Policy Analysis

No. 520 August 4, 2004

Routing

Understanding Privacy—and the Real Threats to It

by Jim Harper

Executive Summary

Properly defined, privacy is the subjective condition people experience when they have power to control information about themselves. Because privacy is subjective, government regulation in the name of privacy can only create confidentiality or secrecy rules based on politicians' and bureaucrats' guesses about what "privacy" should look like. The most important, but elusive, part of true privacy protection is consumers' exercise of power over information about themselves. Ultimately, privacy is a product of personal responsibility and autonomy.

Law has dual, conflicting effects on privacy. Law is essential for protecting privacy because it backs individuals' privacy-protecting decisions, but much legislation plays a significant role in undermining privacy. Indeed, the principal threats to privacy come from governments.

These threats fall into three classes. The first, government surveillance, is a profound and well-recognized threat to privacy. Governments also undermine privacy by collecting, cataloging, and sharing personal information about citizens for administrative purposes. Less acknowledged—but no less important—is the wide variety of laws and regulations that degrade citizens' power to protect privacy as they see fit.

Whether it is anti-privacy regulation, data collection required by all manner of government programs, or outright surveillance, the relationship of governments to privacy is typically antagonistic. Privacy thrives when aware and empowered citizens are able to exercise control of information about themselves. Thoughtful policymakers should recognize the detrimental effects many programs have on consumers' privacy and respond with proposals that reduce the role of government in individuals' lives.

Jim Harper is the editor of Privacilla.org *and director of information policy studies at the Cato Institute.*

CATO INSTITUTE

Although privacy threats from business and new technology are real, the clearest menace to privacy comes from governments.

Introduction

The rapid growth of the Internet in the late 1990s stimulated an important civic discussion of privacy and information practices. Though the Internet spawned the discussion, the privacy debate now extends across the economy—in financial services, health care, and many other areas.

The information practices now being reexamined evolved over decades under principles that are far older. So, even though the Internet brought privacy to the fore, the discussion should not happen at "Internet speed." Too many innovations and consumer benefits are at stake. As it continues to mature, the privacy debate should be carried out deliberately and thoughtfully, by open minds, with an aim toward developing sound long-term policies.

The majority of proposals in Congress, the states, and international bodies have focused on the private sector to achieve privacy goals.[1] This reflects a consensus among politicians and other elites that technology and big business are the greatest privacy threats we face. It is a consensus reinforced by advocates of regulation who have used loaded terms like "Big Browser"[2] to foment privacy concerns.

But George Orwell coined the term "Big Brother" as a warning against the invasive power of governments, not the private sector.[3] Governments are aggressive collectors, users, and sometime abusers of personal and private information.

Although privacy threats from business and new technology are real, the clearest menace to privacy comes from governments. Unlike other social institutions, governments extract information using the force of law. Governments alone can change the rules under which they hold information—without recourse to those aggrieved. And governments routinely frustrate opportunities for individuals to protect privacy as they see fit. Where a web of laws and incentives constrain private-sector use and misuse of data, government databases hang like a sword of Damocles over the privacy and civil liberties of citizens.

Conclusions about privacy should not be drawn lightly or hastily. The subject is too complicated for that. Good policy requires reasoned analysis and thought. Examination reveals that true privacy is threatened most by government action and regulation.

Defining Privacy

An essential starting point, long missing in discussions of privacy, is a definition of the concept itself. The word "privacy" is used casually to describe many concerns in the modern world, and few concepts have been discussed so much without ever being solidly defined. If privacy is going to be a serious topic in information policy—something more than a catch-word in interest-group politics—it needs definition. The attempt below is a serious run at it, but more work from other perspectives will be worthwhile:

Privacy is a state of affairs or condition having to do with the amount of personal information about individuals that is known to others. People maintain privacy by controlling who receives information about them and on what terms. Privacy *is the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values.*

A Personal, Subjective Condition

Importantly, privacy is a subjective condition. It is individual and personal. One person cannot decide for another what his or her sense of privacy is or should be.

To illustrate this, one has only to make a few comparisons: Some Americans are very reluctant to share their political beliefs, refusing to divulge any of their leanings or the votes they have cast. They keep their politics private. Their neighbors may post yard signs, wear brightly colored pins, and go door-to-door to show affiliation with a political party or candidate. The latter have a sense of priva-

cy that does not require withholding information about their politics.

Health information is often deemed intensely private. Many people closely guard it, sharing it only with doctors, close relatives, and loved ones. Others consent to have their conditions, surgeries, and treatments broadcast on national television and the Internet to help others in the same situation,[4] or more commonly, relish the attention, flowers, and cards they receive when an illness or injury is publicized. Privacy varies in thousands of ways from individual to individual and from circumstance to circumstance.

An important conclusion flows from the observation that privacy is a subjective condition: government regulation in the name of privacy is based only on politicians' and bureaucrats' guesses about what "privacy" should look like. Such rules can only ape the privacy-protecting decisions that millions of consumers make in billions of daily actions, inactions, transactions, and refusals. Americans make their highly individual privacy judgments based on culture, upbringing, experience, and the individualized costs and benefits of interacting and sharing information.

The best way to protect true privacy is to leave decisions about how personal information is used to the people affected. Political approaches take privacy decisionmaking power away from the people.

At its heart, privacy is a product of autonomy and personal responsibility. Only empowered, knowledgeable citizens can formulate and protect true privacy for themselves, just as they individually pursue other conditions, like happiness, piety, or success.

The Role of Law

The legal environment determines whether people have the power to control information about themselves. Law has dual, conflicting effects on privacy: Much law protects the privacy-enhancing decisions people make. Other laws undermine individuals' power to control information.

Various laws foster privacy by enforcing individuals' privacy-protecting decisions. Contract law, for example, allows consumers to enter into enforceable agreements that restrict the sharing of information involved in or derived from transactions.[5] Thanks to contract, one person may buy foot powder from another and elicit as part of the deal an enforceable promise never to tell another soul about the purchase. In addition to explicit terms, privacy-protecting confidentiality has long been an implied term in many contracts for professional and fiduciary services, like law, medicine, and financial services. Alas, legislation and regulation of recent vintage have undermined those protections.[6]

Many laws protect privacy in other areas. Real property law and the law of trespass mean that people have legal backing when they retreat into their homes, close their doors, and pull their curtains to prevent others from seeing what goes on within. The law of battery means that people may put on clothes and have all the assurance law can give that others will not remove their clothing and reveal the appearance of their bodies without permission.

Whereas most laws protect privacy indirectly, a body of U.S. state law protects privacy directly. The privacy torts provide baseline protection for privacy by giving a cause of action to anyone whose privacy is invaded in any of four ways.[7] The four privacy causes of action, available in nearly every state, are

- Intrusion upon seclusion or solitude, or into private affairs;
- Public disclosure of embarrassing private facts;
- Publicity that places a person in a false light in the public eye; and
- Appropriation of one's name or likeness.

While those torts do not mesh cleanly with privacy as defined here, they are established, baseline, privacy-protecting law.

Law is essential for protecting privacy, but much legislation plays a significant role in undermining privacy. Dozens of regulatory, tax, and entitlement programs deprive citizens of the ability to shield information from others. And as discussed below, governments

The best way to protect true privacy is to leave decisions about how personal information is used to the people affected.

undermine privacy through both covert and overt surveillance; through administrative recordkeeping and monitoring; and by frustrating the ability of consumers to make privacy-protecting choices when they interact with others.

Consumer Knowledge and Choice

Perhaps the most important, but elusive, part of privacy protection is consumers' exercise of power over information about themselves consistent with their interests and values. This requires consumers and citizens to be aware of the effects their behavior will have on exposure of information about them.

Technology and the world of commerce are rapidly changing, and personal information is both ubiquitous and mercurial. This makes relationships between personal information, behavior, and privacy difficult to catalog, even for full-time students of information policy.

Unfortunately, there is no horn that sounds when consumers are sufficiently aware, or when their preferences are being honored. But study of other, more familiar, circumstances reveals how individuals have traditionally protected privacy.

Consider privacy protection in the physical world. For millennia, humans have accommodated themselves to the fact that personal information travels through space and air. Without understanding how photons work, people know that hiding the appearance of their bodies requires them to put on clothes. Without understanding sound waves, people know that keeping what they say from others requires them to lower their voices.

From birth, humans train to protect privacy. Over millions of years, humans, animals, and even plants have developed elaborate rules and rituals of information sharing and information hiding based on the media of light and sound.

Tinkering with these rules and rituals today would be absurd. Imagine, for instance, a privacy law that made it illegal to observe and talk about a person who appeared naked in public without giving the nudist a privacy notice to that effect. People who lacked the responsibility to put on clothes might be able to sue people careless enough to look at them and to recount what they saw.

A law like that would be ridiculous. But legislation of precisely this character is a staple of the regulation aimed at various economic sectors today. The correct approach, obviously, is for consumers to be educated about what they reveal when they interact online and in business so that they know to wear the electronic and commercial equivalents of clothing.

With the advance of the digital computer over the last few decades, storage and retrieval of information has become increasingly available and widespread. The Internet's even more recent emergence has revealed the digital medium to the public in dramatic fashion. Though digitization is a tiny, incremental change in how information moves and is stored, the consequences will be dramatic, and the benefits of the advance have already been tremendous.[8] Individuals, and society as a whole, are now accommodating themselves to the fact that information can be recorded, maintained, and transferred as never before.

Considering that information practices in physical media evolved over hundreds of generations, society is adjusting to the digital medium very well. Many consumers do struggle, though, to understand how information moves online. The persistence and reproducibility of information in digital form is not intuitive for people who grew up with electric typewriters, though it is for their children. Many people are going online and engaging in e-commerce without knowing how their actions affect privacy. They are right to worry that they are walking around naked in the digital world.

Caught by the rapid, Internet-inspired rise of privacy as a consumer issue, many businesses have been slow to make privacy-protecting options available to their customers. Many markets are too monolithic in their information offerings to accommodate what may be a variety of consumer preferences. Too often a consumer's only option is to share information, which may be inconsis-

The correct approach is for consumers to be educated about what they reveal when they interact online and in business.

tent with his or her preferences, in order to buy a product or service.

That said, it is unclear whether protecting the privacy of ordinary commercial information is a real demand of consumers, or whether it is something they only claim to want when asked by any number of poorly constructed public opinion surveys.[9] Again, there is no horn that sounds when consumers are aware and satisfied.

Though it may be difficult to exercise, consumers in a free market always have the power and choice to absent themselves from privacy-invading transactions. They may use cash if they are not comfortable about how credit card information may be used. They may invest savings in tangible investments like gold bullion if they do not trust financial institutions to protect information consistent with their values. They may refuse to go online because they believe that their behavior on the Internet will be tracked, assembled, and used contrary to their interests. Most importantly, they may educate themselves so that they can make these privacy-protecting choices intelligently.

Privacy Is Not a "Right"

Though generations of advocates have called information privacy a "right," the better view is that it is not. Privacy is a condition people maintain by exercising personal initiative and responsibility. Other legal rights allow them to do this.

An example can illustrate how something as vitally important as privacy is not a right: Most people agree that individuals should be allowed to develop and follow their own sense of morality, as long as they do not harm others. People may decide for themselves, for example, whether a higher power exists; whether bad acts have consequences in a future life; and whether to sing, pray, or remain silent. These, one could argue, reflect a "right" to morality.

As important as morality is, though, there is no "right" to it. Instead, morality is a quality that individuals develop and practice in the shelter given by individual rights like the right to free speech, the right to free exercise of religion, the right to associate with others, and the right to own property. These rights protect individuals from government interference and shelter essential human institutions like morality. People who seek morality as an entitlement from government are censors, at best.

Privacy is the same kind of "good." It is developed and maintained in the shelter of legal rights that give individuals autonomy. Maintaining privacy requires that we know how information moves and that we refrain from sharing what we wish to keep private. Privacy is not a gift from politicians or an entitlement that can be demanded from government. Privacy is a product of personal responsibility.

Like moral living, privacy is the product of careful consideration and concerted effort by individuals. To be sure, protecting privacy can be hard. It involves knowledge, vigilance, and constant trade-offs. But if protecting privacy in private-sector interactions is hard, protecting privacy from government is impossible.

Governments have the power to take personal information from citizens by force of law. After they collect it, they can change the rules under which they keep and use personal information. And they often stand in the way of steps people might otherwise take to protect privacy. That makes governments the most formidable threat to privacy.

Though nearly always animated by good intentions, nearly every government program undermines privacy in some way. It is fair to say that lost privacy is a cost of government. Those interested in allowing individuals to protect their own conceptions of privacy will address this most significant threat to privacy first.

How Governments Threaten Privacy

Governments threaten privacy in three principal ways. Government surveillance is a

Privacy is not a gift from politicians or an entitlement that can be demanded from government. It is a product of personal responsibility.

profound and well-recognized threat to privacy. With the growth of database technologies, overt surveillance has joined its covert sibling as a privacy threat. Less often highlighted is the extent to which governments undermine privacy by collecting, cataloging, and sharing personal information about citizens for administrative purposes. Even less acknowledged—but no less important—is the wide variety of laws and regulations that degrade citizens' power to protect privacy as they see fit. "Anti-privacy" law and regulation is a pervasive cost of welfare-state government.

Privacy too often gives way to other social values, but it should be part of the calculus for all law and regulation. It would be intemperate to call for an end to government programs in the name of privacy, but one of the most fruitful ways to restore privacy would be to reduce the size and scope of government programs and regulation.

Surveillance directly erodes the power of individuals to control information about themselves.

Surveillance

Law enforcement has a difficult job preventing and responding to crime. Agencies and officers of the government are nobly dedicated to protecting citizens and communities from every kind of misdeed, from petty misdemeanors to heinous crimes and terrorism. Information about people helps them do this.

It is no wonder that, with the increasing availability of technology, law enforcement has sought to rely more and more heavily on surveillance. Technological surveillance expands the law enforcement footprint and carries with it many law enforcement benefits.

However, surveillance directly erodes the power of individuals to control information about themselves and the terms on which it is shared. Covert surveillance, like wiretapping, robs people of privacy because it strips them of the awareness they need to protect their privacy. Overt surveillance may erode privacy just as well. Devices like traffic cameras and face-scanning cameras make submitting to observation a condition of appearing on public streets and highways. Though being observed sporadically in public cannot violate reasonable privacy expectations, having data about our public movements cataloged by governments probably does.[10]

There is a constant tension between surveillance powers sought by law enforcement and the privacy-protecting rights enjoyed by all Americans. The rules laid down by the Constitution, chiefly in the Fourth Amendment, demarcate the line between appropriate and inappropriate surveillance.

Fourth Amendment rules on surveillance. The Fourth Amendment is the most direct limit on the power of government to inquire into people's lives, arrest them, and seize their property for criminal investigations. It protects privacy indirectly by extending people's power to conceal information from others. When people have concealed information from society as a whole, the Fourth Amendment's protections generally mean that they have also concealed information from agents of government, unless there is a sufficient legal basis to overcome the concealment.

The Fourth Amendment says: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." It is important to note again that the Fourth Amendment does not protect privacy per se. It allows people to maintain privacy as they see fit. People who expose their affairs to the world expose their affairs to law enforcement.[11] They can make no claim to a free-standing privacy "right."

The Fourth Amendment requires a search to be based on probable cause. That is, government investigators must have a reasonable belief that a crime has been committed and that evidence or fruits of the crime can be found. The first question a court will ask when a citizen claims to have been unconstitutionally searched is whether that person had a reasonable expectation of privacy in the place, papers, or information that government agents have examined or taken.[12]

Until 1967 the Fourth Amendment was largely regarded as protecting places—namely

the home and the areas closely surrounding the home. When the Bill of Rights was adopted, ours was a low-tech, mostly agrarian, and relatively immobile society. The home really was a person's castle. As America has become more mobile and technological, that early interpretation has had to change. *Katz v. United States* is the landmark Supreme Court decision that updated Fourth Amendment law.

In *Katz*, FBI agents without a warrant placed electronic eavesdropping equipment on the outside of a telephone booth where the defendant conducted his business. The Court held that eavesdropping on Katz in this way violated his Fourth Amendment rights because he justifiably relied on the privacy of the telephone booth. The Court stated, in a famous passage, "[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

Consistent with their goal of enforcing the law, governments constantly seek increased surveillance capability, often using new technology. In *Kyllo v. United States*,[13] decided in June 2001, the Supreme Court pushed back against technological surveillance, issuing an important opinion in the development of Fourth Amendment law. Agents of the U.S. Department of the Interior, suspicious that Danny Lee Kyllo was growing marijuana in his home using high-intensity lamps, had aimed an Agema Thermovision 210 thermal imager at his triplex in Florence, Oregon. The imager detected significantly more heat over the roof of the garage and on a side wall of Kyllo's home than elsewhere on the premises. Using this information, the agents obtained a warrant, searched the home, and found the drugs they suspected.

The Supreme Court reversed Kyllo's conviction. It found that when a novel device like a thermal imager is used "to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."

The case required the Court to confront "what limits there are on [the] power of technology to shrink the realm of guaranteed privacy." In remanding Kyllo's conviction, the Court essentially found that the reasonableness of a search is to be judged in light of common privacy-protecting practices, not in light of privacy protection from the best technologies available. Thermal imagers are not in general public use, so people desiring to keep the hours of their sauna private from neighbors do not line their walls with special insulation. The same expectation of privacy applies to law enforcement even if it has the technical capability to observe the heat patterns emanating from houses.

The growth of surveillance continues. The Supreme Court's ruling in Kyllo notwithstanding, government surveillance continues to grow in prominence as a privacy-reducing law enforcement tool. The USA PATRIOT Act and the Homeland Security Act are only two of the most recent in a long list of laws that reduce the privacy protections Americans enjoy.

The USA PATRIOT Act permits "pen register" and "trap and trace orders" for electronic communications such as e-mail (akin to caller ID information made available to authorities). It authorized nationwide execution of court orders for pen registers, trap and trace devices, and access to stored e-mail or communications records. And it lowers the protections for stored voice mail, making it accessible to law enforcement on easier terms than telephonic conversations.[14]

Some argue that these are appropriate updates to the law in light of new technologies, or that they are necessitated by the war on terrorism. It is important to recognize how this view holds that reduced privacy is appropriate—not that privacy is equally protected under the new law. And, as to the claim that the act is an emergency measure justified by the war on terrorism, it has already been used in ordinary crime investigations that have no nexus to national security or terrorism.[15]

The USA PATRIOT Act and the Homeland Security Act are only two of the most recent in a long list of laws that reduce the privacy protections Americans enjoy.

If not properly limited, red-light cameras, speed cameras, and biometric sensors may be used to catalog the movements of innocent citizens, contrary to their privacy expectations and their Fourth Amendment rights.

The list of surveillance laws, technologies, and programs is long and growing. The Communications Assistance for Law Enforcement Act,[16] for example, was passed in 1994. For the first time in history, telecommunications companies were required to modify their equipment to facilitate government surveillance. Federal authorities are working assiduously to extend CALEA requirements to Internet applications that provide voice communications, such as Voice over Internet Protocol (VoIP).[17] From there, little logical difference prevents its extension to all Internet communications.

Such pretensions are well-founded in recent history. "Carnivore," for example, is a specialized computer developed by the FBI and equipped with software that can scan Internet traffic at extremely high speed. It attaches to the systems of Internet service providers (ISPs) and can be used either legitimately, to observe Internet use that is subject to a valid search warrant, or illegitimately, to observe the behavior of everyone using a particular ISP, including entirely innocent people.

As electronic devices are incorporated into our interactions with government, they give governments more and more opportunities for monitoring and surveillance. In the area of transportation, electronic devices, such as the "E-ZPass" on Northeast toll roads and Northern Virginia's "Smart Tag," put government officials in a position to monitor the movements of citizens.

Red-light cameras and speed cameras are another part of the rapidly growing Big Brother infrastructure. Little technical difference separates a digital camera that takes occasional snapshots from one that records continuous footage. Equipped with optical character recognition technology, traffic cameras may soon have the technical capability to read license plates and scan traffic for specific cars. Networked cameras will be able to track cars throughout a city and on the highways. And database technology will make it possible to create permanent records of the movements of all cars captured on camera.[18]

Of course, these technologies can be used for good. Red-light cameras can improve safety—as long as they are not used in conjunction with shortened yellow-light times. When we are able to use traffic cameras to find stolen vehicles, for example, the effect on car-jacking may be dramatic. Criminals will know that they have only minutes from when they steal a car to when that car effectively turns them in. These technologies may help authorities learn about the last movements of missing persons more easily thanks to records of where their cars were. But, to protect privacy, records such as these should be destroyed promptly if they are not being put to such a use.

Biometrics is yet another emerging technology that can be used for government surveillance.[19] Despite a checkered record, facial scanning and other biometric techniques will probably persist and grow as tools of government surveillance.

If not properly limited, red-light cameras, speed cameras, and biometric sensors may be used not just to search for crime suspects but to catalog the movements of innocent citizens, contrary to their privacy expectations and their Fourth Amendment rights. Without protections for innocent people, law enforcement will follow its natural tendency to catalog the actions and movements of all citizens. We know this because the plans have already been announced.

The Transportation Security Agency's Computer Assisted Passenger Pre-Screening program (CAPPS II) will maintain records of all travelers in the United States, without regard to whether they are suspected of any wrongdoing. CAPPS II starts from the premise that law enforcement can stop all travelers to demand their papers, which demands review in terms of constitutional Due Process. CAPPS II becomes a privacy threat by maintaining records of all those who are stopped. Privacy Act notices issued by the Transportation Security Administration suggest that traveler information will be disposed of promptly, but such commitments can change at any time.[20] Unchecked, surveillance of Americans may expand to wherever they are on the move.

"Data-veillance." Real-time, technological monitoring of Americans' public activity is only the newest, most dramatic form of surveillance. It joins a long, growing, and deplorable tradition of amassing databases of information about citizens' financial and commercial privacy in service to ends dictated by government.

The Financial Crimes Enforcement Network, or "FinCEN," is the premier example. FinCEN is a network of databases and financial records maintained by the U.S. Treasury Department. The FinCEN surveillance system handles more than 140 million computerized financial records compiled from 21,000 depository institutions and 200,000 nonbank financial institutions. Banks, casinos, brokerage firms, and money transmitters all must file reports with FinCEN on cash transactions over $10,000. And FinCen is the repository for "Suspicious Activity Reports," which regulators have required financial institutions to file under the Bank Secrecy Act for years. An explicit legal requirement to do this was resoundingly rejected in 1999, then made law in the USA PATRIOT Act after the September 11 attacks.

FinCEN also uses a variety of law enforcement databases, including those operated by the Drug Enforcement Agency and the Defense Department, in addition to commercial databases of public records. FinCEN may also use databases held by the Central Intelligence Agency, the National Security Agency, and the Defense Intelligence Agency.

FinCEN shares information with investigators from dozens of agencies, including the Bureau of Alcohol, Tobacco, and Firearms; the Drug Enforcement Administration; the Federal Bureau of Investigation; the U.S. Secret Service; the Internal Revenue Service; the Customs Service; and the the U.S. Postal Inspection Service. Agents from all of those agencies can investigate names, addresses, and Social Security numbers through FinCEN. Field agents and state and local law enforcement can access data from FinCEN remotely.

The theory behind FinCEN is to constantly survey the financial movements of the entire society in order to root out bad actors, using the financial services sector as a sort of deputy investigator. The privacy of individual consumers' financial data is obliterated by programs such as this.[21]

FinCEN implicates more than privacy, of course. It is the quintessential example of a government database system that can be used to investigate people instead of crimes. An investigator, rightly or wrongly convinced of the guilt of a certain party, may use FinCEN to investigate that person, looking for wrongdoing of any kind rather than the crime the investigator is tasked with solving. Especially today, when exceedingly complex regulation trips up nearly everyone somehow, this is an inversion of the proper way to fight crime. Crime fighters should always identify and punish perpetrators of known crimes. They should not identify people 'suitable for punishment' and then identify what they may have done wrong.

FinCEN is one of many surveillance programs that undermine the privacy all Americans should enjoy. It is at the leading edge of a trend toward deploying data collected by governments into surveillance tools. Elements of the proposed CAPPS II program and the widely discredited Total Information Awareness program would go even further, using private-sector information such as credit card purchases, car rentals, and the like for routine government decisionmaking and investigation purposes. These practices unacceptably blur the line between privately and publicly held data.

As discussed below, databases are routinely shared among federal agencies and between the federal and state governments for administrative purposes. Legislation enacted in a time of crisis could convert them all to surveillance purposes, when they are not already being used in this way.

Though occasionally necessary, neither database surveillance nor traditional surveillance is ever desirable. They should be reduced at every turn. Unfortunately, a particular breed of crime law necessitates them.

Anti-drug laws take a tremendous toll on the privacy of innocents.

Victimless crime laws drive surveillance. In traditional crime-fighting, law enforcement becomes aware of a crime when the victim complains about it. This course is not followed in victimless crime laws. Victimless crimes have no complaining witness because all parties consent to the illegal behavior, even though they may harm themselves. For such crimes to be discovered, law enforcement must take its observation of the public to unusual lengths. The natural effect is to dramatically erode privacy for everyone.

Anti-drug laws, while they may be the product of beneficent motives, take a tremendous toll on the privacy of innocents. While the War on Drugs has raged, a string of U.S. Supreme Court cases has eroded the Fourth Amendment's privacy protections.[22]

Because so many Fourth Amendment search and seizure cases have dealt with whether evidence of illegal drugs should be suppressed, courts have sometimes bent over backwards to validate dubious law enforcement activity as lawful search and seizure. The result is that every American has a weakened right to walk or drive public streets free from interference with their persons, their possessions, and their privacy.

Money-laundering laws began as a fairly direct outgrowth of the perverse economic incentives drug laws create and the difficulty with enforcing them. Prior to September 11, 2001, the groundwork was being laid for a careful review of whether money-laundering laws and practices effectively prevented crime.[23] The results of such a review probably would not have supported the anti-money-laundering regime. The War on Terrorism has unfortunately given new life to money laundering laws.

Though they are motivated by crime prevention, most measures to prevent money laundering undermine financial privacy, best evidenced by programs like FinCEN. The administrative burdens are suffered, and the expenses paid, by everyone who uses the banking system. They prevent financial anonymity and put reams of data about consumer banking activity in the hands of financial institutions and, ultimately, regulators and government investigators.

The growth in money-laundering laws and investigations represents a shift from trying to address crime directly to trying to address crime by tracking its instruments and fruits. Money-laundering laws and investigations are poor substitutes for attacking crime head-on. Among other things, they compromise the privacy of innocent, law-abiding people right along with the criminals.

Gambling is another victimless crime that holds out much privacy-invading potential, thanks to the growth of the Internet. For different reasons, gambling opponents and holders of existing gambling franchises are concerned that Internet gambling will spill across state and national borders and become ubiquitous worldwide.[24] Some politicians are genuinely interested in the financial and social well-being of their constituents. Others are worried about losing a revenue stream for local gambling interests, including state governments.

Internet gambling laws threaten to increase government monitoring of the Internet, including monitoring of innocent, law-abiding citizens. The Internet, of course, substitutes a network for the card room where law enforcement could formerly go to break up an illegal game. But it carries perfectly legitimate communication and commerce right alongside "illegal" traffic. Law enforcers tapping into the Internet looking for gambling will be sorely tempted to abandon limits on the source, destination, and type of Internet traffic that they review. More than any previous surveillance regime, Internet surveillance will bring law enforcement into close proximity with the private communications of entirely law-abiding Americans.

Victimless crimes like drug use, money laundering, and illegal gambling are some of the primary drivers of law enforcement surveillance. Of necessity, government surveillance deprives people of privacy, taking away their power to define what information about themselves will be shared, and on what terms.

Victimless crimes, such as drug use, money laundering, and illegal gambling, are some of the primary drivers of law enforcement surveillance.

Database Nation, Indeed

Whereas surveillance for crime control is an antagonistic collection of personal information, governments erode citizens' power and privacy for beneficent reasons too. To provide benefits and entitlements—and, of course, to tax—governments take personal information from citizens by the bushel. Nearly every new policy or program justifies new or expanded databases of information—and a shrunken sphere of personal privacy. The helping hand of government routinely strips away privacy before it goes to work.

The *National Directory of New Hires* provides a good example. This is a database of information on all newly hired employees, quarterly wage reports, and unemployment insurance claims in the United States. The impulse behind this database is laudable—to help states locate parents who have skipped out on their child support obligations. But, like many databases with laudable purposes, it catalogs everyone to get at the small number of bad people who renege on their child-support obligations.

Such databases also have clear tendencies to grow and adopt new uses, uses that, at some point, may vary dramatically from their original purposes. Already, the New Hires database has been expanded to track down student loan defaulters. The Internal Revenue Service may access the database for the purpose of administering the Earned Income Tax Credit program and verifying claims with respect to employment in tax returns. The Social Security Administration may access it for any reason whatsoever.[25]

There may be plenty of good reasons to have confidential employment relationships. Employers and employees can at least be indifferent to each other's personal details in the day-labor context. But it is it is illegal not to make records of employment relationships because employment is a key avenue through which the government collects information about people. The *National Directory of New Hires* is a national employment dragnet designed to get at the relatively small number of people who may actually do wrong. The cost in lost privacy is disproportionate to the law enforcement benefit.

If employment information is too mundane to get worked up about in terms of privacy, there are plenty of other government databases that collect far more sensitive information—by law and without the consent of citizens. The Centers for Medicare and Medicaid Services, for example, maintains a database called OASIS, or Outcome and Assessment Information Set, which collects data on all Medicare and Medicaid patients receiving skilled home health care services.

The OASIS system collects a breathtaking amount of information. OASIS "data sets" include name, Social Security number, residence, birth date, gender, payment sources for health care, recent medical treatment, current condition, risk factors, living arrangements, safety hazards in patient's residence, sanitation of residence, identity of people assisting patient, vision and speech status, ability to breathe, ability to move bowels and urinate, cognitive function, and much more.[26]

Doctors often need such information to provide health care, but whether it should be collected in a government database is another question entirely. OASIS shows how Medicare and Medicaid deprive patients of the power to protect the privacy of often deeply personal information.

As the cost of health care continues to spiral upward, politicians and bureaucrats will undoubtedly be pressured to make new uses of the information in this database, looking for ways that personal information can be used to cut costs. In light of new priorities, current promises about privacy will be set aside with impunity—because the government holds the data.

Speaking of highly personal and sensitive information—and speaking of acronyms—there is CODIS, the Combined DNA Index System. Established as a pilot project in 1990 and enshrined into law by Congress in 1994,[27] CODIS gives federal funds to states that assist the FBI in collecting DNA information. Today, 48 of the 50 states, the U.S. Army, the FBI, and Puerto Rico participate in

Law-abiding citizens should resist the growth of databases like CODIS because they ultimately represent threats to the privacy and civil rights of everyone.

A number of bureaucracies and politicians are moving to make tax policy even more invasive than it already is.

the program, collecting DNA samples for the federal database.

As with so many government databases, the original purpose of CODIS—to collect only information about convicted sex offenders—was entirely laudable. Now that CODIS is established, however, the push to expand it has begun. As the CODIS program notes on its website, the data includes "individuals convicted of sex offenses (and other violent crimes), with many states now expanding legislation to include other felonies."[28] The time when misdemeanors are added to the list may not be far away.

The temptations presented to bureaucrats and law enforcement by massive government databases of DNA information are great. Law-abiding citizens should resist the growth of databases like CODIS because they ultimately represent threats to the privacy and civil rights of everyone.

Of course, separate databases are one thing. Combined databases and dossiers are quite another. The federal government is very much in that business, too.

Government exchange and merger of citizens' personal information is systematic and routine.[29] During the 18-month period from September 1999 to February 2001, federal agencies announced 47 times—more than once every two weeks—that they would exchange and merge personal information from databases about American citizens.

These programs are only the tip of an information-trading iceberg. The data-sharing programs surveyed in the *Privacilla* report were only the federal agency programs that exchange and merge databases of personal information under the Computer Matching and Privacy Protection Act, an amendment to the Privacy Act of 1974 that deals with a subset of Privacy Act records.[30] Under the broader Privacy Act, federal agencies can combine databases and redeploy them at will after announcing a new "routine use" in the *Federal Register*.[31]

The Veterans Administration announced one such "routine use" in January of 2001, when it established a new "Consolidated Data Information System."[32] The information contained in that system is just about everything under the sun, as the *Federal Register* announcement reflects:

> The categories of records in the system will include veterans' names, addresses, dates of birth, VA claim numbers, SSNs, and military service information; medical benefit application and eligibility information; code sheets and follow-up notes; sociological, diagnostic, counseling, rehabilitation, drug and alcohol, dietetic, medical, surgical, dental, psychological, and/or psychiatric medical information; prosthetic, pharmacy, nuclear medicine, social work, clinical laboratory and radiology information; patient scheduling information; family information such as next of kin, spouse and dependents; names, addresses, Social Security numbers and dates of birth; family medical history, employment information; financial information; third-party health plan information; information related to ionizing radiation and Agent Orange; date of death; VA claim and insurance file numbers; travel benefits information; military decorations; disability or pension payment information; information on indebtedness arising from 38 U.S.C. benefits; medical and dental treatment in the Armed Forces and claim information; applications for compensation, pension, education and rehabilitation benefits; information related to incarceration in a penal institution; medication profile such as name, quantity, prescriber, dosage, manufacturer, lot number, cost and administration instruction; pharmacy dispensing information such as pharmacy name and address.[33]

And the list goes on.

This database is held by the Veterans Administration, which has suffered from notorious computer security lapses. Testimony in September 2000 revealed to the House

Veterans Affairs Committee that a security company hired by the VA's Office of Inspector General had no trouble breaking into the VA's computer system and taking total control of it.[34] An assistant inspector general at VA was reported saying that the hackers "owned the system" and that the VA didn't even know its systems were attacked. The hackers-for-hire had access to the confidential data of veterans, including their personal histories and medical and financial information, in addition to VA's internal data and business systems.

Receiving government benefits is costly in terms of privacy. Paying for them is costly too. Taxation is one of the most pervasive ways that governments threaten the privacy of citizens. To implement tax policies, governments must collect truly massive quantities of data. This includes name, address, phone number, Social Security number, income, occupation, marital status, parental status, investment transactions, home ownership, medical expenses, purchases, foreign assets, charitable giving, and so on.

The list is very, very long because politicians are enamored of social engineering through tax policy. Anyone compiling a dossier on our behavior would find the files of the taxing authorities a terrific resource.

This resource has been misused again and again in recent history. In 1971 a paranoid President Richard Nixon vowed to select an IRS commissioner who would make sure that "every income tax return I want to see I see."[35] Sen. Frank Church's Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities found in 1975 that the IRS regularly gave any tax return requested to the Federal Bureau of Investigation and the Central Intelligence Agency. The IRS at that time had specialized, secret staff whose job was to conduct surveillance and intelligence-gathering activities against various political groups without any basis in tax law enforcement.[36]

Loss of privacy is a direct cost of most tax laws, which could be reformulated to reduce the need for broad collection of individual financial information. Made fair and easy to comply with, rather than complex and punitive, tax laws would see higher compliance without requiring reporting and investigation of individuals' personal financial details. Proposals to replace the current income tax with a flat tax or national sales tax would have the significant additional benefit of enhancing privacy.

But a number of bureaucracies and politicians are moving to make tax policy even more invasive than it already is. The Paris-based Organization for Economic Cooperation and Development, for example, consistently works to increase the ability of its member governments to access the financial information of their citizens.[37] The OECD issued a report in April, 2000, called "Improving Access to Bank Information for Tax Purposes."[38] "Bank information" is, of course, a euphemism for *customer* information held by banks.

Similarly, a group of U.S. state government and tax collection associations continues to press an effort to expand the collection of taxes on retail sales via e-commerce, catalog, and phone.[39] Touted as "streamlined" or simplified taxation, these proposals would invariably require massive databases of consumer-purchasing information. All destination-based systems to tax remote commerce (that is, taxing where the consumer resides rather than where the seller resides) would require consumers' purchases to be tracked and stored in databases.

Government databases cover myriad subjects. With technology's advance, they may soon contain nearly every citizen activity that can be observed by government.[40] Databases, of course, are only the digitized portion of those substantial collections of information known as public records. Public records policy as a whole is in need of reconsideration from the standpoint of privacy.[41]

The solution is smaller government. Public records represent a wide variety of information that is held by government, including deeds to property and liens, drivers' license information, crime records, tax records, entitlement program records, and so on. Public records threaten privacy and related interests

The only satisfactory protection for privacy in the case of public records is to reduce the role of government in the intimate details of citizens' personal, social, and economic lives.

The U.S. government's long battle against private use of strong encryption is probably the best example of anti-privacy regulation.

in a variety of ways. They are produced at the expense of Americans' power over information about themselves. They create opportunity for law enforcement snooping. They prevent anonymity and pseudonymity. They can be improperly used by bureaucrats or released indiscriminately to wrongdoers in the public. And, acquired by criminals, they can be used to further fraud and violent crimes.

Public records have many beneficial uses, of course. Public records enable the press and community leaders to investigate and thwart wrongdoing. Reporters have used such records to uncover alcohol abuse by airline pilots and school bus drivers. Millions of people change their last names each year due to marriage and divorce, and millions of consumers move every year. Credit reporting agencies and others use public records to track these changes and preserve the good credit records of many people, while protecting against people who would hide their bad credit history or other negative background.

Public access to government records also plays a large part in ensuring open government. Access to public records allows citizens to monitor the functions of their government directly, and it allows the press to fully exercise its watchdog role.

Blanketing public records with secrecy is not a satisfactory solution. That would compromise important open-government values and prevent beneficial uses. Governments should not be able to keep secret records on citizens. Nor is redaction, or editing, of records made available to the public a satisfactory solution. That would leave fallible government officials and bureaucracies in control of citizens' personal information—and unanswerable for their conduct.

Instead, loss of privacy must be recognized as a cost of government programs that require citizens to be counted, cataloged, measured, tested, and watched. The only satisfactory protection for privacy in the case of public records is to reduce the need for public records in the first place, by reducing the role of government in intimate details of citizens' personal, social, and economic lives.

To the extent records are collected, they should generally be available to the public to prevent secret government databases from becoming common practice. Information in public records should be kept secret only if that will have a substantial role in preventing identified and discrete harms to the public.

Massive collections of public records—and particularly public records databases—are a sword of Damocles hanging over privacy and civil liberties. Only shrinking the need for such records by shrinking government's role can reduce the threat.

Shrinking government's role can expand privacy by lessening the interference of regulation with individuals' privacy-protecting decisions. Anti-privacy law and regulation is the third kind of threat that governments pose to privacy.

Anti-Privacy Law and Regulation

Perhaps the least recognized category of government threats to privacy is what can be called "anti-privacy" law and regulation. Myriad laws and rules deprive people of autonomy, preventing them in various ways from taking steps to protect privacy as they see fit. Anti-privacy law and regulation may prevent people from using privacy-protecting technologies, it may prohibit privacy-protecting contracts, or, by distorting markets, it may push people to give up privacy in ways they ordinarily would not.

The U.S. government's long battle against private use of strong encryption is probably the best example of anti-privacy regulation. Encryption is a way to encode computer files so that only someone with access to a mathematical "key" can read them. Encryption can protect computer systems and intellectual property from industrial spies and malicious hackers. Just as importantly, encryption can help individuals control what they reveal when they use digital technology. Encryption is essential for protecting individual privacy in the digital age.

Instead of viewing it as an empowering technology, the U.S. government originally viewed

encryption as a threat to the capabilities of law enforcement. While it is true that encryption can be used by criminals, its widespread use would create more benefits than harms, especially in the area of personal privacy.

Ultimately, encryption technology cannot be controlled. Past policies limiting the use of encryption kept it away from law-abiding people, threatening their privacy, without restricting the criminals and terrorists using such technology in spite of the laws.

Anti-privacy laws that prevent privacy-protecting contracts and agreements take myriad forms. The Bank Secrecy Act, for example, prevents financial institutions from assuring their customers of privacy in financial information. In fact, it deputizes them into reporting activities that banks or their employees deem "suspicious."

Congress and the Federal Communications Commission have ensured that the location of mobile phone users can be tracked. E911, or enhanced 911, is a Federal Communications Commission program that was created for the obviously good purpose of helping authorities locate emergency callers.[42] But E911 also represents a significant threat to privacy in that it forces a location-tracking technology onto mobile phone users.

Ironically, pro-regulation privacy advocates tout the threat in having commercial mobile phone providers able to pinpoint customer location; they blame these businesses for considering using this data, overlooking the fact that the U.S. federal government mandated mobile phone tracking in the first place.[43] Most consumers assuredly would want tracking for its safety, convenience, and commercial benefits. Some consumers may value privacy enough to forgo the public safety benefits of mobile phone tracking. The latter will not have this privacy-protecting choice thanks to the anti-privacy E911 mandate.

Another example of anti-privacy law and regulation is the federal government's tax treatment of employee health benefits. Current tax policy creates strong incentives for employers to purchase health care for their employees, discouraging consumers from doing so directly. This drives people to compromise privacy in ways they ordinarily would not. Among the many concerns about health privacy (and discrimination based on health status) is the problem of businesses having employees' personal health information and using it to make decisions about them. The root of this problem is federal tax policy, which distorts the market for health insurance by discouraging individuals from buying the right insurance for their particular needs.[44]

Massive federal regulation aimed at health privacy is the product of systematic, disempowering interference with health care markets by the federal government. Rather than imposing new regulations on how health plans may use information, Congress should address the source of the problem by taking from business and restoring to consumers the incentives to buy insurance. A provision in the recent Medicare prescription drug law expanding Health Savings Accounts may begin to achieve this goal.[45]

Nearly every law has consequences for privacy, and many laws are very harmful to privacy indeed. All of them are intended to protect citizens from various ills, but when privacy is added to the analysis, the bargain they offer is sometimes far less attractive. Privacy should be a consideration whenever a new law or regulation is considered. If it is not, anti-privacy law and regulation will flourish—to the detriment of the technologies, contracts, and markets that protect privacy on the true terms real consumers want.

Conclusion

Claims by regulators and politicians that they are going to deliver privacy usually involve some kind of regulation placed on the private sector. The most productive approach, however, would be for our representatives in Congress and the state legislatures to reduce the privacy-eroding features of the laws and programs they themselves pass and oversee.

Whether it is anti-privacy regulation, data collection required by all manner of govern-

Rather than impose new regulations on how health plans use information, Congress should restore to consumers the incentive to buy insurance.

ment programs, or outright surveillance, the relationship of governments to privacy is typically antagonistic. Privacy thrives when aware and empowered citizens are able to exercise control of information about themselves. It is not a gift from politicians or an entitlement bestowed by government.

As the privacy debate matures, it should become clearer that governments are a chief threat to privacy. Thoughtful policymakers in the future will recognize the detrimental effects many programs have on consumers' privacy and respond with proposals that reduce the role of government in individuals' lives.

As the privacy debate matures, it should become clearer that governments are a chief threat to privacy.

Notes

1. Of the 23 proposals listed in a June 2002 Congressional Research Report on pending legislation, 17 were aimed at the private sector, 4 dealt with the government sector, and 2 addressed both. Half of the proposals aimed at government required only reporting or study. See Marcia S. Smith, "Internet Privacy: Overview and Pending Legislation," Congressional Research Service (June 20, 2002; Order Code RL31408), http://usinfo.state.gov/usa/infousa/tech/reports/rl31408.pdf.

2. Nicholas Morehead, "Dems: 'Big Browser' Is Watching," *Wired News* (Oct. 16, 2000), http://www.wired.com/news/privacy/0,1848,39466,00.html; Sen. John Edwards, "Big Browser Is Watching" (July 14, 2000), http://edwards.senate.gov/press/2000/columns/0714_browser.html.

3. George Orwell, *1984* (New York: Harcourt, Brace, Jovanovich, 1949).

4. See, e.g., "One Man's Experience of Healing from Cancer," http://www.christopher-sheppard.com/health.htm; and Cram et al., "The Impact of a Celebrity Promotional Campaign on the Use of Colon Cancer Screening: the Katie Couric Effect," *Archives of Internal Medicine* (2003), http://archinte.ama-assn.org/cgi/content/full/163/13/1601.

5. See "Contracts," http://www.privacilla.org/business/contracts.html.

6. The Gramm-Leach-Bliley Act and federal regulations under the Health Insurance Portability and Accountability Act institutionalized sharing of personal information with government authorities and various "approved" institutions. See 15 U.S.C. §§ 6802(e)(5)&(8); various subsections of 45 C.F.R. 164.512.

7. "The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection," http://www.privacilla.org/releases/Torts_Report.html.

8. Information about the ongoing growth in the electronic economy is available from the Department of Commerce's E-Stats Web page, http://www.census.gov/eos/www/ebusiness614.htm.

9. Solveig Singleton and Jim Harper, "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us," Competitive Enterprise Institute, June 1, 2001, http://www.cei.org/gencon/025,02061.cfm.

10. See James W. Harper, "Testimony at a Hearing on Red-Light Cameras, U.S. House of Representatives Committee on Transportation and Infrastructure Subcommittee on Highways and Transit," http://www.privacilla.org/releases/redlight_camera_testimony.html.

11. The "plain view" doctrine illustrates this point well. A government agent observing objects and facts from a place where he or she is authorized to be does not conduct a "search" within the meaning of the Fourth Amendment. See *Harris v. United States*, 390 U.S. 234 (1968).

12. *U. S. v. Katz*, 389 U.S. 347 (1967).

13. 533 U.S. 27 (2001).

14. See Charles Doyle, "The USA PATRIOT Act: A Sketch," Congressional Research Service, April 18, 2002, http://www.fas.org/irp/crs/RS21203.pdf.

15. See Clarence Page, "All of a Sudden the Patriot Act Isn't Just about Terrorists Anymore," *Salt Lake Tribune*, Nov. 15, 2003, http://www.sltrib.com/2003/Nov/11152003/commenta/commenta.asp.

16. Pub. L. No. 103-414, 108 Stat. 4279.

17. See, for example, Patrick W. Kelly, Deputy General Counsel, Federal Bureau of Investigation, Letter to John Rogovan, General Counsel, FCC, January 28, 2004, http://www.neca.org/wawatch/wwpdf/013004_7.pdf.

18. See Harper, "Testimony at a Hearing on Red-Light Cameras."

19. See generally, Clyde Wayne Crews Jr., "Human Bar Code: Monitoring Biometric Technologies in a Free Society," Cato Institute Policy Analysis no. 452, September 17, 2002, http://www.cato.org/pubs/pas/pa-452es.html.

20. See "Comments of Privacilla.org on 'Notice of Status of System of Records; Interim Final Notice; Request for Further Comments,'" September 30,

2003, http://www.privacilla.org/releases/TSA_comments_09-30-03.pdf.

21. See James W. Harper, "Prepared Remarks to the Bank Secrecy Act Advisory Group, U.S. Department of Treasury," October 22, 2003, http://www.privacilla.org/releases/BSAAG_remarks_10-22-03.html.

22. Declan McCullagh, "Privacy a Victim of the Drug War," *Wired News*, December 11, 2000, http://www.wired.com/news/politics/0,1283,40532,00.html.

23. See, for example, U.S. Department of the Treasury, Office of Enforcement, "The 2001 National Money Laundering Strategy," http://www.ustreas.gov/press/releases/docs/ml2001.pdf

24. See National Gambling Impact Study Commission, http://govinfo.library.unt.edu/ngisc/index.html.

25. Office of Child Support Enforcement, U.S. Department of Health and Human Services, "Accuracy of Data Maintained by the National Directory of New Hires and the Effectiveness of Security Procedures," July 31, 2002, http://www2.acf.hhs.gov/programs/cse/pubs/2002/reports/ndnh_data_accuracy.html#N100C9.

26. See Center for Health Services Research, "Outcome and Assessment Information Set (OASIS B-1)," December 2002, http://www.cms.hhs.gov/oasis/soc.pdf.

27. The DNA Identification Act of 1994, Pub. L. No. 103-322.

28. National DNA Index System Web page, http://www.fbi.gov/hq/lab/codis/national.htm.

29. "Privacy and Federal Agencies: Government Exchange and Merger of Citizens' Personal Information Is Systematic and Routine," March 2001, http://www.privacilla.org/releases/Government_Data_Merger.html.

30. See U.S. Department of Justice, "Overview of the Privacy Act of 1974, Computer Matching," 2002, http://www.usdoj.gov/04foia/1974compmatch.htm.

31. 5 U.S.C. § 552a(b)(3).

32. Department of Veterans Affairs, "Report of New System of Records—Consolidated Data Information System—VA (97VA105)," *Federal Register* 66 (January 16, 2001): 3650.

33. Ibid., p. 3652.

34. House Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations, "Hearing II on Information Technology," September 21, 2000, http://veterans.house.gov/hearings/schedule106/sept00/9-21-00/witness. htm.

35. Charlotte Twight, *Dependent on D.C.* (Washington: Cato Institute, 2002), p. 271.

36. See Daniel J. Pilla, "Why You Can't Trust the IRS," Cato Institute Policy Analysis no. 222, Washington, April 15, 1995, http://www.cato.org/pubs/pas/pa222.html.

37. See The Prosperity Institute, Task Force on Information Exchange and Financial Privacy, "Report on Financial Privacy, Law Enforcement, and Terrorism," Alexandria, Virginia, March 25, 2002, http://www.911investigations.net/IMG/pdf/doc-386.pdf.

38. See Organization for Economic Cooperation and Development, "Improving Access to Bank Information for Tax Purposes: The 2003 Progress Report," http://www.oecd.org/dataoecd/5/0/14943184.pdf.

39. See Streamlined Sales Tax Project, http://www.streamlinedsalestax.org/.

40. See, for example, "Computer Security: How Vulnerable Are Federal Computers?" Testimony of Solveig Singleton, then director of information studies at the Cato Institute, before a hearing of the Subcommittee on Government Management, Information, and Technology, September 11, 2000, http://www.house.gov/reform/gmit/hearings/2000hearings/000911computersecurity/000911ss.htm.

41. A beginning step has been taken in Alan Charles Raul, *Privacy and the Digital State: Balancing Public Information and Personal Privacy* (Boston: Kluwer Academic Publishers, 2001).

42. See Federal Communications Commission, "Enhanced 911," http://www.fcc.gov/911/enhanced/.

43. See generally, Federal Trade Commission workshop, "The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues," December 11–12, 2000, http://www.ftc.gov/bcp/workshops/wireless/.

44. See "Health Privacy in the Hands of Government: The HIPAA Privacy Regulation—Troubled Process, Troubling Results," April 2003, http://www.privacilla.org/releases/HIPAA_Report.html.

45. Medicare Prescription Drug Improvement and Modernization Act of 2003, Pub. L. No. 108-173, Title XII, § 1201.

OTHER STUDIES IN THE POLICY ANALYSIS SERIES

519. **Nuclear Deterrence, Preventive War, and Counterproliferation** by Jeffrey Record (July 8, 2004)

518. **A Lesson in Waste: Where Does All the Federal Education Money Go?** by Neal McCluskey (July 7, 2004)

517. **Deficits, Interest Rates, and Taxes: Myths and Realities** by Alan Reynolds (June 29, 2004)

516. **European Union Defense Policy: An American Perspective** by Leslie S. Lebl (June 24, 2004)

515. **Downsizing the Federal Government** by Chris Edwards (June 2, 2004)

514. **Can Tort Reform and Federalism Coexist?** by Michael I. Krauss and Robert A. Levy (April 14, 2004)

513. **South Africa's War against Malaria: Lessons for the Developing World** by Richard Tren and Roger Bate (March 25, 2004)

512. **The Syria Accountability Act: Taking the Wrong Road to Damascus** by Claude Salhani (March 18, 2004)

511. **Education and Indoctrination in the Muslim World: Is There a Problem? What Can We Do about It?** by Andrew Coulson (March 11, 2004)

510. **Restoring the U.S. House of Representatives: A Skeptical Look at Current Proposals** by Ronald Keith Gaddie (February 17, 2004)

509. **Mrs. Clinton Has Entered the Race: The 2004 Democratic Presidential Candidates' Proposals to Reform Health Insurance** by Michael F. Cannon (February 5, 2004)

508. **Compulsory Licensing vs. the Three "Golden Oldies": Property Rights, Contracts, and Markets** by Robert P. Merges (January 15, 2004)

507. **"Net Neutrality": Digital Discrimination or Regulatory Gamesmanship in Cyberspace?** by Adam D. Thierer (January 12, 2004)

506. **Cleaning Up New York States's Budget Mess** by Raymond J. Keating (January 7, 2004)

505. **Can Iraq Be Democratic?** by Patrick Basham (January 5, 2004)

504. **The High Costs of Federal Energy Efficiency Standards for Residential Appliances** by Ronald J. Sutherland (December 23, 2003)

503. **Deployed in the U.S.A.: The Creeping Militarization of the Home Front** by Gene Healy (December 17, 2003)

502. **Iraq: The Wrong War** by Charles V. Peña (December 15, 2003)

501. **Back Door to Prohibition: The New War on Social Drinking** by Radley Balko (December 5, 2003)

500. **The Failures of Taxpayer Financing of Presidential Campaigns** by John Samples (November 25, 2003)

499. **Mini-Nukes and Preemptive Policy: A Dangerous Combination** by Charles V. Peña (November 19, 2003)

498. **Public and Private Rule Making in Securities Markets** by Paul G. Mahoney (November 13, 2003)

497. **The Quality of Corporate Financial Statements and Their Auditors before and after Enron** by George J. Benston (November 6, 2003)

496. **Bush's National Security Strategy Is a Misnomer** by Charles V. Peña (October 30, 2003)

495. **The Struggle for School Choice Policy after *Zelman*: Regulations vs. the Free Market** by H. Lillian Omand (October 29, 2003)

494. **The Internet Tax Solution: Tax Competition, Not Tax Collusion** by Adam D. Thierer and Veronique de Rugy (October 23, 2003)

493. **Keeping the Poor Poor: The Dark Side of the Living Wage** by Carl F. Horowitz (October 21, 2003)

492. **Our History of Educational Freedom: What It Should Mean for Families Today** by Marie Gryphon and Emily A. Meyer (October 8, 2003)

491. **Threats to Financial Privacy and Tax Competition** by Richard W. Rahn and Veronique de Rugy (October 2, 2003)

490. **Defining Democracy Down: Explaining the Campaign to Repeal Term Limits** by Patrick Basham (September 24, 2003)

489. **EU Enlargement: Costs, Benefits, and Strategies for Central and Eastern European Countries** by Marian L. Tupy (September 18, 2003)

488. **War between the Generations: Federal Spending on the Elderly Set to Explode** by Chris Edwards and Tad DeHaven (September 16, 2003)

487. **The Balanced Budget Veto: A New Mechanism to Limit Federal Spending** by Anthony W. Hawks (September 4, 2003)

486. **What Does a Voucher Buy? A Closer Look at the Cost of Private Schools** by David F. Salisbury (August 28, 2003)

485. **Mending the U.S.–European Rift over the Middle East** by Leon T. Hadar August 20, 2003)

484. **Replacing the Scandal-Plagued Corporate Income Tax with a Cash-Flow Tax** by Chris Edwards (August 14, 2003)

483. **Casualties of War: Transatlantic Relations and the Future of NATO in the Wake of the Second Gulf War** by Christopher Layne (August 13, 2003)

482. **Property Rights: The Key to Economic Development** by Gerald P. O'Driscoll Jr. and Lee Hoskins (August 7, 2003)

481. **The Constitutional Case against "Free" Airtime** by Laurence H. Winer (August 6, 2003)

480. **Why Subsidize the Soapbox? The McCain Free Airtime Proposal and the Future of Broadcasting** by John Samples and Adam D. Thierer (August 6, 2003)

479. **The Uses and Abuses of Structured Finance** by Barbara T. Kavanagh (July 29, 2003)

478. **All the Players at the Table: A Multilateral Solution to the North Korean Nuclear Crisis** by Doug Bandow (June 26, 2003)

477. **After Victory: Toward a New Military Posture in the Persian Gulf** by Christopher Preble (June 10, 2003)

476. **A Grand Façade: How the Grand Jury Was Captured by Government** by W. Thomas Dillard, Stephen R. Johnson, and Timothy Lynch (May 13, 2003)

475. **Demonizing Drugmakers: The Political Assault on the Pharmaceutical Industry** by Doug Bandow (May 8, 2003)

474. **Bring the Troops Home: Ending the Obsolete Korean Commitment** by Doug Bandow (May 7, 2003)

473. **Welfare Reform: Less Than Meets the Eye** by Michael Tanner (April 1, 2003)

472. **Extremist, Nuclear Pakistan: An Emerging Threat?** by Subodh Atal (March 5, 2003)

471. **Should Congress Repeal Securities Class Action Reform?** by Adam C. Pritchard (February 27, 2003)

470. **Empire of the Sun: An Economic Interpretation of Enron's Energy Business** by Christopher L. Culp and Steve H. Hanke (February 20, 2003)

469. **Accounting at Energy Firms after Enron: Is the "Cure" Worse Than the "Disease"?** by Richard Bassett and Mark Storrie (February 12, 2003)

468. **Cigarette Taxes, Black Markets, and Crime: Lessons from New York's 50-Year Losing Battle** by Patrick Fleenor (February 6, 2003)

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission.

Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001 or call toll free 1-800-767-1241 (8:30 a.m.-4:30 p.m. eastern time). Fax (202) 842-3490 • www.cato.org

CATO INSTITUTE