Assessing Threats to Privacy:

The Government Sector — Greatest Menace to Privacy By Far

A Special Report Issued by Privacilla.org
http://www.privacilla.org

September, 2000

Introduction

Governments are far and away the most voracious collectors, users, and sometime abusers of personal and private information. There is a long and growing list of both threats to privacy and privacy invasions committed by governments and their employees, including the U.S. federal government under the leadership of the Clinton/Gore Administration.

This is not surprising, however. The government sector has many incentives to collect, store, and use personal information. Few incentives cut the other direction or point them toward treating citizens' personal information with care. The U.S. government, although one of the best, operates in a legal environment that fails to protect privacy. It collects too much personal information about its people, keeps that information too long, and sometimes uses it to invade privacy, or worse.

Private sector businesses — which are also quite hungry for information — operate with a more balanced set of incentives. They are subject to both consumerist retaliation and legal action when they invade privacy. Nonetheless, conventional wisdom today holds strongly that business is the major threat to consumer privacy. This is not the case.

While threats from private businesses are not absent, the clearest menace to privacy today, yesterday, and tomorrow is the government sector. Governments collect information aggressively, they frustrate opportunities to protect privacy, and they possess massive databases that are sometimes very wrongly used, in terms of both privacy and civil liberties.

An important civic discussion of privacy is underway in the United States and throughout the world. Though much of it deals with information practices that have been evolving for years, the discussion has been hastened by the rapid growth of the Internet and digital communications technology. But the discussion should not happen at "Internet speed." Too many economic benefits and future innovations are at stake. The privacy debate should be carried out deliberately, by open minds, with an eye on real evidence.

In assessing threats to privacy, the evidence points directly at governments as the greatest menace. Political leaders and regulators who have proposed to protect privacy by clamping down on private sector information practices are truly throwing stones in glass houses. While there is some glass left, they should take a good look at their own reflections. The most plentiful and serious threats to privacy are of their own making.

Government Threats to Privacy

Threats to privacy from the government sector are legion. The United States government under the Clinton/Gore Administration has been no exception. Even an incomplete list shows the varied ways that governments frustrate individual privacy. The Federal Bureau of Investigation's Carnivore surveillance system is only the best known and most recent example.

Carnivore

"Carnivore" is a specialized computer developed by the FBI and equipped with software that can scan millions of e-mails per second. It attaches to the systems of Internet Service Providers (ISPs) and monitors their e-mail traffic.

This technology can be used to monitor the communications of legitimate crime suspects, or to fish through the e-mails of anyone using a particular ISP. The latter is the equivalent of police stopping and frisking everyone who enters a shopping mall or passes a particular city street corner. If the FBI has used Carnivore this way, it has violated the Fourth Amendment privacy rights of thousands of Internet users. Congressional hearings earlier this year revealed that the FBI had sought to attach Carnivore to the systems of EarthLink, a large, popular ISP.

Because the technology is so strong, and because the FBI has so far resisted any truly independent monitoring, there is no way to ensure that government investigators are using Carnivore only for legitimate purposes and within legitimate bounds. The FBI's small steps to reassure Congress and the public that Carnivore will not invade citizens' privacy are not enough. The Clinton/Gore Administration, which could shut Carnivore down overnight, has not done so. It has taken few steps, if any, to ensure that citizens' Fourth Amendment privacy rights are being protected from Carnivore.

The Carnivore system should be made subject to strict controls and independent monitoring if it is to be used at all. It represents only the most recent and technological threat to Americans' privacy.

"Know Your Customer"

Less technological, but no less outrageous was the proposal to invade Americans' financial privacy made in late 1998 by the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Reserve Board, and the Federal Deposit Insurance Corporation. They offered a plan to deputize the nation's financial institutions into a system for monitoring every American's banking habits.

Their regulations would have required these institutions to:

- verify the identities of their customers;
- determine the sources of funds for each customer;
- create a profile of the "normal and expected" transactions of each customer;
- monitor each customer's account activity, measuring it against historical patterns; and
- report any transactions that appeared "suspicious" in light of those patterns.

This government surveillance scheme caused enormous public outrage because it so obviously threatened the privacy of citizens' personal financial information. Over 250,000 people wrote to regulators objecting to the proposal, and the pernicious "Know Your Customer" regulations were ultimately withdrawn.

They are not gone, however. The "Know Your Customer" regulations would only have formalized policies that are currently in place under the ironically named Bank Secrecy Act.

The Bank Secrecy Act authorizes the Treasury Department to require financial institutions to maintain records of personal financial transactions that have a "high degree of usefulness in criminal, tax and regulatory investigations and proceedings." It also authorizes the Treasury Department to require any financial institution to report any "suspicious transaction relevant to a possible violation of law or regulation." These reports, called "Suspicious Activity Reports" are filed with the Treasury Department's Financial Crimes Enforcement Network ("FinCEN").

This is done secretly — without the consent or knowledge of bank customers — any time a financial institution decides that a transaction is "suspicious." The reports are made available electronically to every U.S. Attorney's Office and to 59 law enforcement agencies, including the FBI, the Secret Service, and the Customs Service. A law enforcement agency does not have to suspect actual crime before it can access a report, and no court order, warrant, subpoena, or even written request is needed. Law enforcement agencies can, and allegedly do, download the entire harvest of new information from FinCEN whenever they want it.

National Individual Health IDs

So far, we have learned how the federal government threatens our online privacy and undermines our financial privacy. The third of the big three is medical privacy. There is no end to privacy threats from the government sector in this area. Without question, governments became the biggest consumers of extremely private information about individuals when they got in the business of health care.

Just to administer health care programs, the federal and state governments must collect the names, addresses, telephone numbers, genders, ages, income levels, medical conditions, medical histories, providers' names, and much more information about every single beneficiary.

The prospect of this much information centralized in one federal government database was evidently too much for the American people when they rejected the 1994 Clinton Health Care plan, which proposed a government-issued medical ID card on which all Americans' private medical information would be stored.

Unfortunately, a weakened version of the government-issued medical ID was slipped into law a few years later as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This law required the Secretary of Health and Human Services (HHS) to create a National Individual Health Identifier. The ugly specter of a national health database remains.

The National Individual Health ID could so easily be used in thousands of pernicious ways that the Secretary of HHS, recognizing the writing on the wall, has taken almost no steps to implement this requirement. A National Individual Health ID is the law of the land, however, and the U.S. federal government remains a significant threat to medical privacy.

Encryption

Threats to privacy do not just come from secret government snooping and data collection, however. The U.S. government has also taken steps to prevent Americans from protecting their privacy as they see fit using the best technological tools available.

Encryption is a way to encode computer files so that only someone with access to a secret "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 can be revealed when they use digital technology. Encryption is essential for protecting individual privacy in the digital age.

"Threats to privacy do not just come from secret government snooping and data collection. The U.S. government has taken steps to prevent Americans from protecting their privacy as they see fit using the best technological tools available."

Instead of viewing it as an empowering technology, however, the U.S. government has 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.

In the final analysis, encryption technology probably cannot be controlled. The Clinton/Gore Administration's policies against encryption technology have kept encryption from full use by law-abiding citizens and threatened their privacy, while doing little to prevent criminals from using encryption.

Anonymity and Pseudonymity

One of the most effective ways to protect privacy is to remain anonymous or to use a false name (pseudonymity). There are many legitimate reasons to refuse to be identified. Victims of stalking, for example, may want to hide their actions and whereabouts. Governments that believe in the privacy of their citizens should leave room for anonymity and pseudonymity.

The United States Postal Service does not believe in anonymity or pseudonymity, however. Its regulations of Commercial Mail Receiving Agencies (CMRAs) like Mail Boxes Etc. make it illegal to receive mail anonymously or under an assumed name.

The Postal Service's Domestic Mail Manual requires CMRAs to get two pieces of identification from customers and verify that they give accurate name information and the address where they actually reside or do business. CMRAs must forward this information to the postmaster and maintain copies of it on their premises.

What does this mean for someone who wants to be able to receive alimony checks, but keep a wide berth from an abusive former spouse? It means the spouse has several ways of getting to them, thanks to regulations that compromise privacy by requiring full disclosure of information to CMRAs and the Postal Service.

CALEA

Another way the federal government conscripts the private sector to threaten privacy is illustrated by the Communications Assistance for Law Enforcement Act (CALEA). Passed in 1994, CALEA requires telecommunications companies to modify their equipment, making it easier for government investigators to snoop on communications.

The original proposal for CALEA, made by the Federal Bureau of Investigation in 1992, was much broader. It would have required all communications services, including computer networks, to assist in government surveillance.

A consistent threat to privacy, wiretapping of suspected criminals by law enforcers can easily evolve into monitoring of the general public, which violates the Fourth Amendment privacy rights of law-abiding citizens.

The "Clipper Chip"

CALEA was not the first attempt by federal government snoops to mold the technology we use into surveillance equipment. It was only the most successful.

The "Clipper Chip" was a proposal in the early 1990s to require installation of cryptographic chips in computer and telecommunications equipment. These chips would provide a "back door" to allow surveillance by the government. Though its proponents attempted to assure the public that the Clipper Chip would only be used with proper legal authorization, there was overwhelming public opposition to giving the government nearly ubiquitous surveillance capabilities. This obvious threat to privacy has now, thankfully, been abandoned.

L.A. Wiretapping Scandal

Speaking of wiretaps evolving into monitoring of the general public, there is the Los Angeles wiretapping scandal, which proved that the U.S. federal government is far from the only one threatening privacy.

In 1998, it came to light that the Los Angeles Police Department was extensively using illegal wiretaps to monitor citizens, collect evidence illegally, and invade the privacy of innocents. The police avoided revealing the existence of their electronic intercepts using a procedure known as "the handoff." Officers gathering information on one suspect would turn over information about other people to other detectives without identifying the source of the information. The other detectives would then gather facts independently to provide the "probable cause" needed to convince a judge to sign a search warrant targeting the new suspect. This could go on a long time without ever revealing the existence of the first wiretap.

This system may have persisted for many years in Los Angeles, resulting in many illegal arrests and convictions, and — just as importantly — causing many innocent citizens to be eavesdropped on by police. The number of illegal convictions may number in the hundreds, and the number of innocents who were illegally deprived of their Fourth Amendment privacy rights is unknown.

Echelon

And, of course, the United States is far from the only place where governments threaten privacy. Echelon, a project of the United States' National Security Agency (NSA), is a worldwide network for intercepting communications. It made headlines in February 1998 when a report from an arm of the European Parliament revealed that telephone, fax, and e-mail traffic in several parts of the world were routinely intercepted.

The NSA has many partners. In England, the Government Communications Headquarters (GCHQ) takes part. In Australia, it is the Defence Signals Directorate (DSD). In Canada, the Communications Security Establishment (CSE) is the Echelon affiliate, and in New Zealand the Government Communications Security Bureau (GCSB) does its part. Other countries involved with Echelon include Germany, Japan, Norway, South Korea, Turkey, China, and the Netherlands.

Communications outside the United States are not subject to the Fourth Amendment's privacy protections. Investigators can snoop on our international phone calls without technically violating our legal rights. Whether they violate our privacy is another question entirely, of course.

The IRS, the Social Security Administration, and the Census Bureau

Secret snooping is not the only way to threaten privacy. Government databases and collections of information are a threat to privacy in and of themselves because governments can change or ignore the privacy laws that apply to them. Even the United States government, one of the most solicitous of privacy and the rule of law in the world, has done this.

"Governments can change or ignore the privacy laws that apply to them. Even the United States government, one of the most solicitous of privacy and the rule of law in the world, has done this."

Just think of the massive quantities of personal information residing in government databases and archives today. Every year, when Americans file tax returns with the Internal Revenue Service (IRS), they must reveal a great deal of personal information, much of which is private or at least sensitive. 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 gifts. The list is very, very long because politicians are addicted to social engineering through tax policy. If anyone ever needed to compile a dossier on our behavior, the IRS would be a good place to start.

Indeed, Senate hearings on the IRS revealed in 1998 that some IRS agents had illegally searched through the tax records of their neighbors. Tax returns had been transported by ordinary bicycle couriers and treated without regard for the personal financial information they contained.

To perpetuate the myth that Social Security is something other than a tax Americans pay in the hope of a future entitlement, the Social Security Administration has begun mailing out notices that contain individuals' earning histories over their entire lives. Obviously, and necessarily, this government agency is keeping a more thorough

employment and earnings dossier on Americans than many Americans keep on themselves.

And then there is the census. The Constitution authorizes the federal government to "enumerate" persons in order to apportion congressional representatives among the states. To do this, the government needs only to know how many individuals reside at a given residence. This question is on the first page of the census.

The remaining questions in the census long form ask Americans about matters that have nothing remotely to do with apportioning electoral votes. It asks for a detailed breakdown of income, how people get to work, and so on. Census forms ask questions about employment, how many toilets families have, and how much they pay annually for electricity, gas, water, sewers, oil, coal, kerosene, and wood.

If asked these questions by a business or neighbor, most people would scoff and refuse to answer, defending their natural senses of privacy. Because the intrusive census questions are tied to questions that apportion representatives, most people answer out of a sense of duty. Responding to the census is not optional, however. The law requires it. The U.S. Census Bureau is a repository of massive amounts of sensitive personal information about Americans.

"If asked these questions by a business or neighbor, most people would scoff and refuse to answer, defending their natural senses of privacy."

Though there are statutes that protect the confidentiality of census information, those laws have been overstepped in the past. During World War II, the United States government used information gathered by the Census Bureau to round up American citizens of Japanese ancestry. Census Bureau employees opened their files and drew up detailed maps that showed where Japanese Americans were located and how many were living in given areas. Nearly 112,000 people were captured and sent to internment camps with the help of the census.

The American example pales in comparison to others. As is well known, during World War II, government authorities in Nazi Europe used public records in the course of perpetrating unspeakable acts on their residents. Those who view government databases as appropriate or even benign ignore history.

The government sector is indeed a major threat to privacy. Just in the past few years, we have seen multiple examples of this in the United States, which has a government relatively more protective of privacy than many. It collects massive quantities of personal financial and medical information on citizens, and treats it shabbily. It conscripts private businesses into collecting personal information on its behalf. It attaches snooping technologies to phone lines and Internet connections. And it

prevents encryption use, anonymity, and pseudonymity by law-abiding citizens. The United States government under the Clinton/Gore Administration has continued to be comprehensively anti-privacy. The government sector is the greatest menace to privacy by any measure.

Why the Government Sector Threatens Privacy

Given substantial evidence that the government sector is the premier threat to privacy, one must ask why it poses this threat. A two-part analysis makes the reasons fairly apparent. First, governments have many incentives to collect personal information and few incentives to protect privacy. Second, the laws that require the government to protect privacy in the United States are narrow and weak.

Incentives Predispose Governments to Invade Privacy

The government sector thrives on information about people. Personal information allows governments to collect taxes, serve entitlements and benefits up to their citizenry, and enforce laws and regulations.

Governments use personal information to collect taxes. Taxation requires massive collections of information without regard to whether it is private. The list of information required by tax laws is very, very long because the government sector is addicted to using taxation as a tool of social policy.

In the modern welfare state, governments use copious amounts of information to serve up various entitlements and benefits as well. Any program that doles money out to citizens based on their condition or status must know what that condition or status is, often in comparison to the condition or status of the population at large. A program to provide medical care, as an example, requires the government to collect the beneficiary's name, address, telephone number, sex, age, income level, medical condition, medical history, providers' names, and much more.

The Social Security number was created so citizens could receive government benefits. Its adoption as a standard personal identifier for many financial transactions has added to the list of information that people must guard as private.

A third use the government sector makes of personal information is to investigate crime and enforce laws and regulations. Governments' ability to do these things correlates directly to the amount of information they can collect about where people go, what they do, what they say, to whom they say it, what they own, what they think, and so on. We rely on government to investigate wrongdoing by examining information that is often regarded as private in the hands of the innocent. It is a serious and legitimate

concern of civil libertarians that government collects too much information about the innocent in order to reach the guilty.

All of the incentives governments have as institutions point them toward greater collection and use of personal information about citizens. This predisposes them to violate privacy. The erosion of privacy by governments is completely consistent with the large and growing welfare state, and the large and growing regulatory state.

Laws Are Insufficient to Protect Privacy From the Government Sector

The legal framework in which the government sector operates only weakly counteracts these incentives. This framework has two components. First, governments alone can take and use information under the authority of law. Second, the legal limits on government use of private information are self-imposed and unreliable. The privacy laws governments operate under provide insufficient protection for individual privacy from the government sector.

The fact that governments collect information using the force of law cannot be emphasized strongly enough. When a government agency or program needs personal information to carry out its mission, that information *will* be collected. Individuals have no choice in the matter. They may not opt out.

This does not just mean that individuals who refuse to give up their information will be fined, sent to jail, or lose their benefits. It means that government agencies and bureaucrats do not have incentives to be cautious with personal information in their files and databases. Whether they protect it or not, they can continue to collect more.

"When a government agency or program needs personal information to carry out its mission, that information *will* be collected. Individuals have no choice in the matter. They may not opt out."

In other words, personal information collected by law is cheap. Governments and bureaucrats act accordingly. They have no reason to be anything other than cavalier with the personal information that they hold. To governments, private information about citizens is easy-come easy-go.

The laws intended to counteract this and protect citizens' privacy are weak, spotty, and inflexible. The Fourth Amendment, which applies only to criminal suspects, has been eroded by Supreme Court decision in recent years. And we have seen investigators use technology to pry further and further into private communications using outdated legal standards. The Electronic Communications Privacy Act, for example, is what arguably allows the FBI to attach Carnivore to Internet Service Providers.

Massive amounts of personal information are collected for administrative purposes. The protections of the Fourth Amendment do not apply when the U.S. government collects this information.

The Privacy Act of 1974 is intended to provide individuals with broad protection from the unauthorized use of records that federal agencies maintain about them. It requires agencies to account for disclosures of records, and to take steps to minimize the quantity of records they hold, in addition to protecting their accuracy. It also gives individuals a right to gain access to records about them. Individuals may sue in federal District Court if their rights under the Privacy Act are violated, and there are criminal penalties for knowing and willful violations of the Act.

A recent General Accounting Office study commissioned by Senator and Vice Presidential candidate Joseph I. Lieberman (D-CT) revealed just how weak the Privacy Act is — and how weakly Office of Management and Budget dictates on privacy protection are followed. In a survey of online privacy protections at government-run Web sites, GAO found that 23 of the 70 agencies it surveyed had disclosed personal information gathered from Web sites to third parties, mostly other government agencies. At least four agencies had shared information with private entities.

The Privacy Act is an extremely long statute that is riddled with exceptions and caveats. Its laudable intentions have not limited government information collections in any significant sense. The Privacy Act would benefit from a revision that strengthens and clarifies its terms so the public can be confident that information will not be abused by federal agencies or bureaucrats.

Other laws protecting individual privacy from government include the Right to Financial Privacy Act, the Drivers Privacy Protection Act, the Privacy Protection Act of 1980, and the Family Education Rights and Privacy Act. Each of these laws was passed *ad hoc*, often in reaction to the privacy crisis or concern of the day. They do not provide protection from the next intrusion by government into privacy, which will assuredly happen in an area these statutes do not cover.

The statutes that attempt to protect the privacy of Americans from their information-hungry government are not up to the task. Every incentive the government sector has is to collect too much information about people, keep it too long, and fail to safeguard it. This is why governments — even the U.S. government, which is one of the most solicitous of privacy in the world — are the chief menace to privacy.

How the Privacy Playing Field for Business Compares

Though conventional wisdom today holds that private sector businesses are the primary threat to privacy, businesses operate in an environment that is much less conducive to invading the privacy of consumers.

Unlike governments, to whom information is cheap, businesses regard information as precious. They must treat information more carefully than the government sector does. And, unlike governments, businesses are subject to consumerist retaliation and tort lawsuits if they invade privacy.

Value of Information in the Private Sector Leads to Proper Incentives

Businesses do want information about their customers, and they work very hard to get it. This is because information has great value to them. Businesses use information to learn what customers want and need. They also use it to more efficiently offer products to customers through advertising. Accurate consumer information gives a business an advantage over its competitors, allowing it to create better products and make them known to customers more efficiently. For consumers, this means better products are delivered more cheaply when they want them.

The fact that information has this value leads us to important points about how businesses will treat personal information about consumers. Unlike the government sector, the business sector can be expected to safeguard consumer information that it holds. Certainly, businesses sell information — some businesses specialize in precisely that — but both the seller and the buyer have strong business reasons to protect the information they have acquired, hold it close, and keep it from disclosure.

Businesses also have a fundamental interest in protecting their relationships with customers. A business that loses information or unwittingly reveals personal information about consumers to others is wasting its own assets, driving down future revenues, and violating its duties to stockholders. This is undoubtedly why software companies issue patches so quickly when privacy flaws in their applications are revealed.

A business that offends consumers with its use of personal information spoils its relationship with them and wastes the value of information it has. For this reason, invasions of privacy under the law that has developed over the last 100 years are extremely rare.

Along with destroying the trust that businesses are constantly trying to develop with individual customers, careless or tactless use of personal information can bring adverse publicity, which threatens the public image of the business.

DoubleClick provides a good example of how this works. This online ad serving company caused a stir when it announced plans to combine click-stream information with personal information in the Abacus database it had acquired. DoubleClick had failed to explain the public benefits of the highly customized and targeted advertising it was preparing to deliver. Responding to public pressure, DoubleClick announced in March 2000 that it would not go forward with this custom-marketing plan. No click-stream information was ever combined with personally identifiable information, and no consumer's privacy was ever violated, but DoubleClick suffered substantial adverse publicity and harm to its share price.

In short, businesses take and hold consumer information with an obligation to treat that information carefully, with sensitivity and tact. Consumers and investors will penalize them heavily, taking dollars out of their bottom lines and market capitalizations, if they do not.

Tort Law Nests With Business Incentives to Protect Consumers

The incentives businesses have to safeguard consumer information nest with consumers' legal right to sue anyone who harms them by publicizing their personal information. Discussions of privacy too often ignore the law of torts, but there is a substantial body of common law that gives consumers the right to sue anyone who invades their privacy.

The most influential source of privacy as a part of American legal culture was an article written by Samuel D. Warren and Louis D. Brandeis called *The Right to Privacy* in the 1890 Harvard Law Review. In 1960, eminent legal scholar William L. Prosser documented how privacy as a legal concept had come to constitute four distinct torts. These torts still exist today, and are contoured as four separate branches:

1. Intrusion upon seclusion or solitude, or into private affairs;
2. Public disclosure of embarrassing private facts;
3. Publicity which places a person in a false light in the public eye; and
4. Appropriation of name or likeness.

A person whose privacy has been invaded can sue for damages.

The privacy torts do not create a world of perfect convenience and isolation for those who are especially sensitive. No law could allow people to enjoy the full benefits of our vibrant commercial society at the exact moments they want to, then withdraw from it at the moments they do not. Information does have value and, for people outside the mainstream, there may be high costs for declining to participate in the information economy. But, as the U.S. Department of Commerce reported in a July 2000 memorandum to the European Commission, "The right to recover damages for invasion of personal privacy is well established under U.S. common law."

Businesses do see information about consumers as a valuable commodity. They do work very hard to collect it. But, just as importantly, businesses have every incentive to treat that information carefully, use it tactfully, and reveal it only to those who treat it with similar care. This incentive system is backed up by consumers' right to sue invaders of privacy under established legal doctrines.

> "As the U.S. Department of Commerce reported in a July 2000 memorandum to the European Commission, 'The right to recover damages for invasion of personal privacy is well established under U.S. common law.'"

There is an unwritten ending to the story of business and privacy. Many privacy advocates today use the mere existence of large, detailed databases as a justification for establishing new privacy laws and regulations on the private sector. Traditionally, in the United States, information has flowed freely while only harmful uses of information have been punished. This has left room for the kind of innovation that we are only beginning to enjoy as we enter the Information Age. Whether a new paradigm will emerge, where information can only be used if law and regulations permit it, remains to be seen.

It would be deeply ironic if the government sector, which has the largest collections of personal information by far, and an unfortunate history of using them wrongly, were to restrict information flows in the private sector because private databases are the perceived threat. Instead of broad restrictions on freedom of information, any regulation of information practices in the private sector should meet discreet and identifiable harms directly.

Unlike governments, which have few incentives to safeguard personal information about citizens, businesses already have strong incentives to take care of consumer information. Where businesses are subject to lawsuits if they invade the privacy of consumers, governments are subject to a frayed patchwork of statutes that fail to protect privacy as often as not. The result is that the government sector represents the far larger menace to privacy than private-sector businesses.

Conclusion

The rapid growth of the Internet and digital communications has caused privacy to emerge as a public policy issue rather quickly. Responding to a perceived crisis — or perhaps a perceived political opportunity — some policymakers have rushed headlong into the issue, advocating policies that purport to protect privacy by clamping down on our innovative and highly productive private-sector information economy. These policymakers have failed to consider some of the most important facets of this complex

issue. Serious and thoughtful policies will protect the public from real, identifiable harms while allowing innovation and economic growth to continue.

Misconceptions about privacy abound. One of the most significant is that private-sector information practices pose the greatest threat to privacy. In fact, the government sector is home to the most voracious collectors, users, and sometime abusers of personal and private information about citizens.

The evidence for this is plentiful. Governments themselves collect tremendous amounts of information about their citizens. They conscript private industry to help collect personal information. They seek to require the private sector to modify technologies, enhancing the ability of investigators to snoop. And their regulations limit the ability of citizens to control their information and protect their privacy. The United States government under the Clinton/Gore Administration has been no exception to this rule.

Governments have overwhelming incentives to collect, store, and use personal information about their people. Few incentives keep them from over-collecting, overusing, and ultimately abusing the information they possess. The patchwork of statutes intended to protect the privacy of Americans from their government has insufficient coverage and strength.

By contrast, the private sector operates with a more balanced set of incentives. Businesses must treat information as a precious commodity. If they do not, they suffer in the marketplace. The private sector also operates under a legal system that protects consumers' privacy interests, as the U.S. Department of Commerce has confirmed.

The civic discussion of privacy now underway is a good thing. The modern age does pose new challenges to individual privacy. How people maintain control of information about themselves is one of those challenges, and anything that increases consumers' awareness of their role in protecting privacy is good.

Privacy debates today will help decide in coming years whether consumers will use their power in the marketplace to control how their personal information is used, or whether politicians and bureaucrats in the government sector will decide. Policymakers who truly want to advance the cause of privacy, and not some other value masquerading under the name, will look at the spending programs, regulatory agencies, privacy-invading regulations, and investigative agencies that they are responsible for. This is where they can do the most fruitful work on protecting privacy.

Given the proclivity of the government sector to collect massive amounts of personal information and use it to invade privacy or worse, governments should be regarded not as a major source of privacy protection, but as one of privacy's greatest threats.