the unique powers of government. Growing government access to medical information remains a valid concern. Practices such as massive scrutiny of medical records by law enforcement are unrelated to medical benefits and may indeed be medically harmful.

So long as the federal government is entangled in our health care system, it is hard to argue against some federal actions on privacy. But they need not push health costs higher or restrict competition. It may simply be time to explore new private-sector uses of medical information. Our health care system desperately needs some informed decisions.

Comparison and Analysis

This section draws on the previous sections to determine what the different aspects of the privacy problem have in common and what they do not. All of the concerns raised above can be fitted in one or more of the several vague definitions of "privacy." These include Justice Brandeis's famous "right to be left alone," as well as the claim that people have a right to control information about themselves. Nevertheless, privacy policies cannot be based on the assumption that all of these areas are alike.

The Role of Computerization. In each of the above areas, computerization has upset understandings of what is private and what is not. Records stored on a computer are considered more dangerous than records stored on paper. They are easier to copy and to send anywhere in the world. Some people make the leap from knowing that a database is electronic to thinking that the data is on the Internet, which isn't so.

"Computerization has upset understandings of what is private and what is not."

In reality, however, electronic databases are not a fundamentally more threatening phenomenon that ordinary gossip and conversation. At least in the private sector, the new world of electronic information is less threatening. Unlike gossip, the companies that compile electronic records have a business incentive to get the records right, and electronic databases are impersonal. Your name and address are not sold as an individual's name and address — rather, you are one of a thousand on a list of "people who own single family homes" or "people who bought lawn mowers." Usually, the companies that compile the databases view them as valuable property and work hard to keep them secure.

Historically, the electronic database represents the fact that information users in government and in the private sector will finally be able to keep up with the vast numbers of people moving throughout a vast country. We can move to a world where information flows where it is most needed without geographical limits. The information movement can finally be as sophisticated as the movement of people.

Comparing Harms and Solutions. Where the privacy problems that we have considered are fundamentally unalike is in the degree to which they threaten individuals as consumers or citizens. Some might call for constitutional or targeted legislative remedies. Many others warrant no action at all. But consider the following list of issues that might arise under each category.

All are privacy problems in some sense. Yet a quite different level of concern is appropriate to each problem. And no single, broad legislative solution could effectively address all of the problems without also hindering legitimate and harmless information exchanges:

- A brutal search is conducted without a proper warrant.
- Information collected by the Census Bureau is used by local authorities to evict a group of immigrants from a home on grounds of housing density restrictions.
- Someone is annoyed at being sent an advertisement in the mail from a new company.
- A person is the victim of credit card fraud.
- A clerk is disciplined for visiting sexually explicit Web sites on company time.
- A patient is disturbed to discover that her treatment notes are being reviewed by a team of federal auditors looking for Medicare fraud at the clinic she goes to.

What is the level of harm experienced by these different privacy "victims?" The subjects of the warrantless search and the credit card fraud have suffered harm in the sense of an injury to property that can legally be measured and addressed by the judicial system. The former endured a search by big scary men with guns without accountability to anyone, even a judge; the other was a victim of fraud. Here, the power to collect information or the information itself was used to do evil.

At the other extreme is someone annoyed at being sent an advertisement in the mail. The suggestion is that the information itself was an evil. Yet it was merely a communication. The interest was not evil, nor is the effect long-lasting.

Just as harms to privacy are very different, solutions to privacy problems are very different. Because governments are good at passing statutes exempting themselves from restriction on their own authority, the Constitution is probably the best place for restrictions on government information-gathering. Also, the risk of harm to be prevented is very broad — the risk that government power to collect information could help carry out broad human rights violations. In this sense, general, sweeping legal principles akin to the Fourth Amendment are appropriate. Legal rules already target such criminal behavior as identity theft and are also appropriate. Broad, sweeping rules aimed at the private sector will impose unjustifiable costs on many legitimate businesses and activities. The criminal, not everyone else, should bear the penalty for committing a crime.

"Just as harms to privacy are very different, solutions to privacy problems are very different."

Where no measurable harm is involved, legal measures are not an appropriate response. The harm is very slight and easily controlled simply by

the individual who got the ad's taking a deep breath to calm down. Each individual's response is likely to be different. And the circumstances under which ads will be welcome and under which they will be annoying are bafflingly complex. Businesses do not want to send annoying ads; they want to send welcome information. They have a good incentive to fix the problem on their own.

Conclusion

Cultural, legal and technological changes have created the perception of a privacy crisis. This is because people are sometimes puzzled about how the old rule favoring the free flow of information in the private sector (with privacy being the exception) will apply to new cases. It does not follow, however, that a real and dangerous privacy crisis exists. Most alleged harms are either speculative or vague. As a general rule, there is not, and never has been, any real problem with continuing to embrace people's ability to learn about other people.

When it comes to privacy from government intrusion, new legal rules — unless adopted at the constitutional level — are in effect Band-Aids on a bleeding wound. It is simply too easy for government to exempt itself from restrictions on its information-gathering powers whenever those restrictions become inconvenient. Still, government is the one entity that wields enough unchecked power for us to be concerned about its access to information. And such concern is consistent with the U.S. Constitution's tradition of limited government.

"It is too easy for government to exempt itself from restrictions on its information-gathering."

In the area of privacy and consumer protection, the biggest challenge is to sort out technophobia from real harms like identity theft. Consumers do not need to be protected from coupons. They do need enforcement institutions that will recognize the harm of identity theft and facilitate real solutions for victims of fraud.

In the area of employment privacy, common sense should stem the tide to shut employers off from information they need to control costs and employee behavior. Wise employers will generally inform their employees about monitoring practices. But sometimes a secret monitoring system will be necessary so that employees bent on misconduct will not set out to deliberately defeat it. Too many restrictions on employers' access to information, and we'll be back in the era of the Good Ol' Boys.

Medical privacy is perhaps the most complicated area. Medicine is no longer a purely private-sector activity. Sometimes, familiar constitutional principles are relevant to analyzing medical privacy problems such as police access to medical records. For practices like marketing, it may be necessary for companies to take special measures to reassure the public that these uses

will not harm them. But private-sector uses of data in medicine have potential public benefits, and medicine should not be constrained by a rigid model of privacy.

Despite the perception of a privacy crisis, there is excitement in the air about the potential for enormous gains in business and government administration and in consumer welfare and service from new uses of information. The changes wrought by information access and electronic databases are just beginning. After all, every single human action — the decisions to buy or not to buy, whose Web sites we visit, how much we spend, at what time of day — is something someone somewhere might learn something from. If more information on human behavior could be saved, business could grow faster; consumers could enjoy cheaper goods and services with less hassle; wrongdoers could be captured more quickly; and the vast economic losses that result from fraud, misunderstanding, confusion and poor planning could be slashed.

"Despite the perception of a privacy crisis, there is excitement in the air about the potential for enormous gains from new uses of information."

The good news about new information technology is that it is not the boogeyman. Human beings rarely make better decisions by having less information about themselves and their fellow human beings. The principle that freedom of information should only rarely give way to privacy concerns is as reliable today as it was formerly.

NOTE: Nothing written here should be construed as necessarily reflecting the views of the National Center for Policy Analysis or as an attempt to aid or hinder the passage of any bill before Congress.

Notes

[1] See generally Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999).

[2] *U.S. v. Toscanino*, 500 F.2d 267 (2nd Cir. 1974) holding that district court must consider the question of whether its jurisdiction was illegally obtained by kidnapping.

[3] The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. U.S. CONST. amend. IV.

[4] See, e.g., *Washington v. Nordskog*, 76 Wash. 472, 136 P. 694 (Wash. 1913), wiretapping by the *Seattle Times* of a detective agency did not violate the law for malicious injury to property because wiretapping does not injure property.

[5] *Olmstead v. United States*, 277 U.S. 438 (1928).

[6] *Olmstead* was controversial in its day, as well. See generally Robert M. Pitler, "Independent State Search and Seizure Constitutionalism: The New York State Court of Appeals Quest for Principled Decisionmaking," 62 *Brooklyn Law Review*, 1, 45-47 (1996), describing response of state governments to *Olmstead*.

[7] 387 U.S. 294 (1967).

[8] *California v. Greenwood*, 486 U.S. 35, 39 (1988); *California v. Ciraolo*, 476 U.S. 207, 211 (1986); *Oliver v. United States*, 466 U.S. 170, 177 (1984).

[9] See, e.g., Anthony G. Amsterdam, "Perspectives on the Fourth Amendment," 58 *Minnesota Law Review*, 349, 384-85 (1974) stating that the expectation-of-privacy theory is so circular that it "obviously [can have] no place in... a theory of what the Fourth Amendment protects;" see also *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting), "The [Fourth Amendment] analysis must ... transcend the search for subjective expectations ....".

[10] Jay Bookman, "In Your Face: The Ways Surveillance Equipment Can Scan, Tape, Track and Profile You," *Atlanta Journal and Constitution*, March 25, 2001, p. D1. A house with unusually intense warm spots in the attic or basement may be suspected of harboring an array of special lamps and marijuana plants. A similar heat signature might be given off by tropical fish tanks or equipment for growing legal plants.

[11] Berni Dwan, "Prepare for Screen Warfare," *Irish Times*, October 9, 2000, p. 8. All computer screens give off radio-frequency waves that can be captured by an antenna directed towards a particular monitor or room. The signals can be captured from another office in the same building or from a building across the street.

[12] Lawrence Lindsey, "The Money-Laundering Conundrum: Mugging Privacy in the Assault on Crime?" in *The Future of Financial Privacy: Private Choices versus Political Rules* (Washington, D.C: Competitive Enterprise Institute, 2000), p. 166.

[13] The Office of Management and Budget has passed guidelines on federal information-gathering. The eerie-sounding rule stipulates that "the racial and ethnic categories should be comprehensive in coverage and produce compatible, nonduplicative, exchangeable data across Federal agencies." See http://www.whitehouse.gov/omb/fedreg/ombdir15.html.

[14] David Beers, "Protecting Privacy by Cutting Back Census Operations," November 2000, available at http://www.freespeaker.org/policydebate/privacy/census.html.

[15] Jennifer Goldblatt, "Freeport, Maine-Based L.L. Bean among Catalog Merchants Extending Reach," *Virginian-Pilot*, August 5, 2000.

[16] It is easy enough to disable cookies or be warned when one is about to be placed. If you are using Netscape Navigator, go to the taskbar and click on "Edit." Select "Preferences," go to "Advanced." Next click on "Cookies" and select "Disabled," or ask to be warned before your browser accepts a cookie. If you are using Internet Explorer, go to "Internet Options" and select "Security." Go to "Custom" and scroll down to "Cookies," again, select "Disabled" or ask for a warning.

[17] See Rep. James Leach, "Identity Theft Vexes Lenders, Consumers," *Mortgage Servicing News*, November 2000, p. 4, "Despite [the] profusion of Federal and State statutory authority . . . there is little evidence that law enforcement agencies have

made combating this crime a priority. A recurring theme at last week's hearing was the difficulties encountered by victims of identity theft and the financial institutions that bear the losses in obtaining redress, either because financial thresholds established by prosecutors' offices have not been met or because resources are simply being directed elsewhere." See also Jackie Hallifax, "Task Force Grapples with Privacy Issues in Technology Age," *Associated Press State and Local Wire*, December 15, 2000, which outlines better enforcement methods for identity theft.

[18] Stephen E. Arnold, "Internet Users at Risk: The Identity/Privacy Target Zone." *ASAP*, January 1, 2001, p. 24.

[19] Brian Krebs, "People Want More Control Over Personal Info Online," *Newsbytes*, August 21, 2000.

[20] Paul Rubin and Tom Lenard, *Privacy and the Commercial Uses of Information* (Washington, D.C.: Progress and Freedom Foundation, forthcoming in 2001).

[21] See, e.g., Peter Raducha, "Preliminary Results of a Nationwide Survey of Youth," Global Youth Action Network, July 2000; and Frank Newport, "Economy, Education, Health, Crime and Morality Most on Americans' Minds This Election Year," Gallup News Service, June 22, 2000.

[22] See, e.g., "Caught with the Cookie Jar," *National Journal's Technology Daily AM Edition*, April 4, 2001, p. 4, "Web analysis service Web Side Story found that in over 1 billion page views cookies were disabled just .68 percent of the time"; "Mining for Privacy Gold," *San Francisco Business Times*, March 9, 2001, p. 21, noting that 3 percent of Americans opt out of marketing mailings; Carey Adams, "The Internet and Security," *Access Control & Security Systems Integration*, November 2000, stating that 18 percent never change their passwords, 33 percent only when forced to do so, and 17 percent only once per year, while 22 percent have passwords that can be cracked in seven minutes or less; and Krebs, "The Future of Consumer Privacy," reporting that 9 percent use encryption, 5 percent use software that hides their identity.

[23] Rubin and Lenard, *Privacy and the Commercial Uses of Information*.

[24] Krebs, "The Future of Consumer Privacy," reporting that 10 percent of those who know about cookies take steps to block them.

[25] Ryan James, "Safety on the Net," *Toronto Sun*, June 8, 2000, p. 66, describing Privada survey reporting that "27 million adults gave up using the Internet for lack of privacy last year, and that over half of all Net users gave up an online transaction because they were asked for information they didn't feel comfortable giving out."

[26] Harris Interactive, Inc./Privacy Leadership Council Poll, December 20, 2000, p. 6 (on file with the author).

[27] "Commissioned Research Confirms Privacy Is a Key Issue Influencing Consumer Influence of Internet Billing," *Canada Newswire*, January 16, 2001.

[28] "Motor Insurance Gets into Fast Lane," *Marketing Week*, March 29, 2001, p. 59.

[29] Joris Evers, "U.S. Beats Europe in Online Privacy Protection," *InfoWorld.com*, January 24, 2000.

[30] Larry D. Rosen & Michelle M. Weil, "Public Interest in the Information Superhighway," (1995), at http://www.csudh.edu/psych/study3.html.

[31] Kate Fitzgerald, "Poll: Consumers Sharply Divided on Privacy Issue," *Advertising Age*, November 13, 2000, pp. 80, 88.

[32] "EU Preparing Plans for Battling Cybercrime," *Deseret News*, December 13, 2000, p. A13, also noting that 3 percent of Europeans believe the Internet is secure.

[33] Rubin and Lenard, *Privacy and the Commercial Uses of Information*.

[34] See also "Customer Benefits from Current Information Sharing by Financial Services Companies," December 2000 (Conducted for the Financial Services Roundtable).

[35] Sherman Fridman, "Most Workers Don't Mind Workplace Online Monitoring," *BizReport*, May 8, 2000, at http://www.bizreport.com/career/2000/05/20000508-2html.

[36] See Curtis Cotton, "Electronic Mail in the Workplace: Employer Monitoring vs. Employee Privacy," p. 1, at http://www.gcwf.com/articles/interest/interest_40.html.

[37] Association of Certified Fraud Examiners, *Report to the Nation: Occupational Fraud and Abuse* (1997), p. 5; see also Steve

Myers, "Workers Blamed in Store Thefts," *News and Observer*, Raleigh, N.C., December 22, 2000, p. B1, citing study showing $11 billion nationwide in losses due to employee theft from retailers alone in 1999.

[38] Joseph G. Schmitt, "Escaping the Privacy Bind: An Outline for Employers," *Corporate Risk Spectrum*, December 2000, p. 18.

[39] Patricia Monaghan, "Big Brother Is Reading Your E-mails," *Irish Times*, September 7, 2000, p. 13, quoting Simon Stuart of Softech Telecom.

[40] Al Berg, "Pulling the Plug on Surfing and Spam," *Information Security*, April 2000, p. 57.

[41] Ibid.

[42] Kenneth Bredemeier, "Billing Arrangements Are Up to the Employer," *Washington Post*, February 2, 2001, p. E3; see also Berg, "Pulling the Plug on Surfing and Spam," citing another study showing increase in monitoring among 200 businesses surveyed.

[43] Allison R. Michael and Scott M. Lidman, "Monitoring of Employees Still Growing," *National Law Journal*, January 29, 2001, p. B9, citing American Management Association survey from April 2000.

[44] Ibid.

[45] Because of the Americans with Disabilities Act, it is not legal to fail to promote or hire someone because of a disability that does not affect his or her ability to perform a job.

[46] See, e.g., Paul Starr, "Health and the Right to Privacy," 25 *American Journal of Law and Medicine*, 193, 198 (1999).

[47] Daniel B. Klein and Jason Richner, "In Defense of the Credit Bureau," *Cato Journal,* 12 (1992), pp. 402-7, discussing Consumers Union study "What Are They Saying about Me," April 29, 1991.

[48] Ibid., pp. 403-04.

[49] Ibid., pp. 405-07. The PIRG study also failed to identify the source of the errors and reported anecdotes featuring consumers' unconfirmed assertions that their reports contained errors.

[50] Ibid., pp. 407-08.

[51] T. Shawn Taylor, "E-Lessons: Love Notes and Other Internet Faux Pas Could Lead to Embarrassment or Worse — You Could Get Fired," *Chicago Tribune*, February 14, 2001, p. C1.

[52] See *Doe by Doe v. B.P.S. Guard Services*, 945 F.2d 1422, 1427 (8th. Cir. 1991), secret camera in models' private dressing room is invasion of privacy; *Harkey v. Abate*, 346 N.W.2d 74, 76 (Mich. Ct. App. 1983), hidden surveillance device in dressing room is highly offensive interference with privacy; and *Speer v. Department of Rehabilitation & Correction*, 646 N.E. 2d 273, 274 (Ohio Ct. Cl. 1994), monitoring in areas such as restrooms states a valid claim for invasion of privacy.

[53] See *Smyth v. The Pillsbury Co*, 914 F. Supp 97 (E.D. Pa. 1996), dismissing wrongful discharge claim.

[54] See e.g. Michael J. Smith et al., University of Wisconsin & Madison Department of Industrial Engineering, "Electronic Performance Monitoring and Job Stress in Telecommunications Jobs, 1, 5, 20 (1990), stating that monitored workers reported more wrist, neck and back problems and had higher incidence of stress-related mental conditions; see also Melanie Payne, "New View of Surveillance," *Sacramento Bee*, January 22, 2001, p. 1, reporting statement of researcher Carl Botan of Purdue's Center for Education and Research in Information Assurance and Security that employees who know of monitoring tend to think the employer is more interested in quantity of work than quality.

[55] 18 U.S.C. section 2511(1)(a)-(d); see also *Pascale v. Carolina Freight Carriers Corp*., 898 F. Supp. 276 (D.C. N.J. 1995).

[56] *Arias v. Mutual Central Alarm Svcs, Inc.*, 1998 U.S. Dist. LEXIS 14414 (1998), aff'd 202 F. 3d 553 (2d. Cir. 2000).

[57] Michael and Lidman, "Monitoring of Employees Still Growing," describing statutes proposed in California and passed in Connecticut, as well as the "Notice of Electronic Monitoring Act" proposed in the Senate and in Congress.

[58] See a survey of such proposals in S. Elizabeth Wilborn, "Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace," 32 *Georgia Law Review*. 825, 849-864 (1998).

[59] Two cases consistent with this theory include *Ritter v. Rush-Presbyterian-St. Luke's Med. Ctr.*, 532 N.E.2d 327, 331 (Ill. App. Ct. 1988), holding that the doctor-patient privilege disallows communications out of court between a doctor and his patient's legal opponent; and *Alexander v. Knight*, 177 A.2d 142, 146 (Pa. Super. Ct. 1962) (same).

[60] "Rights to privacy are valid claims against unauthorized access that have their basis in the right to authorize or decline access. These rights are justified by rights of autonomous choice . . . expressed in the principle of respect for autonomy. In this respect, the justification of the right to privacy is parallel to the justification of the right to give an informed consent." Tom Beauchamp and James Childress, *Principles of Biomedical Ethics*, 4th ed. (New York: Oxford University Press, 1994), p. 410; see also p. 406 (defining privacy as "a state or condition of physical or informational inaccessibility").

[61] See, e.g., *Territory v. Corbett*, 3 Mont. 50 (Mont. 1877), wherein doctor/patient privilege was not recognized at common law.

[62] *Hammonds v. Aetna Cas. & Sur. Co.*, 243 F. Supp. 793, 801 (N.D. Ohio 1965), finding implicit contractual obligation that "any confidential information gained through the relationship will not be released without the patient's permission"; and *Doe v. Roe*, 400 N.Y.S.2d 668, 674 (Sup. Ct. 1977), finding that the doctor's duty to keep patient's information confidential was violated when doctor reported patient's thoughts and feelings.

[63] Lawrence Gostin & James Hodge, "The 'Names' Debate: The Case for National HIV Reporting In the United States," 61 *Albany Law Review* 679, 687 (1998).

[64] See, e.g., *Simonsen v. Swenson*, 177 N.W. 831 (Neb. 1920), finding that doctor does not breach duty of confidentiality by reporting contagious diseases.

[65] U.S. General Accounting Office, "Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Is Limited," *Report to Congress*, February 1999, p. 1.

[66] See Benjamin Banahan and Suzy Buckovich, "Patient Privacy, Confidentiality and Security," *Drug Topic*s, February 21, 2001, p. 77.

[67] See Sue Blevins and Robin Kaigh, "The Final Federal Medical Privacy Rules: Myths and Facts," Institute for Health Freedom, February 2001, p. 3.

[68] Banahan and Buckovich, "Patient Privacy, Confidentiality and Security," p. 77.

[69] Ibid.

[70] See generally, John C. Goodman and Gerald L. Musgrave, *Patient Power* (Washington, D.C.: Cato Institute, 1992).

[71] Market-based reforms would include reducing the role of government subsidies, encouraging individuals to shop for policies on their own rather than through their employers, and medical savings accounts.

[72] Lynn M. Paltrow, "Pregnant Drug Users, Fetal Persons and the Threat to Roe v. Wade," 62 *Albany Law Review* 999, 1055 (1999); see also "Report of American Medical Association Board of Trustees, Legal Interventions During Pregnancy," 264 *Journal of the American Medical Association* 2663, 2667 (1990).

[73] Mia M. McFarlane, "Mandatory Reporting of Domestic Violence: An Inappropriate Response for New York Health Care Professionals," 17 *Buffalo Public Interest Law Journal,* 1, 24 (1998/1999).

[74] Drew Clark, "HHS Will Accept Comments on Medical Privacy," *National Journal's Technology Daily P.M. Edition*, February 26, 2001, p. 5.

[75] Hogan & Hartson L.L.P., "Hogan & Hartson Health Law Advisory," December 22, 2000, p. 4, describing need for authorization, and noting "Authorization is not required when communication to an individual occurs face-to-face with an individual, concerns products or services of a nominal value, or concerns health-related products and services of the covered entity or a third party," so long as certain disclosure requirements are met.

[76] Robert Pear, "Medical Industry Lobbies to Rein in New Privacy Rules," *New York Times*, February 12, 2001, pp. A1, A19.

[77] Peter Schnitzler, "Insurers, Others Brace for Privacy Standards: HIPAA Compliance Could Be Complicated," *Indianapolis Business Journal*, January 8, 2001, p. 19A, quoting Wes Rishel of the Gartner Group putting costs at $43 billion.

[78] See, e.g., Phyllis Schlafly, "At Stake in New HHS Privacy Regulations," *Washington Times*, February 24, 2001, p. A13.

[79] Before HIPAA, for example, Medicare would release records to state or federal agencies or law enforcement upon receipt of documentation of the agency's intent to comply with the Privacy Act of 1974. Testimony of Aronovitz at 5.

[80] Blevins and Kaigh, "The Final Federal Medical Privacy Rules: Myths and Facts."

[81] See Mark A. Hall, "Should the Law Restrict Insurers' Use of Genetic Information? A Guide to Public Policy," draft paper on file with author, p. 15: "The law protects as confidential the communications between patients and doctors, but does not protect the privacy of medical information per se. The reason is that, although medical information in the abstract is private and important, the greatest social harm is chilling patients' willingness to consult a doctor." See also "What Washington Has in Store for Benefits Managers in 2001," *Managing Benefits Plans*, February, 2000, p. 2: "Research by several health care privacy advocates says 17 percent of consumers pay for care that would otherwise be covered by their insurance, or choose not to seek care, because they fear their condition or treatment will be improperly disclosed."

About the Author

Solveig Singleton is a Senior Policy Analyst with the Competitive Enterprise Institute's Project on Technology and Innovation. She is a popular and sometimes controversial speaker at many industry and academic events. Ms. Singleton is the former director of information studies for the Cato Institute. She also served as vice chair of publications for the Telecommunications and Electronic Media Practice Group of the Federalist Society for Law & Public Policy Studies from 1996 to 1999. Her articles have appeared in the *Journal of Commerce, Washington Times, Philadelphia Inquirer, Wall Street Journal, Internet Undergound* and *Hotwired*. She is the co-editor of two books, *Regulators' Revenge (1998) and Economic Casualties (1999).* Her undergraduate degree is from Reed College, where she majored in philosophy. She graduated cum laude from Cornell Law School and worked for two years at a telecommunications law firm.

About the NCPA

The National Center for Policy Analysis is a nonprofit, nonpartisan research institute founded in 1983 and funded exclusively by private contributions. The mission of the NCPA is to seek innovative private-sector solutions to public policy problems.

The center is probably best known for developing the concept of Medical Savings Accounts (MSAs). The *Wall Street Journal* called NCPA President John C. Goodman "the father of Medical Savings Accounts." Sen. Phil Gramm said MSAs are "the only original idea in health policy in more than a decade." Congress approved a pilot MSA program for small businesses and the self-employed in 1996 and voted in 1997 to allow Medicare beneficiaries to have MSAs.

Congress also relied on input from the NCPA in cutting the capital gains tax rate, in creating the Roth IRA and eliminating the Social Security earnings penalty. These proposals were part of the pro-growth tax cuts agenda contained in the Contract with America and first proposed by the NCPA and the U.S. Chamber of Commerce in 1991. Two other tax changes — an increase in the estate tax exemption and abolition of the 15 percent tax penalty on excess withdrawals from pension accounts — also reflect NCPA proposals.

Another NCPA innovation is the concept of taxpayer choice — letting taxpayers rather than government decide where their welfare dollars go. Legislation to create taxpayer choice at the state level was sponsored last year by Reps. John Kasich, J.C. Watts and others. The idea is also a priority of President Bush.

Entitlement reform is another important area. With the grant from the NCPA, economists at Texas A&M University have developed a model to analyze Social Security and Medicare, and is publishing a series of studies on the future of the two entitlement programs. This work is directed by Texas A&M Professor Tom Saving, who has been appointed a Social Security and Medicare trustee. The NCPA has also established an interactive online Social Security calculator (www.mysocialsecurity.org), that allows visitors to compare their Social Security benefits with returns if they payroll taxes had instead been invested privately.

In the 1980s, the NCPA was the first public policy institute to publish a report card on public schools based on results of student achievement exams, and an NCPA task force made the case for school choice. Subsequently, the NCPA pioneered the concept of education tax credits as one route to school choice. The NCPA and Children First America have published an Education Agenda for the new administration, a book whose contributors include Nobel laureate Milton Friedman, Sen. Jon Kyl and other school choice experts.

The NCPA's Environmental Center works closely with other think tanks to provide common sense alternatives to extreme positions that frequently dominate environmental policy debates. In 1991 the NCPA organized a 76-member task force, representing 64 think tanks and research institutes, to produce *Progressive Environmentalism*, a pro-free enterprise, pro-science, pro-human report on environmental issues. The task force concluded that empowering individuals rather than government bureaucracies offers the greatest promise for a cleaner environment. Later, the NCPA produced *New Environmentalism*, written by Reason Foundation scholar Lynn Scarlett. The study proposes a framework for making the nation's environmental efforts more effective while reducing regulatory burdens. More recent publications include a pathbreaking study that showed the costs of the Kyoto protocol on global climate change would far exceed any benefits.

In 1990 the NCPA's Center for Health Policy Studies created a health care task force with representatives from 40 think tanks and research institutes. The pro-free enterprise policy proposals developed by the task force became the basis for a 1992 book, *Patient Power*, by John Goodman and Gerald Musgrave. More than 300,000 copies of the book were printed and distributed by the Cato Institute, and many credit it as becoming the focal point of opposition to Hillary Clinton's health care reform plan.

A number of bills before Congress promise to protect patients from abuses by HMOs and other managed care plans. Although these bills are portrayed as consumer protection measures, NCPA studies show they would make insurance more costly and increase the number of uninsured Americans. An NCPA proposal to solve the problem of the growing number of Americans without health insurance would provide refundable tax credits for those who purchase their own health insurance. The NCPA has assisted members of Congress to formulate a bipartisan tax credits proposal.

NCPA studies, ideas and experts are quoted frequently in news stories nationwide. Columns written by NCPA experts appear regularly in national publications such as the *Wall Street Journal, Washington Times* and *Investor's Business Daily*. NCPA Policy Chairman Pete du Pont has a weekly column on the *Wall Street Journal's* OpinionJournal.com and another weekly column distributed by the Knight-Ridder Tribune news wire. In addition, his radio commentaries reach 2.2 million listeners across America.

According to Burrelle's, the NCPA was mentioned or quoted in about 15 news articles every day somewhere in the United States in 2000. The advertising dollar equivalent of all print and broadcast coverage was more than $50 million.

The NCPA Internet site (www.ncpa.org) embraces the philosophy of one-stop shopping, linking visitors to the best available information on public policy, including studies produced by think tanks all over the world. Brittanica.com named the NCPA Web site one of the best on the Internet for quality, accuracy of content, presentation and usability.

What Others Say about the NCPA

"...influencing the national debate with studies, reports and seminars."

— TIME

"...steadily thrusting such ideas as 'privatization' of social services into the intellectual marketplace."

— CHRISTIAN SCIENCE MONITOR

"The NCPA is unmistakably in the business of selling ideas...(it) markets its products with the sophistication of an IBM."

— INDUSTRY WEEK