Institute For Policy Innovation IPI

Synopsis: *While most of the debate about privacy has been focused on the private sector, because of government's unique powers, the issue of privacy from government is much more critical. Governments can take and use personal information, knock down doors, audit finances, break up families and throw people in jail. A bright line should separate our concerns about privacy from government and privacy in the private sector.*

Why Government is the Greater Threat to Privacy

by Jim Harper

Individuals enjoy privacy when they have the power to control information about themselves and when they have exercised that power consistent with their interests and values.

But while most of the debate about privacy has been focused on privacy with regard to private companies, government poses a much greater threat to privacy. In terms of privacy, the public sector and the private sector are worlds apart.

Because of governments' unique powers, the issue of privacy from government is of a much more critical nature than privacy from companies. Governments can invade privacy by taking and using personal information against the will of individuals. Private companies cannot get information from people who refuse to share it. Moving beyond privacy, governments can knock down doors, audit people's finances, break up families, and throw people in jail. A bright line should separate our contemplation of privacy from government and privacy in the private sector.

Different Powers, Different Incentives

Governments and businesses operate in entirely different legal environments and have entirely different incentives when they collect and use personal information.

Governments take and use information by force of law. They must be hemmed in by rules aimed at privacy (and related interests) because they lack the incentives to do so on their own. In the marketplace, on the other hand, good information practices are good business. Companies are in the business of pleasing their customers. Consumer dollars pressure companies toward privacy protection on the terms consumers want.

Governments:
Taking and Using Information by Law

When a federal agency like the Internal Revenue Service wants personal information, it has an easy option. It demands the information from taxpayers and businesses under penalty of law. Annual income tax forms and various information collections throughout the year are a treasure trove of information for the IRS. Governments take information by law, giving citizens no right to opt out.

And their information demands are substantial. Not only tax forms, but applications for licenses, permits, and benefits of all kinds come laden with requirements to hand over information. Employers, banks, and investment houses have been conscripted to collect information about Americans and turn it over to the government too, as required by law.

Governments can change how information may be used. When information is collected by governments with promises of confidentiality, those promises are not a contract but a naked assertion about an unpredictable future. Governments can make new uses of data they hold if a new law or regulation is passed—regardless of what they have promised. In many cases, U.S. federal agencies can make new uses and new disclosures of data merely by stating in the Federal Register that they are doing so.

When a government agency violates the rules about information, the penalties are minimal. An agency may suffer bad press if lax security leads to a privacy debacle, but its funding continues—or even increases to fix the problem. When U.S. federal agencies have tripped over the extremely low hurdles of the Privacy Act and suffered lawsuits, no capital has been at risk. Courts have minimized government payouts, but if they ever come due, they will be just another cost of governing, appropriated by Congress out of taxpayer dollars, and having no influence on the agency's bottom line.

Business:
Hemmed in by Markets and Law

For businesses, information practices can directly affect the balance sheet. Businesses have no legal power to take information from consumers. They must bargain for it, constantly seeking information from customers so that they can tailor their products and pitches to serve consumers better. If they demand too much customer information, they risk losing business, profit, and value for shareholders.

Businesses trade data among themselves, but the existence of markets for personal information does not prove that "people have no privacy." Rather, it shows that businesses value information. If they do not use it to benefit their customers, they are wasting an investment. Businesses do not succeed by abandoning customer information to their competitors or by maintaining poor security practices that allow information to leak out.

Likewise, private entities are swarmed by sanctions if they invade privacy or fail to adopt proper security procedures. Customers can simply choose to do business elsewhere if they find a company's information practices to be invasive or objectionable. Anyone that publicizes private embarrassing information can be sued under state common law. A company that collects, uses, or shares personal information in violation of its privacy policy or other contractual promises can be sued for damages by individuals. It can also be charged with deception by the Federal Trade Commission and state attorneys general. Just the hint of unpopular information practices—even a security mistake that raises privacy questions—can hurt a company's reputation, sully its brand name, and drive new and existing customers away. All these threats go directly to the bottom line.

Good information practices are good business. Winning businesses collect and use information aggressively to benefit consumers, while striving to avoid privacy problems. Governments, meanwhile, are relatively indifferent to privacy. They lumber forward whether or not their actions are in tune with the privacy preferences of citizens.

The Results: Privacy-Invasive Government, Privacy-Protective Business

Because they face different legal regimes and different incentive structures, governments and businesses treat personal information differently. The rapid advance of the Information Age has certainly exposed and created flaws in corporate information practices, but governments are and will be the greater, more persistent threat to privacy and related interests.

Governments:
Demanding, Careless, Expanding and Abusive

Not surprisingly, government agencies make many demands for personal information, have notoriously lax security, and are constantly building, growing, and

combining databases of personal information. Governments have used information abusively both historically and in the recent past.

Government demands for information and new uses of information are constant. As discussed above, each program and agency that serves or acts on people demands information about them to do so. Once government agencies have that information, they redeploy it constantly. The Federal Register contains announcements every day of new "routine uses" that U.S. federal agencies are making of Americans' personal information.

Lax security practices threaten the privacy of information held by governments. The Veterans Administration's computer system provides a premier example. The VA has reams of highly personal medical information about thousands of American servicemen and women, and their families. In late 2000, congressional hearings and inquiries revealed that hackers could access all of the information without the VA even knowing it. Its own employees sued it for Privacy Act violations.

Government demands for information continue unabated. Federal data mining programs such as the Total Information Awareness program at the Department of Defense and CAPPS II at the Transportation Security Administration are just two examples of federal agencies' headlong, legally privileged foray into maximum nonconsensual use of Americans' personal data. Officially discontinued, these programs have reincarnated themselves behind the secrecy wall (TIA) and have been repackaged as "trusted traveler" programs.

Over the long run, government abuses of personal information are routine. In World War II, the federal government used census data to round up and intern Americans of Japanese ancestry. In the 70's, the Church Committee found that the FBI had used electronic surveillance on Dr. Martin Luther King, Jr., Congressman Harold Cooley, dissident groups, and many others. IRS agents have routinely browsed files to learn personal information about ex-spouses, neighbors, and even movie stars. Until 1998, there was no law against "browsing" by IRS employees, and the technical rules against it were poorly enforced.

And if the U.S. government, which is at least accountable in some way to its citizens, has so much potential to abuse privacy, imagine the even greater potential of foreign governments to abuse the privacy of U.S. citizens. Yet that is exactly what European governments, the Organization for Economic Cooperation and Development, and some American politicians push in their attempt to rid the world of "tax havens." Free exchange among governments (including many undemocratic governments) of tax, banking, credit card and other information on individuals throughout the world would be devastating for privacy and liberty.

Business:
Hungry, Careful, Responsive, and Sensitive

Like governments, businesses are hungry for personal information, and they are far from perfect in their information husbandry. But, as discussed above, they cannot get their fill just by demanding it. They have to coax it from consumers or buy it from each other. When they have it, they must protect it like any other property.

Privacy and, more often, security breaches do occur, but millions of transactions occur daily with no breach of privacy or security. If contentedness were newsworthy, there would be story after story of consumers being satisfied by beneficial uses of information about them.

Businesses are extremely responsive when privacy concerns are raised. At the outset of the modern privacy debate, online advertising company DoubleClick famously announced a plan to combine online and offline consumer information. It was swarmed with adverse public reaction and determined not to implement the plan. Radio Frequency Identification tags (RFID) were the source of much privacy concern for a period when retailers proposed to use them for tracking merchandise in stores. But they have not seen mass adoption because the benefits did not match the costs, including privacy costs to consumers, perceived or real. There are lessons here when anti-commercial activists tout the latest technology or business practice as the death of privacy.

Companies today are constantly following public debate and comparing notes to be sure that their information practices fit into the mainstream. Time and again, companies quietly turn away from privacy practices that they recognize as raising consumer hacklers. A single privacy mistake—even a security mistake that raises privacy questions—can hurt a company's reputation, sully its brand name, and drive new and existing customers away.

Conclusion

Between government and the private sector, government is the clearest threat to privacy. Governments have the power to take information from people and use it in ways that are objectionable or harmful. This is a power that no business has: People can always turn away from businesses that do not satisfy their demands for privacy.

Privacy advocates and concerned citizens should be far more concerned about governments as potential abusers of privacy.

About the Author

As director of information policy studies at the Cato Institute, Jim Harper works to adapt law and policy to the unique problems of the information age in areas such as privacy, telecommunications, intellectual property, and security. Harper was a founding member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee and he recently co-edited the book *Terrorizing Ourselves: How U.S. Counterterrorism Policy Is Failing and How to Fix It*. He has been cited and quoted by numerous print, Internet, and television media outlets, and his scholarly articles have appeared in the Administrative Law Review, the Minnesota Law Review, and the Hastings Constitutional Law Quarterly. Harper wrote the book *Identity Crisis: How Identification Is Overused and Misunderstood*. Harper maintains online federal spending resource WashingtonWatch.com. He holds a J.D. from University of California Hastings College of Law.

About the Insitute for Policy Innovation

The Institute for Policy Innovation (IPI) is a nonprofit, non-partisan educational organization founded in 1987. IPI's purposes are to conduct research, aid development, and widely promote innovative and nonpartisan solutions to today's public policy problems. IPI's focus is on developing new approaches to governing that harness the strengths of individual choice, limited government, and free markets.

IPI is a public foundation, and is supported wholly by contributions from individuals, businesses, and other non-profit foundations.

Direct all inquires to: Institute for Policy Innovation,
1660 S. Stemmons Freeway,Suite 245
Lewisville, TX 75067
972.874.5139
email: ipi@ipi.org
www.ipi.org