

Privacy

GLOSSARY

Carnivore

The code name of a software program developed for the FBI to monitor e-mail and other Internet traffic; it is installed on the premises of an Internet service provider.

Cookie

A record of a visit to a Web site; by itself, a cookie cannot identify the visitor.

Hotmail

A free Internet e-mail service owned by Microsoft. Hotmail does not check the validity of registrant identities, thus one may obtain an e-mail address without revealing one's true identity. Other companies, including Yahoo, offer similar, free e-mail accounts.

Magic Lantern

The code name of a virus-like software program developed for the FBI to capture the user's keystrokes as they are typed, defeating any encryption program the user relies on to protect the privacy of e-mail and other electronic communications; it can be surreptitiously installed, via e-mail or other means, on a user's computer.

Privacy

The state of being free from unsanctioned intrusion.

Screen saver

A computer program designed to prolong the useful life of computer monitors; many are offered free over the Internet.

BACKGROUND

For Americans, individual liberty includes a right to personal privacy, as manifested in the Fourth Amendment to the U.S. Constitution. The amendment was written in an age—long before the advent of computer databases and digital communications—when an invasion of privacy perforce was a physical, manual, focused, short-term, expensive, and relatively obtrusive act that might involve entering premises, intercepting and opening mail, questioning acquaintances, and, later, tapping a telephone line or taking photographs—all without the subject's permission or knowledge.

Today's invasion of privacy is more likely to be virtual, automated, unobtrusive, inexpensive, and lifelong. Others can find out what we buy and from whom, what we say and to whom, what we read, what turns us on, what turns us off, what ails us, where we go, and even whether we exceed the speed limit in getting there. Not only has the secluded and shuttered 18th century home held inviolable by the Fourth Amendment been replaced by a 21st century glass house, but technology also has given Peeping Tom much more powerful binoculars.

DISCUSSION

Michigan's first public act of the new millennium, P.A. 1 of 2000, was privacy legislation, and the state attorney general's office reports that Internet privacy is one of the main consumer concerns. But legislation may not be enough to halt the erosion of privacy in the Internet age. Human ingenuity, greed, and carelessness can overcome the best-intentioned legislation, and in the shrinking, borderless world of the Internet, state and local legislation can conflict with federal law, other nations' laws, and a growing body of international law.

Two key questions are emerging:

- Is privacy—among other democratically derived civil liberties—compatible with the privatization of America's critical information infrastructure and its governing functions?
- Does the rapid evolution of technology, relative to the necessary slowness of deliberative democracy, put privacy legislation in perpetual catch-up mode and thus render it ultimately ineffectual?

The view often is expressed that increasing our computer defenses should not come at the expense of civil liberties, that the very freedoms we seek to protect should not be undermined. Some point out that technology empowers both law enforcers and law-breakers, and the latter cannot be stopped without impinging on personal privacy at least to some extent. Others say that lost in all the rhetoric is consideration of who has the right to own and control a citizen's private information.

But perhaps the bigger challenge is whether technology's rapid evolution renders privacy moot. For example, while a good deal of attention currently is being paid to the intrusive activities of large corporations, we may be overlooking smaller "spyware" operators and their hidden programs, sometimes bundled (unknown to the recipient) with

PRIVACY

screen savers and other free computer programs. Much more intrusive than passive “cookies,” spyware actively can track the Web sites and pages a user accesses, create a profile of the user’s interests, deliver tailored pop-up ads, and even collect the personal and financial information people submit when they use the Internet to order goods or subscribe to services. In some cases, spyware operators hide behind essentially anonymous e-mail addresses (such as provided by Hotmail, Yahoo, and others) or a P.O. box number and may operate abroad as well. It is questionable whether legislation can protect Internet privacy at all, given the absence of borders on the Internet and the rapid evolution of spyware.

Substantial legislative activity, nationally and in Michigan, reflects public concerns about Internet, medical, financial, and genetic privacy. Exhibit 1 summarizes major privacy-related legislation enacted or introduced in Michigan since 1999. The fundamental issues underlying the concerns include ownership and control of personal data, national security, the expansion of personal data down to the genetic level, and identity theft.

We can distinguish between two principal privacy intruders: the private sector and the government. Private parties may seek to intrude not only for institutional security (e.g., monitoring employee e-mail) but also for sales, marketing, and promotional purposes. Intrusion of privacy by government is confined largely to record keeping and security concerns and bound by Constitutional guarantees to a standard of accountability higher than that which binds private parties.

Private-Sector Intrusion

Opt In versus Opt Out

Since we cannot survive in modern society without sometimes sharing our financial, medical, and other private information with strangers, the central issue becomes one of ownership and control: Who owns our private information, and should it be used by others with—or without—our explicit permission?

Many commercial Web site owners and advertisers that collect personal data from us use it for marketing or other purposes *unless* we take the initiative to ask that it not be so used; in other words, unless we specifically *opt out*. Businesses have been criticized and sued for not always making it clear that this is their policy and/or for making it difficult or tedious for customers to opt out. Under pressure from consumer groups and sometimes the threat of prosecution, some companies have switched to a policy of not using customer information for purposes other than the transaction at hand unless customers take the initia-

tive to authorize such use; in other words, unless they specifically *opt in*.

The Pew Internet and American Life Project finds that 86 percent of Internet users support an opt-in standard in regard to collection of personal information, which is at odds with the opt-out alternative favored by industry groups and endorsed by the Federal Trade Commission (FTC). The issue extends to telephone-user privacy: Telecommunication companies now are seeking permission to sell “customer proprietary network information,” which includes names, addresses, calling records, and service options used. Consumer groups, citing the Pew data, are urging the FTC to insist on an opt-in standard for this proposal. In a case involving similar circumstances, however, a federal judge ruled that there was inadequate evidence that an opt-in standard would protect customer privacy interests, thus, in that instance it violated the First Amendment.

What happens when the stranger to whom you have entrusted personal information gets married and endows to the spouse all his/her worldly goods—including your data? The 1999 federal Gramm-Leach-Bliley Act allows banks, insurance companies, and brokerage companies to merge or affiliate and share consumers’ personal information with one another. Supporters focus on the business efficiencies the act was intended to encourage. The act also requires financial institutions to offer individuals notice and an opportunity to opt out before selling their name, address, or Social Security number to an outside entity, but critics complain that most opt-out notices are not written in the plain language stipulated in the act and warn consumers to look carefully at the privacy notices.

The federal law does not extend the customer-notice provision to the insurance industry, however, and this led to P.A. 24 of 2001, which prohibits Michigan insurers from disclosing a customer’s personal financial information to a third party unless the customer is notified and does not opt out. As with the federal mandate, the problem remains that people must read the fine print in notices, which, with all the appearance of being a solicitation, may be discarded unread.

Government Lists

Until 2000, private individuals, companies, and organizations could buy certain State of Michigan lists, but P.A. 192 of 2000 now prohibits the secretary of state from selling such information as driver’s license and other agency records for the purpose of “surveys, marketing, or solicitations.” (The act does not prohibit the sale of the lists for such other purposes as “motor-vehicle market-research activities,” however.)

EXHIBIT I. Selected Privacy-Related Legislation, Michigan, 1999–April 1, 2002

<i>Act or Bill and Year of Enactment or Introduction</i>	<i>Legislation Summary</i>
<i>Medical Genetic Privacy</i>	
P.A.s 26–28 (2000)	Prohibits insurers from using genetic tests for the purpose of denying coverage application or renewal.
P.A. 29 (2000)	Prohibits a genetic test from being ordered without the written, informed consent of the test subject.
P.A. 30 (2000)	Provides that if the State Police forensic laboratory determines after analysis that a sample has been submitted by an individual who has been eliminated as a suspect in the crime, the laboratory must dispose of the sample.
P.A. 31 (2000)	Specifies the destruction of genetic testing material following a court-ordered paternity test.
P.A. 33 (2000)	Provides for the retention and disposal of blood specimens taken from a newborn for the screening tests required by the act.
P.A. 32 (2000)	Prohibits an employer from requiring an individual to submit to a genetic test as a condition of employment or promotion.
P.A.s 86, 88–89, 91 (2001) HBs 4609–14, 4633 (2001)	The acts require DNA samples to be collected and maintained in certain felony crimes. The bills would extend the law to cover all felonies plus a number of misdemeanors and ordinance violations; included are fourth-degree criminal sexual conduct, enticing a child for immoral purposes, indecent exposure, window peeping, and various prostitution-related offenses. For juveniles, the requirements would apply to assault with intent to commit murder, manslaughter, and certain misdemeanor and ordinance violations. Collection would be required on conviction or, in the case of incarcerated offenders who had not previously been tested, prior to release.
HB 4936 (2001)	Would prohibit disclosure of individual patient health care information (except that specifically allowed by federal or state law, rule, regulation, or Medicaid policy) without the patient's (or authorized representative's) written consent. Separate written consent would be required for disclosure of genetic information.
<i>Workplace/Employee Privacy</i>	
HB 5481 (2001)	Would prohibit disclosure of public school employee records to for-profit businesses for the purpose of soliciting business from the employees.
HB 5527 (2001)	Would prohibit employer monitoring of employee communications unless the employer establishes an employee-monitoring policy and discloses the policy to employees.
<i>Identity Theft</i>	
P.A. 1 (2000)	Prohibits state and local government agencies from printing or writing Social Security, drivers license, or state identification numbers in such a way that they might be seen on or through envelopes or packages.
SB 955 (2001)	Would increase penalties for reproducing, altering, counterfeiting, forging, or duplicating a license photograph.
<i>Telemarketing</i>	
HB 4042 (2001)	Would require the Public Service Commission to establish or designate a do-not-call list and prohibit telephone solicitations to residential telephone subscribers on the list.
HB 4631 (2001)	Would require a residential telephone directory to include information about how a consumer may be included on the do-not-call list.
<i>Financial Privacy</i>	
P.A. 24 (2001)	Prohibits Michigan insurers from disclosing a customer's personal financial information to a third party unless the customer is notified and does not opt out.



PRIVACY

<i>Wiretap</i>	
SB 497 (1999)	Would permit prosecutors to authorize, and judges to approve, applications by state and local law enforcement agencies to intercept communications if other investigative techniques have failed, are reasonably unlikely to succeed, or are too dangerous.
HB 5240 (2001)	Would authorize certain communication interceptions, the use of interception devices for certain offenses, and provide for and regulate the application, issuance, and execution of interception orders.
<i>Consumer Privacy</i>	
P.A. 192 (2000)	Amended P.A. 300 of 1949 to prohibit the sale by the Secretary of State of driver's license and other lists for purposes of "surveys, marketing, and solicitation."
SB 433 (2001)	Would allow the state to enter into a multistate sales and use tax agreement by which sales and use taxes on out-of-state purchases made via the Internet, telephone, and mail would be collected. Private-sector certified service providers (CSPs) would be contracted with to collect the taxes and distribute the revenue. The CSPs would be prohibited from retaining or disclosing personally identifying information except where a consumer claims exemption from tax liability; in such a case the consumer usually would have to be notified of that retention and afforded access to his/her own data, with a right to correct inaccuracies.
<i>Internet Privacy</i>	
HB 4680 (2001)	Would prohibit Internet service providers from (1) keeping any records of customers' browsing patterns or selling or distributing such information without first obtaining written permission or (2) divulging a customer's e-mail messages without the customer's written authorization. The bill also would prohibit a person or any other legal entity from placing an individual's "personal nonpublic information" (i.e., telephone or Social Security number, home/business/e-mail addresses, or medical information that the person has not given written authorization to disclose) on the Internet or otherwise distributing or using such information with the intent to cause the individual physical or financial harm.

SOURCE: Summarized from legislative texts and analyses available on the Michigan Legislature Web site www.michiganlegislature.org/mileg.asp?page=Bills

State facility and profession/occupation licensing and registration information is provided on the Michigan Department of Consumer and Industry Services Web site. Although presented to enable consumers to find service providers and check their credentials, the information may be used for whatever purpose the seeker wishes to put it, including telemarketing and other forms of solicitation.

Government Intrusion

National ID Card

Many people are concerned about direct government intrusion of privacy, and in particular over a move toward a national identification card, an idea made at least thinkable by the September 11, 2001, terrorist attacks. Michigan and federal legislation aiming to establish standardized medical records (see below) also evokes such fears. Databases, whether government, commercial, or both, could be integrated much more efficiently and cost effectively if everyone had a unique national identifier, but such databases carry the risk of being all-revealing to any person or institution that gains access to them. Some seek to overturn current law prohibiting the use of the Social Security number as a national identifier; others seek a new and unique identifier for specific purposes, such as an electronic medical record.

A related proposal would have every individual retaining some control over his/her personal data by storing it on an electronic "smart card." Several European and Asian countries have implemented limited smart card systems containing one's national identity number, driver's license information, and medical records.

National Security

Even before September 11 the need to protect defense, economic, and other key national information and transaction systems (including private-sector systems judged critical to national defense or the economy) from intruders and saboteurs was the basis of additional and strengthened government "cyber-security" measures that have significant privacy implications.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, enacted after the September 11 attacks, significantly expanded government surveillance authority, reduced judicial oversight, and criminalized as terrorism a wide range of activities, including computer hacking.

The act includes a sunset (expiration) date (December 31, 2005) on the enhanced electronic-surveillance provisions and an amendment providing judicial oversight of

law enforcement's use of the FBI's Carnivore computer system. The latter enables the agency to eavesdrop on electronic communications, including e-mail. Nevertheless, the act vastly expands government investigative authority, especially with respect to the Internet. Exhibit 2 summarizes a selection of the expanded federal government powers.

Michigan's anti-terrorism package (P.A.s 112–137 and 140–143 of 2002) includes state-authorized wiretapping, a definition for terrorism in state criminal law, authority to seal affidavits used in issuing search warrants, and authority to search premises without notifying the resident. Objections to the laws center on their privacy-intrusive aspects, but proponents contend that the legislation not only combats terrorism but also strengthens state law enforcement officials' hand in investigating crimes involving drugs, gambling, racketeering, money laundering, computer-related crimes against children, and more.

Genetic Profiling

Since completion of the Human Genome Project, genetic profiling has taken center stage as the technology with the most immediate and substantial implications for privacy. In Michigan, for example, P.A. 250 of 1990 (DNA Identification Profiling System Act) requires a DNA sample from all felons and people convicted of certain sex-related misdemeanors, permitting investigators to compare DNA strands in hair, tissue, or bodily fluids found at a crime scene with the DNA of those previously convicted of a crime in Michigan. (Eight other states and the United Kingdom have similar laws.) Opponents say that there are scientific concerns about the reliability and validity of DNA tests and that the next step may be to collect DNA samples from anyone accused of a crime and, ultimately, from everyone. Supporters point out that DNA evidence is as important in protecting innocent people as it is in implicating the guilty and that the DNA database will be an invaluable investigation tool.

Medical Records

The 1996 federal Health Insurance Portability and Accountability Act (HIPAA) requires health care providers, health plans, and clearinghouses to adopt and use common data formats for sharing patient clinical and billing information electronically. The legislation includes strong privacy and data-security rules to which the industry must adhere by April 2004. The privacy rules require covered organizations to secure patient opt-in before releasing information to another entity, except in emergencies, and the information released has to be the minimum necessary to accomplish its purpose. Information that has been "de-identified" by removing name, address, and various other potential identifiers may be freely distributed. Pa-

EXHIBIT 2. Federal Government Powers Expanded by the USA PATRIOT Act, Selected Examples

Computer fraud

Government may wiretap anyone suspected of causing more than \$5,000 worth of combined damage via a computer used in interstate commerce.

Definitions of terrorism

New and expanded definitions expose more people to electronic surveillance (and potential "harboring" and "material support" liability).

DNA database

Government may collect DNA samples not just from terrorists but from any violent criminal.

Hackers

Government may spy on suspected computer trespassers without a court order.

Intelligence sharing

Allows U.S. foreign intelligence agencies to share their findings with the FBI, thus circumventing limitations on domestic surveillance.

Internet surveillance

Government may spy on American Web surfers' activities, including the terms they enter into a search engine, on the basis that the surveillance may produce information relevant to an ongoing criminal investigation.

ISP customer information

Internet service providers may voluntarily hand over to law enforcement agencies all "non-content" information about their customers—i.e., a court order or subpoena is not needed. Government may now subpoena ISP records of users' session times and duration, temporarily assigned network (I.P.) addresses, and means and source of payments, including credit card or bank account numbers.

SOURCE: Selected and summarized from an Electronic Frontier Foundation analysis, available at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html

tients have the right to access and request changes to their health records. Supporters say the shared information will improve health care and reduce administrative costs, and they believe the privacy provisions are adequate. Opponents generally focus on the cost and complexity of implementing the requirements, but some fear that the privacy provisions may prove to be less adequate than thought, at the expense of patient privacy.

In Michigan, pending legislation (HB 4936) also aims to establish all Michigan residents' rights to medical privacy and to access their own medical information. All health care providers—not just physicians and hospitals/clinics, as is the case now—would be required to maintain the

PRIVACY

confidentiality of patients' medical records. The legislation complements HIPAA and would prohibit unauthorized disclosure, sale, or transfer of any information in any patient record, including electronic records stored on a computer, without first obtaining the written consent of the patient and would further require that any information disclosed be used only for the expressed purpose agreed to by the patient. The draft legislation has so far attracted little in the way of public debate.

Criminal Intrusion

ID Theft/Use

Identity theft occurs when someone uses someone else's identity (e.g., name, date of birth, Social Security number, driver's license number) to masquerade as that person. In the 18 months preceding the end of 2001, in metropolitan Detroit alone, the identity of some 3,000 residents was stolen and used for obtaining credit and other purposes. The high-tech crime unit of the Michigan Department of the Attorney General, working with federal, state, and local law-enforcement agencies, has taken action against counterfeit credit-card and check operations, and SB 955 would toughen penalties for forging driver's licenses, a common practice of identity thieves.

The federal government has mandated that states must collect Social Security numbers from motorists applying for or renewing a driver's license, and the Michigan secretary of state is preparing to comply. The federal intent is to help states track parents who are delinquent in making child-support payments. In Michigan, only about one parent in three pays required child support, and the total amount owed but not paid exceeds \$7 billion. Supporters say collecting drivers' Social Security numbers will facilitate finding "deadbeat" parents and thereby help their children. Opponents argue that it is a step down the slippery slope toward creating a national identity system and an identity-theft risk as well.

Other

Space precludes a full discussion here of all the areas in which privacy is an issue. (See Exhibit 1 for a sampling of

other areas.) The debate about privacy is intense and, as set out with regard to the matters discussed above, generally focuses, on the one hand, on providing efficiency and better tools to accomplish a purpose and, on the other hand, protecting individuals' private information from the consequences of its use by others.

See also Civil Rights and Liberties; Consumer Protection; Crime and Corrections; Emergency Preparedness and Response.

FOR ADDITIONAL INFORMATION

Electronic Frontier Foundation
454 Shotwell Street
San Francisco CA 94110
(415) 436-9333
(415) 436-9993 FAX
www.eff.org

Electronic Privacy Information Center
1718 Connecticut Avenue, N.W., Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 FAX
www.epic.org

Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554
(888) 225-5322
(202) 418-0232 FAX
www.fcc.gov

Federal Trade Commission
CRC-240
Washington, D.C. 20580
(877) 382-4357
www.ftc.gov

Michigan Legislature
www.michiganlegislature.org
[Contains detailed and searchable records of Michigan laws and legislative activity]