

Privacy Today: A Review of Current Issues

Used with the permission of the Privacy Rights Clearinghouse
www.privacyrights.org

Contents:

1. [Biometrics Technologies](#)
 - a. [Biometric Encryption](#)
 2. [Video Surveillance](#)
 3. [Online Privacy and E-commerce](#)
 4. [Workplace Monitoring](#)
 5. [Wireless Communications and Location Tracking](#)
 6. [Data Profiling](#)
 7. [Criminal Identity Theft](#)
 8. [Background Checks](#)
 9. [Information Broker Industry](#)
 10. [Public Records on the Internet](#)
 11. [Financial Privacy](#)
 12. [Medical Records Confidentiality](#)
 - a. [Genetic Privacy](#)
 13. [Wiretapping and Electronic Communications](#)
 14. [Youth Privacy Issues](#)
 15. [Digital Rights Management](#)
 16. [Digital Television and Broadband Cable TV](#)
 17. [Radio Frequency Identification \(RFID\)](#)
 18. [Real ID](#)
 19. [Absence of Federal-Level Privacy Protection Law](#)
 20. [Behavioral Targeting](#)
 21. [Cloud Computing](#)
- [Appendix: Nonprofit public interest groups working on these issues](#)

The purpose of this report is to highlight and summarize key privacy issues affecting consumers today and tomorrow. Readers who want to explore issues in depth should visit the Web sites of government agencies, public interest groups, industry associations, and companies. A list of public interest groups that are working on these issues is provided at the end of the report.

1. BIOMETRICS TECHNOLOGIES

Description of issue. The secret video surveillance of the thousands of football fans who attended the 2001 Superbowl in Tampa, Florida was the first time that many Americans learned of something called "facial recognition biometrics." The technology used was not the common form of video monitoring that we are familiar with in convenience stores, at shopping malls, and on city streets. These systems do not have the capability to *identify* individuals whose faces are captured on videotape.

In contrast, the system used at the Superbowl and in the restaurant/bar district where many of the revelers gathered was able to *identify* known criminals and suspected terrorists from among the tens of thousands of faces scanned by the cameras using a biometrics technology called facial recognition biometrics.

Privacy and civil liberties advocates were quick to decry the use of this technology by the Tampa Police Department. It is not difficult to envision how such systems could be used to identify, for example, individuals who participate in public demonstrations against unpopular government actions. The "chilling effect" on individuals would be a likely result.

Biometrics is the term used for the many ways that we humans can be identified by unique aspects of our bodies. Fingerprints are the most commonly known biometric identifier. Other biometric identifiers are hand prints, vein dimensions, our iris designs, blood vessels on our retinas, body odor, the way that we walk, and our voices, among others. Our genetic profile is also unique to each of us. In facial recognition biometrics, the geometry of the face is measured.

The biometrics industry is booming, especially since the terrorist attacks of September 11, 2001.

- Several airports in the U.S. and other countries have since installed facial recognition biometrics systems to identify individuals on law enforcement agencies' "most-wanted" lists.
- Biometrics technologies are seen by the financial services industries as a way to deter fraud and identify fraudsters.
- Many casinos now use facial recognition biometrics systems to identify known card-counters and cheaters and expel them from their facilities.
- Various biometrics systems are being employed to provide secure access to computer systems, for example in health care institutions.
- Many national governments, including the U.S., use biometrics to speed border crossings and customs entry for frequent travelers.
- Some states and counties use fingerprinting to prevent welfare fraud.

Looking ahead. Privacy and civil liberties advocates are gravely concerned about the widespread adoption of biometrics systems. I have already discussed the chilling effect that a facial recognition system could have on our First Amendment right to protest government actions in public demonstrations. Such systems could easily be used to develop a database of known dissidents, to be used for social control purposes.

If one biometrics system were widely adopted, say fingerprinting, the many databases containing the digitized versions of the prints could be combined. While such a system is most likely to be developed by the commercial sector for use in financial transactions, government and law enforcement authorities would likely want to take advantage of these massive databases for other purposes, especially if we were to enter a time of social unrest. Indeed, government agencies and law enforcement are the top subscribers to the many databases compiled by private sector information brokers. I will return to the topic of information brokers later.

Privacy and civil liberties advocates have become more vocal about the threats of untrammelled and unregulated uses of biometrics technologies since the aftermath of the 9-11 terrorist attacks. Of the many biometrics technologies that are being developed, facial recognition biometrics is one of the most threatening because it can be deployed secretly, and can be invisible to those surveilled. Further, tests have found that the error rates for facial biometrics technologies are high. As a result, innocent people can be wrongly identified as criminals (false-positives), and known criminals and suspected terrorists can fail to be detected altogether (false-negatives).

Unless law enforcement and other government users establish guidelines and strict oversight of such systems, many innocent individuals are likely to be apprehended. There must be limits on the kinds of uses that can be made of biometrics technologies by government and law enforcement authorities, as well as clear-cut and expeditious procedures to handle cases of erroneous identification.

a. BIOMETRIC ENCRYPTION

Description of issue. Biometrics are now being used deployed in a wide range of public and private sector applications such as access control, attendance recording, payment mechanisms, crime prevention, and border security. While biometrics promise many benefits, including stronger user authentication, greater user convenience, and improved security and operational efficiencies, they pose data privacy and security concerns that are significant. Some of these concerns include unauthorized secondary uses (function creep), expanded surveillance and profiling of individuals, data misuse (including identity theft), false matches, non-matches, and system errors. Significant data security risks include potential spoofing, tampering, various security attacks, and insufficient accuracy.

Looking Ahead. There are ongoing efforts to help minimize the privacy and security risks of biometrics to more acceptable levels and to encourage user confidence. Some of these efforts include strengthening legal oversight mechanisms, developing clear data usage policies, and improving awareness, education, and training. However, the addition of privacy-enhancing technologies could enable individuals to manage their own personally identifiable information (PII) and minimize privacy risks at an earlier level. Biometric encryption is a process that securely binds a PIN or a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is recreated only if the correct live biometric sample is presented on verification. Some of the key benefits and advantages of biometric encryption technology include:

- No retention of the original biometric image or template
- From the same biometric, multiple and unlinkable identifiers for different uses can be generated that are cancelable and revocable
- Improved authentication security: stronger binding of user biometric and identifier
- Improved security of personal data and communications
- Greater public confidence, acceptance, and use
- Suitable for large-scale applications

These advantages and solutions are set out in greater detail in Ann Cavoukian and Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy* (http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf).

2. VIDEO SURVEILLANCE

Description of issue. Facial recognition video surveillance aside, we have seen the dramatic growth of video monitoring throughout the public and private sectors, both in the U.S. and other countries. The United Kingdom is perhaps the most developed in its use of video monitoring by the government in public places.

Looking ahead. Widespread implementation of garden-variety video surveillance is harmful for several reasons. We are becoming used to being watched, and at earlier and earlier ages. Many schools have installed video monitoring throughout their campuses. An increasing number of day care centers are connected to the Internet so parents can check in on their children. As time goes on, we are not as likely to fight to maintain a strong Bill of Rights (especially the First and Fourth Amendments) the more accustomed we become to video surveillance. A further threat is that "low-tech" video surveillance can be converted into facial recognition biometrics systems with the growth of digital technologies. As the cost of biometrics systems decreases, the temptation to convert low-tech video surveillance units to facial recognition systems will increase.

3. ONLINE PRIVACY AND E-COMMERCE

Description of issue. News stories of Internet privacy threats are commonplace these days. The Internet was designed as an inherently *insecure* communications vehicle.

- Hackers easily penetrate the most secure facilities of the military and financial institutions.
- Internet companies have designed numerous ways to track web users as they travel and shop throughout cyberspace. "Cookie" is no longer a word associated solely with sweets. It now refers to cyber-snooping.
- Identity thieves are able to shop online anonymously using the credit-identities of others.
- Web-based information brokers sell sensitive personal data, including Social Security numbers, relatively cheaply.

Looking ahead. One of the positive results of media coverage of online privacy is public awareness of the issue. Congressional representatives have taken notice, although to date legislation has not been passed into law. Some form of an Internet privacy law is expected to be passed in the coming years. But will such a law possess meaningful consumer protections, giving consumers the full complement of the "fair information principles" (FIPs)? Will the principles of notice, consent, access, security, enforcement, redress, and collection limitation be codified into law? Or will an online privacy law be a watered down version, simply notice and choice, or worse, just notice -- what privacy advocates call "FIPs-lite?"

It is one thing to mandate that every commercial Web site provide a privacy policy. It is quite another to require that commercial Web sites clearly explain their data-collection practices and provide meaningful methods for visitors to prevent their personal information and "clickstream" data from being captured and sold to other companies. So far, legislative bills mandating effective consumer privacy protection provisions have not advanced in Congress.

Knowledgeable individuals can take steps to prevent their web-surfing practices from being captured by the Web sites they visit. But, realistically, few people have the requisite knowledge or patience to take advantage of such privacy-enhancing strategies.

4. WORKPLACE MONITORING

Description of issue. Privacy advocates often use these words to describe the workplace: "You check your privacy rights at the door when you enter the workplace." Ubiquitous employee monitoring is now possible. Many forms of monitoring technologies are available in the marketplace and are becoming cheaper each year: video surveillance, telephone monitoring, e-mail and voice mail monitoring, computer keystroke tracking, Internet Web site monitoring, location tracking using badges worn by employees, and satellite tracking of the company fleet.

What makes matters worse is that these systems can be deployed secretly and invisibly. Employers are not required by law to disclose to their employees that such monitoring is being conducted, with the exception of Connecticut where a state law requires employer disclosure. Similar legislation has failed in Congress and in the California state legislature. The only places where employees can expect to be free from surveillance are in bathrooms and locker rooms, but even this protection is not absolute.

Looking ahead. The future is here. An American Management Association study found that a majority of employers are conducting some kind of monitoring, the most common being e-mail and web-surfing.

Employers make several arguments to justify their use of monitoring systems.

- The employer owns the systems used by the employees to do their work - primarily the phone and computer systems.
- Employers are responsible for the work product of their employees. Therefore they have a right, even a duty to monitor.
- Employers must guarantee a safe work environment for employees. They must be able to thwart sexual harassment, for example. And if an employee appears to be violent toward other workers, the employer must be able to detect and prevent such violence.
- Employers must be able to detect and prevent the sharing or selling of trade secrets and other matters of corporate intellectual property.

Employers have been successful in making these arguments when aggrieved workers have filed lawsuits for privacy violations. The few court cases have largely been decided in the employers' favor.

Workplace rights advocates recommend that monitoring be relegated to narrow situations where there is "reasonable suspicion," and that random or workplace-wide monitoring be prohibited. Whether a better balance will be adopted by U.S. employers is an open question. Legislation is often motivated by "horror stories." As workplace privacy abuses continue to make the news, there is always the possibility that a handful of precedent-setting court cases could change the landscape.

5. WIRELESS COMMUNICATIONS AND LOCATION TRACKING

Description of issue. The products and services offered by the wireless industry are advancing at a dizzying pace. Digital cell phones are becoming smaller, cheaper, and smarter. Mobile phone users can send and receive e-mail and pager messages and surf the Internet. Hand-held personal digital assistants, PDAs, are also equipped for wireless communications. Location-tracking features are offered by several companies, including Loopt, Networks in Motion, Wavemarket, OmniTRAKS, FindWhere, Motorola Rhino, Autodesk, and Google Latitude. These are generally marketed as "opt-in" services and many have been available since about 2005.

Many people don't realize that a cell phone, Blackberry or wireless laptop broadcasts its location whenever the power is on, whether or not a call is in progress. This has led to the ability to automatically identify somebody's location. This may be used to track you or for you to track your children, to monitor employee activities, to provide real time mapping assistance, or to deliver restaurant recommendations or targeted advertising content.

Location tracking is not just a single technology. It actually combines several technologies. Three basic techniques can be used to determine the location of a wireless phone or laptop:

- GPS compares the timing of radio signals from satellites in space
- Triangulation collects directional signals from cell phone towers
- Wi-Fi local area networks track high-frequency radio signals from transmitters

Thus, mobile devices, which know our location and other intimate details of our lives, are being turned into portable behavioral tracking and targeting tools that consumers take with them wherever they go.

Looking ahead. The vision of many marketers is to be able to deliver location specific advertising to wireless devices. So, if you're traveling through the city on I-494, you might receive a message telling you that just off the next exit is a restaurant that serves your favorite cuisine, Thai food. Or as you walk past Starbucks, you'll be flashed a message offering a special on double lattes.

OJ Simpson found out the hard way that cell phones can serve as location detection devices. His travels in the white Ford Bronco were tracked throughout Southern California because of the ability to triangulate the signals emitted from cell phones to and from the nearest communications towers. In fact, location tracking is now required by federal law. Cell phones must be able to pinpoint the user's location to the nearest 100 feet for emergency assistance.

Unfortunately, the trade-off for these conveniences and personal safety features is personal privacy. We Americans cherish our ability to travel freely and anonymously. But the new generation cell phones and other electronic devices threaten to track us everywhere.

The wireless industry is well aware that consumers do not want their communications devices to double as surveillance technologies. Some industry representatives are taking steps to develop privacy guidelines. They know that the wireless industry will not thrive unless customer privacy can be protected.

The legal standards of privacy for use of your location data are inconsistent, depending upon who is holding the data. Telecommunications carriers generally may not disclose your location data without a consumer opt-in. Other entities with access to your location information may not be subject to that standard.

In August 2002, the Federal Communications Commission turned down the telecommunications industry's request to adopt wireless location information privacy rules that would cover notice, consent, security and customer integrity.

In a 2009 FTC complaint, the Center for Digital Democracy and US Public Interest Research Group asked for an investigation into a number of practices involving tracking and targeting, including location-based advertising. A copy of the complaint is available at http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing. Stay tuned to see whether any regulatory standards might develop from the FTC complaint.

6. DATA PROFILING

Description of issue. As we make our way through everyday life, data is collected from each of us, frequently without our consent and often without our realization.

- We pay our bills with credit cards and leave a data trail consisting of purchase amount, purchase type, date, and time.
- Data is collected when we pay by check.
- Our use of supermarket discount cards creates a comprehensive database of everything we buy.
- When our car, equipped with a radio transponder, passes through an electronic toll booth, our account is debited and a record is created of the location, date, time, and account identification.
- We leave a significant data trail when we surf the Internet and visit websites.
- When we subscribe to a magazine, sign up for a book or music club, join a professional association, fill out a warranty card, give money to charities, donate to a political candidate, tithe to our church or synagogue, invest in mutual funds, when we make a telephone call, when we interact with a government agency . with all of these transactions we leave a data trail that is stored in a computer.

We are not yet to the point where the contents all of these many databases are combined, but we have come close. In the aftermath of the 9-11 terrorist attacks, government and law enforcement

authorities proposed the development of an airline traveler screening program that would compile data from many consumer data files. That proposal was highly controversial and was not implemented. But a limited version of the no-fly program, called Secure Flight, is not expected to be developed for several years.

Privacy and civil liberties advocates are often asked, "What are you afraid of? What do you have to hide? If you haven't done anything wrong, what's there to worry about?." The sentiment behind these questions is that the data being compiled is benign and is not going to harm us. But as law professor Jeffrey Rosen points out in his 2000 book *The Unwanted Gaze, you are not your profile*. Databases can contain errors. And data compiled from disparate sources and from differing contexts can lead the user to arrive at the wrong conclusions. (*The Unwanted Gaze: The Destruction of Privacy in America*, by Jeffrey Rosen, Random House, 2000)

[W]hen intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences. (p.9)

He used the 1998 subpoena by prosecutor Kenneth Starr of Monica Lewinski's book purchases from a Washington, D.C., bookstore as an example of how profiling can harm individuals. This occurred during the Clinton administration sex scandal. Rosen states:

Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge. (p.8)

Here is another story to illustrate the potential harm of untrammelled data collection and profiling.

In 1998 the *Salt Lake Tribune* reported that the supermarket chain Smith's Foods was subpoenaed by the U.S. Drug Enforcement Agency (DEA) for its discount card data on several named suspects. Was the DEA looking for high-volume purchases of non-prescription medicines that make up the chemical formula for "speed," like Sudafed? No. They were interested in finding out if these individuals had purchased a lot of plastic "baggies," the presumption being that if you're manufacturing and selling "meth," you will need plastic bags to package it in.

This story should alarm each of us. How many situations can we think of where someone might buy many "baggies" - the parent who wraps school lunches for a large family, the Girl Scout troop leader who makes sandwiches for the girls' outings, the jewelry maker who sells her creations at weekend arts fairs. Yet, if law enforcement were to request supermarket discount card data for "fishing trips," without court-ordered warrants -- something far more likely in the post-9-11 era of weakened checks and balances -- many individuals would be on the suspects list, most if not all of whom would not be drug dealers.

Looking ahead. The supermarket club card story illustrates the fair information principle of secondary usage: Information that has been gathered for one purpose should not be used for other purposes without the consent of the individual (paraphrased from the "use limitation principle," Organization of Economic Cooperation and Development, 1980).

The unfettered collection of data from numerous sources, in an environment where there are few legal restrictions on how the data can be used and merged, will inevitably lead to secondary uses that will violate privacy and trample on civil liberties. The legal protections for privacy in the U.S. are weak. They have been further weakened by the hasty passage of the USA PATRIOT Act, following the 9-11 terrorist attacks. There are few restrictions in the U.S. on how data can be collected and merged, in contrast to European Union countries, Canada, New Zealand, and Australia.

When I first wrote this report in March 2001, I said the following:

It is not farfetched to envision a future when such data will be used for a variety of secondary uses. If we were to enter a time of social unrest and political turmoil, our government might seek to use such information to investigate dissidents. We do not have to look very far to see such an investigation in our own time - Kenneth Starr's 1998 subpoena of Monica Lewinski's bookstore purchases during the Clinton impeachment proceedings.

The future is here. The terrorist attacks of 9-11 have launched us into just such an era of turmoil and uncertainty. The checks and balances that had previously been counted on to place limits on government access to consumer data have been largely lifted by the USA PATRIOT Act. Some -- but not all -- of the provisions of this law came with a sunset provision, so they could be evaluated and even reversed. But when the sunset date was reached in March 2006, those provisions were not reviewed for possible elimination, but rather were extended by Congress.

This situation is fortified by the strength of the information industries in the legislative arena. When there have been legislative attempts to regulate the collection and use of consumer data by private sector entities, industry associations have responded with a call for self-regulation. To date, this argument has been successful. The direct marketing and information broker industries are virtually unregulated, and their members collect a massive amount of data from consumers. Will such data be used for secondary purposes? We can count on it, especially in this post-9-11 era.

7. **CRIMINAL IDENTITY THEFT**

Description of issue. The number one topic of those who contact the hotline of the Privacy Rights Clearinghouse is identity theft -- when an imposter is able to obtain credit in the victim's name by having just a small amount of information about that person, typically the Social Security number (SSN). We refer to this crime as credit-related identity theft.

A growing form of identity theft is what we call criminal identity theft. In 2000 we joined with CALPIRG to conduct a survey of credit-related identity theft victims. One of the findings surprised us - that 12% of those who had experienced credit fraud were also burdened with a wrongful criminal record due to the activities of the imposter. Similarly, Federal Trade Commission statistics show that 15% of the identity theft victims in its database are dealing with criminal identity theft.

Criminal identity theft occurs when the imposter uses the innocent person's identification when arrested, say, for a traffic violation, shoplifting, marijuana possession, or another misdemeanor. When that individual fails to appear in court on the appointed day, a warrant is issued for the arrest of the innocent person.

The warrant may go unused for quite some time - until the unfortunate individual is stopped by law enforcement for speeding or a broken tail light, for example, or when going through U.S. Customs after returning from another country. Then the innocent individual may be arrested or even jailed -- until they can successfully prove that they are being impersonated by someone who used their identification data upon arrest.

It is virtually impossible to clear one's wrongful criminal record. There are no standard procedures, as there are with credit-related identity theft, to wipe the slate clean. Victims must obtain a certificate of clearance from the law enforcement unit where the arrest was made, and/or from the court system in that jurisdiction. But that document is not universally accepted by other law enforcement units.

Looking ahead. Cases of criminal identity theft are going to increase, perhaps substantially, for

several reasons. First, credit-related identity theft is on the rise. The Federal Trade Commission says that identity theft is the fastest growing crime in the nation. We know from survey data that approximately one in six such victims will also have to deal with wrongful criminal records.

Second, commercial sector information brokers are collecting an increasing amount of arrest and conviction data and are making it available for a variety of purposes, among them, law enforcement investigations and employment background checks. There is no such thing as a perfectly accurate database. Because these files are not updated as diligently as they should be, and because identity theft is on the rise, those who use such data are going to obtain inaccurate information on countless numbers of innocent individuals.

Law enforcement agencies and court systems at the local, state, and federal levels are going to need to adopt procedures to enable individuals with wrongful criminal records to remove or amend those records. It is likely that laws must be passed to establish such procedures. The California legislature has begun this process, passing laws in recent legislative sessions to assist individuals with wrongful criminal records.

But the process of establishing procedures to enable victims to remove erroneous criminal records data is very complex. Procedures vary from jurisdiction to jurisdiction, and from state to state. Criminal records agencies (the Departments of Justice in each state and the FBI) want to ensure that the accuracy and security of their data files are protected. For the sake of those innocent individuals who are burdened with wrongful criminal records, it is vitally important that this issue be addressed on a national basis, something that is likely to take considerable time.

8. BACKGROUND CHECKS

Description of issue. Previous sections describe what can happen if data files contain erroneous information. This situation is particularly harmful to job applicants when background checks uncover wrongful criminal records and other inaccurate data. Unless the employer notifies the job applicant of the contents of the investigation, that individual may not learn why he or she was rejected. Federal law requires such disclosure (Fair Credit Reporting Act). But the law contains loopholes that the employer can use to avoid notifying the applicant that negative information in the background investigation resulted in their not being hired.

The information broker industry is growing dramatically. More and more government records are being sold by county and state governments, and to a lesser degree, by federal agencies to private sector data vendors. Companies like Choicepoint and Lexis-Nexis compile records from thousands of sources and make them available to their subscribers, usually law enforcement agencies, private investigators, attorneys, debt collectors, skip-tracers, insurance claims investigators, and media outlets, among others.

Some information brokers provide their databases for a fee on Internet Web sites, hawking their wares with "spam" messages that promise, "You can find anything about anyone for just \$19.95." Anyone with a working credit card account can access these services, whether or not they have a legitimate business purpose. Those who use the services of these online information vendors are under no obligation to report their findings to the data subject.

The information broker industry has attempted to weed out those online vendors that sell data to anyone and everyone, instead of to individuals and organizations that have a so-called "legitimate business purpose." But "rogue" data vendors that operate online are still a reality. One company advertises that it can compile the following on individuals: criminal records check, bankruptcies and liens, small claims and judgments, sex offender check, alias names, address history, relatives and

associates, neighbors, home value and details, and more. Indeed, most of these data elements are public record and/or publicly available.

Looking ahead. The cost of background checks has decreased dramatically in recent years. As a result, more employers are conducting them. Investigations are going beyond a simple reference verification or credit report to include criminal background checks. Since the terrorist attacks of 9-11, an increasing number of employers are conducting background checks of new hires as well as existing employees.

It's fair to say that a significant percent of background checks are retrieving information that is either incorrect or misleading. As discussed in the "data profiling" section above, there is no such thing as a perfect database. Because of loopholes in the law, the subjects of background checks might never know the contents of their investigations and the reasons they are not able to land a job.

Legislative amendments to federal and state laws that govern "investigative consumer reports" must be passed into law in order to prevent a significant number of individuals from being harmed by erroneous reports. California recently amended its investigative consumer reporting act to require that all individuals who are the subject of background checks, with exceptions for suspicion of wrongdoing, have the opportunity to receive a copy of the report.

9. INFORMATION BROKER INDUSTRY

Description of issue. In previous sections, I discussed some of the privacy-related issues regarding the growing information broker industry. This industry is virtually unregulated except for the background check requirements in the Fair Credit Reporting Act.

A set of voluntary guidelines was adopted by the information broker industry in conjunction with the Federal Trade Commission in 1997. But the guidelines are weak and have resulted in no meaningful privacy protections for U.S. consumers. In addition, the industry group that developed the guidelines, the Individual Reference Services Group, has since disbanded.

Looking ahead. An incident from the November 2000 election illustrates what can go wrong when information broker data files are improperly used to make critical decisions about individuals. The Florida Secretary of State Division of Elections contracted with Database Technologies (DBT) to check its voter rolls against the data compiled by DBT. Many individuals were wrongly identified as being felons, and turned away at the polls. The original "scrub list," as it was called, included nearly 60,000 names. One county that checked each of the 700 names on its list could only verify 34 as former felons. ("Ex-Con Game," by Greg Palast, *Harper's Magazine*, March 2002). DBT has since been purchased by Choicepoint.

Without the effective regulation of this industry, a significant number of individuals are going to suffer privacy violations, lost job opportunities, ruined reputations, and discrimination. So far, the information broker industry has been effective in preventing laws from being passed on the federal level.

J. PUBLIC RECORDS ON THE INTERNET

Description of issue. One of the hallmarks of our democracy is open government. Most government agency and court records are considered "public" records, primarily so "we the people" can monitor our government. In the past, individuals accessed public records by traveling to the courthouse or to the government office and using the records there, a time-consuming and often expensive task. In recent years, however, a growing number of government agencies and court

systems have made these records available on the Internet.

Upon first consideration, it might be thought beneficial for government records to be easily available to the public via the Internet. After all, our government is supposed to be accessible to citizens.

- But what happens when the full texts of divorce records are available to anyone with an Internet connection, complete with sensitive financial data and family histories?
- What about access to an individual's criminal records of years gone by, showing a crime for which the individual has long since paid his or her debt to society, and which may have been legally expunged?
- Will an employer have a forgiving attitude toward a 30-year-old whose criminal record shows a conviction for shoplifting when the applicant was 19 years of age?
- Will an employer overlook a DUI conviction even after the individual has lived free of alcohol for many years?
- Is one's bankruptcy cause for negative value judgements by employers, relatives and neighbors?
- Should stalkers be able to locate their victims just because that person votes or drives, thereby revealing the home addresses in public records?
- Should identity thieves be able to pluck Social Security numbers, dates of birth, and mothers' maiden names from public records posted on the Internet?

Looking ahead. Unless we are somehow transformed into a tolerant society, our "transparent society," to borrow a term from sci-fi writer David Brin, is going to pose significant problems for a large number of individuals. The full texts of criminal and civil court records, divorce decrees, bankruptcies, and more are slated to be available from government and information broker websites. Employers are likely to use such information to make adverse hiring decisions. Identity thieves will find their pot of gold at the end of the rainbow simply by clicking a mouse. And neighbors and relatives may learn more about us than we are comfortable with.

Georgetown University law professor Jeffrey Rosen wrote *The Unwanted Gaze* about just such a scenario. He explains the value of privacy protection as follows:

Privacy protects us from being objectified and simplified and judged out of context in a world of short attention spans, a world in which part of our identity can be mistaken for the whole of our identity. (p.115)

There are several potential drawbacks for posting public records online, especially the full texts of court records.

- Fewer individuals will choose to participate in government in order to prevent information about them from being posted on the Internet.
- Many will choose not to seek justice through the court system. Justice will only be available to those with the resources and know-how to seek private judicial proceedings.
- Individuals will experience shame and embarrassment, even discrimination, when details of their personal lives are broadcast in court records available on the Internet.
- Reputations will be destroyed because of errors.
- Data from electronic public records files will be used for secondary purposes that stray far from the original public policy purposes for which they were first created, that being government accountability.
- A particularly troubling consequence of untrammelled access to electronic public records is the loss of "social forgiveness." The 30 year-old who has turned his life around might be judged harshly for his transgressions at age 19.

- Our society will see a growing number of individuals who are disenfranchised for life. Large numbers will not be able to find employment because of negative information in court files - whether true or not - from years gone by. Or they will be relegated to lower-paying jobs in the service industries.

The solution is *not* to ban public records altogether from the Internet. Instead, records should be selectively redacted, for example, by removing Social Security numbers and financial account data. Instead of publishing the *full texts* of sensitive proceedings such as divorce cases, on the Internet, just the *index* information should be published. Certain categories of case files, family court records for example, should be available at the court house and not online. These and other solutions must be sought in order to prevent the negative consequences of publishing public records online, but without losing sight of the need for access to public records in order to provide oversight of our government.

11. FINANCIAL PRIVACY

Description of issue. As a result of the federal Financial Services Modernization Act, banks, insurance companies, and brokerage firms are now able to affiliate with one another under one corporate roof. This law, known as Gramm-Leach-Bliley (GLB) after its sponsors, was implemented in 2001.

Credit card companies, banks, insurance companies, and brokerage firms may share their respective databases with one another -- called affiliate sharing -- but they cannot sell customer data to third parties without providing an opt-out notice to their customers.

Looking ahead. Unless legislation is passed at both the federal and state levels to strengthen the Financial Services Modernization Act, the process of affiliate sharing will enable these merged corporations to assemble customer data files of unprecedented scope. Some financial institutions have more than 2,000 affiliates spanning a broad array of businesses.

While "junk" mail, e-mail, and telemarketing solicitations are a likely result of widespread affiliate sharing of customer data, privacy advocates are even more concerned about the potential for harmful uses of data merging and data profiling:

- Decisions on one's credit worthiness might hinge on medical information gleaned from insurance company data.
- A scam artist might use one's profile as a risk-taking investor to pitch get-rich-quick schemes.
- Elderly individuals with cash-rich portfolios could be vulnerable to fraud artists' promises of lucrative returns on risky investments.

The GLB Act contains a provision that enables state legislatures to pass stronger privacy provisions. Indeed, several states have debated privacy bills that allow for an opt-in for third party data sharing, thereby setting the default at no sharing unless the customer says "yes." In contrast, the GLB standard is opt-out.

The California legislature passed the Financial Information Privacy Act that requires an "opt in" by customers before a financial institution can sell personal information to third parties. Customers are given the ability to "opt out" of the sharing of personal information with company affiliates.

Given the high percent of the population favoring strong privacy protection -- 80% to 90% in most

polls -- state legislatures and Congress are expected to grapple with this issue for years to come. The financial services industry is likely to exert considerable pressure on Congress to pass an amendment to GLB that prohibits states from enacting stronger privacy measures.

12. MEDICAL RECORDS CONFIDENTIALITY

Description of issue. It is not an exaggeration to state that our video rental records have had more privacy protection than our medical records in the past. The Clinton Administration's Health and Human Services Department (HHS) attempted to rectify this situation by developing privacy regulations as required by the passage of HIPAA, the Health Insurance Portability and Accountability Act.

The HIPAA regulations, effective in April 2003, made significant strides for American healthcare consumers, especially in requiring healthcare institutions to give patients notice of their information practices, and in enabling individuals to gain access to their own medical records. But some of the privacy provisions have been rolled back due to pressure from the healthcare industry, in particular the patient consent requirements. Consent is not required for information sharing involved in treatment, payment, and operations.

During the first 5 years of HIPAA enforcement, HHS did not assess a single civil penalty in response to well over 30,000 complaints. The agency claims to focus on voluntary compliance and correction by covered entities.

In July 2008, for the first time since the privacy rules went into effect in 2003, the HHS entered into a resolution agreement with a covered entity requiring the organization to pay \$100,000.

Looking ahead. Most individuals consider their medical information to be among the most sensitive of any information about them. And many are under the mistaken impression that the Hippocratic oath still holds true today.

Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets. Hippocrates, 4th Century B.C.

But in truth, one's medical information is an open book in our far-flung healthcare system -- from medical providers, to insurance companies, to self-insured employers, to laboratories, and to payment companies, medical transcriptionists, pharmacies and pharmacy benefits systems, government regulators, and more.

It remains to be seen whether HHS will depart from its current policy of voluntary compliance and begin to take a more aggressive approach in enforcing the HIPAA regulations.

12a. GENETIC PRIVACY

Description of issue. Genetics is the science of differences and can be used to categorize people, stigmatize them, or subject them to social or economic discrimination. Persons being tested aren't the only people with an interest in the test results. Family members and potential mates, employers, insurers, the press and the government all may desire information about a person's genetics. Hence, genetic information raises a host of privacy issues.

The use of genetic data to discriminate in both employment and health insurance is of growing concern to consumers, healthcare professionals, and policymakers alike. In 2001, U.S. News &

World Report reported that the railroad company Burlington Northern secretly conducted genetic tests on employees who had filed worker's compensation claims for carpal tunnel syndrome. The company's intention was presumably to be able to reject some claims because of genetic predisposition to the condition, despite the fact that predisposition to this ailment is questionable. (Dana Hawkins, "The dark side of genetic testing," U.S. News & World Report, Feb. 19, 2001)

Another key issue is determining when disclosure of genetic information should be permitted in order to protect third parties from harm. For example, can a physician over a patient's objection reveal a positive test result for an inherited disorder to the patient's children, on the ground that disclosure is necessary to enable the children to protect themselves?

A number of states have enacted legislation to prohibit health insurers from collecting or using certain types of genetic information, but this is not a complete solution. Most of these laws cover only limited types of genetic information and apply only in limited settings. They also do not address the problem of employment discrimination.

On the federal level, the Genetic Information Nondiscrimination Act of 2008 (GINA) was designed to prohibit the improper use of genetic information for insurance and employment purposes. GINA prohibits insurers from denying coverage to a healthy individual or charging that person higher premiums based solely on a genetic disposition to developing a disease in the future. The legislation also bars employers from using genetic information when making employment decisions. Unfortunately, the legislation does not go far enough in enabling personal control over genetic testing results. For a more detailed analysis of GINA and other genetic privacy issues, see the World Privacy Forum's Genetic Privacy page at <http://www.worldprivacyforum.org/geneticprivacy.html>

Looking ahead. Notwithstanding the potentially valuable information that genetic testing may provide, we must be wary of the potential threat to our privacy. There are no simple solutions. As biotechnology and computer technology advance, substantial privacy issues will continue to arise.

The challenge of protecting health information is compounded by the increasing reliance upon digital data. Medical records are shifting from largely paper-based systems to electronic health records (EHRs). Ultimately, a person's EHR may include all of their medical information from "cradle to grave." In a paper-based system, privacy is mainly protected by fragmentation and chaos. Because the system is fragmented, it can be difficult or impossible to compile an individual's records from multiple providers over extended periods.

The number of genetic tests and the number of people taking them will increase significantly in the coming years. EHRs will make it easier to disclose genetic information widely. As the U.S. and other countries contemplate better ways to deal with genetic information, policymakers are seeing that protecting privacy is neither cheap nor easy. Improved security measures can keep information from being disclosed without authorization, but restricting the scope of authorized disclosures is equally important. It is essential, and challenging, to decide which individuals and entities have a right to which information and for what purposes.

Effective legislation should, at minimum, include four elements, according to experts. First, it should address the underlying difficulties in gaining access to health insurance and carefully balance the rights of employers and employees. Second, legislation should limit nonmedical uses of predictive health information, including for life insurance, disability insurance and long-term care insurance. Third, any legislation should limit the scope of disclosures, penalize wrongdoers and provide remedies for people harmed by wrongful disclosures. And fourth, EHRs should be designed so that they can limit disclosures to relevant health information. Tackling these matters will provide an effective first step toward shaping the future of medical privacy. (Mark A. Rothstein, "Tougher Laws

Needed to Protect Your Genetic Privacy", Scientific American, August 19, 2008, www.sciam.com/article.cfm?id=tougher-laws-needed-to-protect)

13. WIRETAPPING AND ELECTRONIC COMMUNICATIONS

Description of issue. The FBI during the Clinton Administration made several attempts to strengthen its wiretapping capabilities, especially of digital telephone communications and Internet communications. Its "Carnivore" technology is a "black box" that can be installed in Internet Service Providers' (ISP) systems to monitor the e-mail traffic of its subscribers.

In the wake of the terrorist attacks of September 11, 2001, the USA PATRIOT Act has made it easier and faster for authorities to obtain telephone wiretaps as well as access to Internet communications. Procedural requirements, notably showing probable cause that a crime had been or was about to be committed, have been weakened.

Looking ahead. The checks and balances provided by the U.S. Constitution and a host of laws have been weakened considerably by the USA PATRIOT Act regarding wiretapping and the interception of e-mail and web-surfing transactions. The law contains a number of secrecy clauses which prevent individuals from reporting ways in which the law is being used. The sunset provisions would have enabled several subsections to be evaluated and possibly overturned upon renewal of the Act. But when the PATRIOT Act was renewed in March 2006, the sunset provisions were renewed as well.

Civil liberties organizations are using the Freedom of Information Act (FOIA) to attempt to determine how the Patriot Act is being implemented by government authorities, and whether or not abuses are occurring. In addition, members of Congress who are concerned about widespread violations of civil liberties are attempting to monitor the law's implementation. In light of the secrecy clauses in the law, it is actions such as these that will be needed to shine light on whether or not government authorities have overstepped their bounds.

14. YOUTH PRIVACY ISSUES

Description of issue. Children and youth are vulnerable to a number of privacy threats.

- Their marketing profiles are highly prized. And since children are avid Internet users, marketers have attempted to capture data from their web surfing.
- Children watch a lot of television. With TV going "digital," (see below) marketing information is likely to be compiled from such new technologies as TiVo and ReplayTV.
- State education departments are developing databases that track students throughout their K-12 school years.
- States are developing databases to track children's vaccine inoculations.
- Students are often asked to complete surveys that ask sensitive questions about themselves and their families.
- Given the incidents of violence in schools, administrators and school psychologists have the incentive to use profiling tools (Mosaic is one example) to attempt to identify individuals who are supposedly predisposed to violence, and then share that information with local law enforcement.

Looking ahead. While these threats do not necessarily interrelate with one another, it is evident that children and youth are the targets of a great deal of data collection. Congress has acted to limit online data collection from children under age 13 by passing the Children's Online Privacy Protection Act, implemented in April 2000. And the Bush Administration signed into a law a provision to require

that schools give parents the opportunity to opt the student out of participation in marketing related surveys that collect personal information. This is part of the No Child Left Behind Act of 2001.

But as we've seen with the other issues discussed in this report, laws are not able to keep up with the fast pace of technology. Children are early adopters of computer and wireless technologies, and are far more skilled than many of their elders in using them. Children are also voracious consumers of the latest trends in clothing, music, sports, and entertainment. Marketers are not likely to bypass the opportunity to collect data from children and to solicit both them and their parents. The tension between laws and technology regarding children will persist for time to come.

15. DIGITAL RIGHTS MANAGEMENT

Description of issue. The First Amendment gives Americans the right to explore ideas in books, music, and movies without having to identify ourselves. The right to anonymity is a vital foundation stone of our democratic society. Our strong First Amendment tradition protects people with dissenting, unpopular, or controversial ideas.

But the migration of print, music, and images to the Internet has spawned new technologies called "digital rights management" systems (DRM) that infringe upon intellectual freedom. Copyright owners, including the entertainment industry and publishers, are attempting to monitor those who download copyrighted files in order to prevent piracy and ensure payment for their products. In developing DRM systems, they threaten to create technologies that identify those who read, listen to, and view Internet content.

The companies that collect this information will be able to develop profiles of those who access Internet content. And as I've discussed elsewhere in this report, with profiling comes the potential for secondary uses to be made of that data, from marketing to government surveillance.

Looking ahead. Intellectual property scholars point out that copyright and privacy have traditionally been compatible because copyright provisions control public distribution of content. Private use of copyrighted material has been governed by the fair use doctrine, enabling individuals to make limited copies for their own use.

But DRM systems threaten to monitor private use by implementing technologies that capture personally identifiable information for each and every use. A challenge for policymakers and industry is to develop DRM systems that can confirm the eligibility of individuals to access content without identifying the actual user. Another challenge is to preserve the principle of fair use.

16. DIGITAL TELEVISION AND BROADBAND CABLE TV

Description of issue. We are at the dawn of a revolution in television technology. Our TV sets are going digital. Custom-made television viewing is now possible with set-top boxes like TiVo and ReplayTV that can capture only those TV programs that we want to watch and enable us to view them at any time. These devices rely on two-way communications to send and receive data about consumers' viewing preferences. This data is going to be highly prized by marketers.

In a legal environment of weak privacy protection, consumers have little ability to control what is done with such data. A California state senator introduced legislation in 2000 to create an opt-in right of consent before third parties can obtain data compiled from digital television viewing patterns. The bill was defeated by strong industry lobbying.

Looking ahead.. In the era of digital television, TV viewers are likely to be served advertisements based on their unique interests. Many consumers may appreciate this. But privacy advocates are concerned about the secondary uses that could be made of such data. In a post 9-11 world where consumer data is considered fair game for profiling purposes, information obtained from digital TV-viewing is likely to be part of the mix unless laws are passed to give individuals the ability to control data collection and to prevent secondary uses.

17. RADIO FREQUENCY IDENTIFICATION (RFID)

If you are able to wave your keychain in front of the gasoline pump's meter to automatically pay for the fuel you just pumped, you are likely to be using RFID technology. Attached to your keychain is a card that contains a small data chip and antenna called Radio Frequency ID.

Another present-day use of RFID technology is within building-access cards – ID cards that enable individuals to gain entry into a building or into an office within a building. Yet another application is student identification cards issued by universities. These are often called contactless ID cards because the user need only wave the card within a few inches of the reader in order to gain entry to the building or office.

In the applications described here – paying for fuel and gaining entry into a secured building – the individual is well aware of each and every use in which the RFID tag is accessed. But RFID tags are tiny and can be embedded in items in ways that are virtually invisible. And reading devices can also be invisible.

Looking ahead. One futuristic scenario – akin to the plot in the Tom Cruise movie *Minority Report* – involves the tracking of individuals by location as they make their way through each day. RFID readers would be embedded in, say, street-light poles. In this scenario, the RFID tag associated with the individual – perhaps embedded in one's driver's license -- also records the transactions that person engages in as each day progresses such as buying a newspaper at the corner vending machine, entering a supermarket and purchasing groceries, using public transit, entering the person's place of work, and so on.

In an even more troubling futuristic scenario, law enforcement and government agencies could identify which individuals participate in anti-government demonstrations on the Capitol Mall in Washington, D.C. – an activity that can be engaged in anonymously now, and in which the First Amendment indeed guarantees the possibility of anonymous participation. If RFID tags were embedded in driver's licenses – which most people carry with them at all times – we could live in a society where locational privacy and anonymity are a thing of the past.

Will such a scenario actually happen? Many people find it hard to imagine that we would allow such uses of RFID to actually occur. But if we were to experience another terrorist attack, perhaps even more destructive and widespread than 9-11, we as a society might be willing to accept such uses of technology to track and monitor our movements and transactions.

18. REAL ID

The Real ID Act creates a federal identity document that every American will need in order to fly on commercial airlines, enter government buildings, open a bank account, and more. The purported reason for this law is to fight terrorism by creating driver's licenses in all 50 states that are more or less uniform and that serve as a de facto national ID card.

But the Real ID Act has many opponents, including civil liberties and privacy groups. They point out that it would create a nationwide identity system and would function as an internal passport, something that has long been opposed in this country. Real ID would not likely be effective in thwarting terrorism because terrorists would quickly learn how to counterfeit Real ID cards.

Because Congress appropriated no funding for the states, the financial burden on state governments and the adults living in those states would likely be considerable. Further, the creation of a single interlinked database as well as the requirement that each DMV store copies of every birth certificate and other identity documents of drivers in each state would create a highly desirable target --one-stop shopping if you will -- for identity thieves and other kinds of fraudsters.

Looking ahead. The Real ID Act has encountered considerable opposition across the country. Maine is the first state to pass a bipartisan resolution to repeal the law. And many more states have introduced similar bills. If Real ID survives at all, Congress will likely weaken it significantly.

19. ABSENCE OF FEDERAL-LEVEL PRIVACY PROTECTION LAW

Citizens of nearly all developed countries throughout the world enjoy rights to privacy through laws that are called “data protection acts.” In most such nations, comprehensive, or omnibus, data protection laws govern how personal information can be used by government agencies as well as commercial-sector entities. The use of personal information is usually an “opt in” under such laws. In other words, an individual’s personal information cannot be used, say, for marketing unless that person gives affirmative consent.

The U.S. has no such law. Instead, we have what are known as sectoral privacy laws. Examples are the Telephone Consumer Protection Act (telemarketing), the Fair Credit Reporting Act (credit reports and employment background checks), the FACT Act (financial privacy), and HIPAA (medical records privacy). But a sectoral approach leaves many uses of personal information unprotected. For example, the “junk” mail that we receive when we subscribe to magazines is not covered by a specific law.

The approach taken in the U.S. is referred to as “opt out.” For example, your personal information is used to send you unsolicited ads until and unless you sign up for the direct marketing industry’s Mail Preference Service (MPS). And even that does not guarantee that your mailbox will be “junk”-free. The MPS is a voluntary standard. Although members of the Direct Marketing Association must subscribe to it as a condition of membership, not all companies that market to individuals are members. Witness the “spam” in your email inbox.

Legal experts explain that commercial entities are protected by the First Amendment, just as individuals are. In other words, a company has a right to “speak” to individuals by sending them unsolicited ads through the mail and by emailing them “spam” ads.

20. BEHAVIORAL TARGETING

Description of issue. Behavioral tracking refers to the practice of collecting and compiling a record of individual consumers' online activities, interests, preferences, and/or communications over time.

Behavioral targeting then uses behavioral tracking to serve advertisements and/or otherwise market to a consumer based on his or her behavioral record. Behavioral targeting may use information collected on an individual's web-browsing behavior, such as the pages they have visited or the searches they have made, to select which advertisements to display to that individual. Advertisers believe that this may help them deliver their online advertisements to the users who are most likely

to be influenced by them. Behavioral information can be used on its own or in conjunction with other forms of targeting based on factors like geography or demographics.

Looking ahead. The collection, use, maintenance, and disclosure of personal and behavioral information for marketing purposes promises to be a growing threat to consumers' privacy rights. According to a study commissioned by consumer privacy organization TRUSTe, 71 percent of online consumers are aware that their browsing information may be collected by a third party for advertising purposes, but only 40 percent are familiar with the term "behavioral targeting." 57 percent of survey respondents are not comfortable with advertisers using browsing history to serve ads, even when that information cannot be tied to their personal information.

http://www.truste.org/about/press_release/03_26_08.php

Marketers and advertising networks will continue to expand the ways in which they monitor and maintain data on consumers' online behavior. The expansion of behavioral tracking and targeting of consumers through the Internet and other networked devices will continue to demonstrate the failures of the current structure for addressing consumer privacy interests. This expansion will threaten privacy in new ways that consumers are largely unaware of. Future consolidations of information powerhouses (such as DoubleClick and Google) will only exacerbate the privacy threats posed by behavioral targeting.

Even more disturbing is the small but growing trend of internet service providers (ISPs) tracking the online behavior of their subscribers. By their very nature, ISPs have access to virtually everything you do online. "Deep-packet inspection," (DPI) allows ISPs to readily know the packets of information you are receiving online including e-mail, Web sites, music and video sharing and software downloads. Every bit of data is divided into packets that can be accessed and analyzed for content. While some uses of DPI may be necessary for ISPs to properly maintain their operations, DPI poses a significant challenge to privacy when the information is used for behavioral targeting purposes. Companies such as Front Porch, NebuAd, and Phorm market this type of behavioral targeting to ISPs as an additional revenue service.

21. CLOUD COMPUTING

Description of issue. It is difficult to come up with a precise definition of cloud computing. In general terms, it's the idea that your computer's applications run somewhere in the "cloud," that is to say, on someone else's server accessed via the Internet. Instead of running program applications or storing data on your own computer, these functions are performed at remote servers which are connected to your computer through the Internet.

With more reliable, affordable broadband access, the Internet no longer functions solely as a communications network. It has become a platform for computing. Rather than running software on your own computer or server, Internet users reach to the "cloud" to combine software applications, data storage, and massive computing power.

It's a bit easier to understand the concept of cloud computing by providing examples. Google operates several well-known cloud computing services. It offers its users such applications as e-mail, word processing, spreadsheets, and storage, and hosts them "in the cloud" -- in other words, on its own servers, not yours.

Other examples of cloud computing include: web-based email services such as Yahoo and Microsoft Hotmail, photo-storing services such as Google's Picassa, spreadsheet applications such as Zoho, online computer backup services such as Mozy, file transfer services such as YouSendIt, online medical records storage such as Microsoft's HealthVault, and applications associated with social networking sites such as Facebook.

Looking ahead. When users store their data with programs hosted on someone else's hardware, they lose a degree of control over their sensitive information. The responsibility for protecting that information from hackers and internal data breaches then falls into the hands of the hosting company rather than the individual user.

Government investigators trying to subpoena information could approach that company without informing the data's owners. Some companies could even willingly share sensitive data with marketing firms. So there is a privacy risk in putting your data in someone else's hands. For any cloud application that you decide to use, be sure to read its privacy policy carefully. Obviously, the safest approach is to maintain your data under your own control.

The concept of handing sensitive data to another company worries many people. Is data held somewhere in the cloud and sent over the Internet as secure as data protected in user-controlled computers and networks? Privacy and security can only be as good as its weakest link. Cloud computing increases the risk that a security breach may occur.

One of the problems with cloud computing is that technology is frequently light years ahead of the law. There are many questions that need to be answered. Does the user or the hosting company own the data? Can the host deny a user access to their own data? And, most importantly from a privacy standpoint, how does the host protect the user's data?

Appendix: Nonprofit public interest groups who are working on these issues include the following:

- American Association of Retired Persons, www.aarp.org
- American Civil Liberties Union, www.aclu.org
- California Public Interest Research Group, CALPIRG, www.calpirg.org
- Center for Democracy and Technology, www.cdt.org
- Center for Digital Democracy, www.democraticmedia.org
- Computer Professionals for Social Responsibility, www.cpsr.org
- Consumer Action, www.consumer-action.org
- Consumer Federation of America, www.consumerfed.org
- Consumers Union, www.consumer.org
- Council for Responsible Genetics, www.gene-watch.org
- Electronic Frontier Foundation, www.eff.org
- Electronic Privacy Information Center, www.epic.org
- Genetic Alliance, www.geneticalliance.org
- Health Privacy Project, www.healthprivacy.org
- National Consumers League, www.nclnet.org
- National Work Rights Institute, www.workrights.org
- Privacy Activism, www.privacyactivism.org
- Privacy Rights Clearinghouse, www.privacyrights.org
- U.S. Public Interest Research Group, USPIRG, www.pirg.org
- World Privacy Forum, www.worldprivacyforum.org