Technology Review
PUBLISHED BY MIT

July/August 2009

Privacy Requires Security, Not Abstinence

Protecting an inalienable right in the age of Facebook.

By Simson Garfinkel

I'd be a fool to include my Social Security number in this article: doing so would leave me vulnerable to all manner of credit fraud, scams, and even criminal arrest. All of this would surely happen because a few bad people would read the article, write down my SSN, and pretend to be me.

We know a lot more about the use and abuse of SSNs today than we did back in 2002. That was the year the California state legislature passed SB 1386, the first U.S. law requiring that consumers be notified when computer systems holding their personal information are "breached" or that information is otherwise compromised. Because of SB 1386, we learned in 2005 that ChoicePoint--a company most Americans had never heard of--had somehow sold detailed credit histories on more than 163,000 consumers directly to identity thieves (more than 800 people suffered direct losses as a result). And in 2007, we learned that identity thieves had broken into the computer systems of the discount retailer TJX and stolen more than 45 million credit-card numbers.

We've also learned that governments are equally bad at securing personal information, as demonstrated by the half-million records breached at the Oklahoma Department of Human Services, the eight million records reportedly exposed at the Virginia Department of Health Professions, and the 26.5 million records stolen (along with a laptop and portable hard drive) from a work-from-home employee of the U.S. Department of Veterans Affairs.

All these cases, and many more, paint a disturbing picture of what is really threatening privacy in America today.

Privacy matters. Data privacy protects us from electronic crimes of opportunity--identity theft, stalking, even little crimes like spam. Privacy gives us the right to meet and speak confidentially with others--a right that's crucial for democracy, which requires places for political ideas to grow and mature. Absolute privacy, also known as solitude, gives us to space to grow as individuals. Who could learn to write, draw, or otherwise create if every action, step, and misstep were captured, immortalized, and evaluated? And the ability to conduct transactions in privacy protects us from both legal and illegal discrimination.

Until recently, people who wanted to preserve their privacy were urged to "opt out" or abstain from some aspects of modern society. Concerned about having your purchases tracked by a credit-card company? Use cash. Concerned that E-ZPass records might be used against you in a lawsuit? Throw coins at that toll booth. Don't want to show your ID at the airport? Drive. Don't want your location tracked minute by minute? Turn off your cell phone. And be in a minority: faced with the choice of convenience or privacy, Americans have overwhelmingly chosen the former. Companies like TJX haven't even suffered from allowing their customers' personal data to be leaked.

Now, however, abstinence no longer guarantees privacy. Of course, it never really did. But until the past two decades it was always possible to keep some private information out of circulation. Today, although you can avoid the supermarket savings card, the market will still capture your face with its video cameras. You can use cash, but large cash transactions are reported to the federal government. You can try to live without the Internet--but you'll be marginalized. Worse, you won't be able to participate in the public debate about how your privacy is wasting away--because that debate is happening online. And no matter what you do, it won't prevent your information from being stored in commercial networked systems.

In this environment, the real problem is not that your information is out there; it's that it's not protected from misuse. In other words, privacy problems are increasingly the result of poor security practices. The biggest issue, I've long maintained, is that decision makers don't consider security a priority. By not insisting on secure systems, governments and corporations alike have allowed themselves to get stuck with insecure ones.

Consider the humble Social Security number. As a privacy advocate, I always chafe when people ask me for my "social." As a security professional, I am deeply disturbed that a number designed as an *identifier*--for the single specific purpose of tracking individuals' earnings to calculate Social Security benefits--has come to be used as a *verifier* of identity for countless other purposes. Providing my SSN should not "prove" that I am who I say I am any more than providing my name or address does. But in the absence of any better system, this number has become, in the words of Joanne McNabb, chief of California's Office of Privacy Protection, the "key to the vault for identity thieves."

Yes, privacy as we know it is under attack--by a government searching for tax cheats and terrorists; by corporations looking for new customers; by insurance companies looking to control costs; and even by nosy friends, associates, and classmates. Collectively, we made things worse by not building strong privacy and security guarantees into our information systems, our businesses, and our society. Then we went and networked everything, helping both legitimate users and criminals. Is it any wonder things turned out this way?

All of a sudden, we have a lot of work to do.

But while our current privacy issues feel as new as Twitter, the notion of privacy as a right is old. Americans have always expected this right to be maintained, even as technology opened ever more powerful tools for its subversion. The story of privacy in America is the story of inventions and the story of fear; it is best told around certain moments of opportunity and danger.

The Constitution

The word *privacy* doesn't appear in the U.S. Constitution, but courts and constitutional scholars have found plenty of privacy protections in the restriction on quartering soldiers in private homes (the Third Amendment); in the prohibition against "unreasonable searches and seizures" (the Fourth Amendment); and in the prohibition against forcing a person to be "a witness against himself" (the Fifth Amendment). These provisions remain fundamental checks on the power of government.

Over time, however, the advance of technology has threatened privacy in new ways, and the way we think about the concept has changed accordingly.

Back in 1890 two Boston lawyers, Samuel Warren and Louis Brandeis, wrote an article in the *Harvard Law Review* warning that the invasive technologies of their day threatened to take "what is whispered in the closet" and have it "proclaimed from the house-tops." In the face of those threats, they posited a direct "right to privacy" and argued that individuals whose privacy is violated should be able to sue for damages.

Warren and Brandeis called privacy "the right to be let alone" and gave numerous examples of ways it could be invaded. After more than a century of legal scholarship, we've come to understand that these examples suggest four distinct kinds of invasion: intrusion into a person's seclusion or private affairs; disclosure of embarrassing private facts; publicity that places a person in a "false light"; and appropriation of a person's name or likeness.

In our world, "intrusions into a person's seclusion or private affairs" might describe someone's hacking into your computer system. Consider the case of Patrick Connolly, a U.S. military contractor accused of victimizing more than 4,000 teenagers by breaking into their computers and threatening to make their pictures and videos public unless they sent him sexually explicit photos and videos of themselves. You can also be intruded upon in many lesser ways: when companies force advertisements onto your screen, for example, or make pop-ups appear that you need to close. It's intrusive for a telemarketer to call you during dinner. That's why programs that block Internet advertisements and the federal government's "do not call" list are both rightly seen as privacy-protecting measures.

The desire to prevent the disclosure of embarrassing private facts, meanwhile, is one of the driving forces behind the privacy regulations of the Health Insurance Portability and Accountability Act (HIPAA). Because of this law and the regulations deriving from it, a health-care provider cannot disclose information in your medical records unless you give explicit permission. Another law, the Video Privacy Protection Act of 1988, makes it illegal for Netflix to disclose the movies you rent.

"False light" is a problem we still don't know how to address online. It's all too easy on today's Internet to attack a person's reputation with anonymously posted false statements. And even though free-speech advocates invariably say that the antidote to bad speech is more speech, experience has shown that this remedy is less effective in the age of Google. For example, two years ago AutoAdmit, an online message board for law students and lawyers, was sued by two female Yale Law students who said they'd been unable to obtain summer associate positions because vile and malicious sexual comments about them appeared whenever someone searched for their names.

Using a name or likeness without permission is at the heart of most "sexting" cases that reach the newspapers. Journalists often focus on the fact that teens are willingly sending sexy or downright pornographic photos of themselves to their boyfriends or girlfriends. But the real damage happens when a recipient forwards one of these photos to friends. That is, the damage is caused by the appropriation, not the receipt.

The fact that a dusty *Harvard Law Review* article corresponds so closely with the online privacy problems we face today suggests that even though technology is a driving factor in these privacy invasions, it's not the root source. The source is what sits in front of the computer's screen, not behind it.

For another example, consider electronic surveillance. Although e-mail and telephones give the appearance of privacy, sensitive electronic communications have always been an attractive target. Wiretapping was employed by both sides during the Civil War, prompting some states to pass laws against it. But it was the invention of the microphone and the telephone that brought the possibility of electronic surveillance into the homes of ordinary Americans. This shifted the action in U.S. privacy law from information to communication.

In 1928, in a case called *Olmstead v. United States*, the Supreme Court heard the appeal of a Seattle bootlegger whose phones had been tapped by federal agents. The agents had not trespassed or broken any laws to install the wiretaps, but they didn't have a search warrant either, as would have been required for a physical search of Roy Olmstead's property.

Brandeis, who had been appointed to the court by Woodrow Wilson in 1916, was appalled. "Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential and privileged, may be overheard," he wrote in his opinion. Alas, it was a dissent. By a 5-4 majority, the court found in favor of the government: search warrants were not required for eavesdropping on electronic communications, because "there was no searching." Olmstead went to prison, federal agents got the right to wiretap without a warrant, and that's how the law stood for another 39 years, until the case was overturned by a more liberal court in 1967.

It's comforting to know that U.S. law eventually gets things right with respect to privacy--that is the power of our republic, after all. But it's also troubling how long it sometimes takes. A lot of injustice can happen while we wait for the law to accommodate advances in technology.

The Computer

Consumer data banks as we know them today--big repositories of personal information, indexed by name and specifically constructed for the purpose of sharing information once regarded as "private"--didn't start with computers. But computers certainly helped.

One of today's largest consumer reporting firms was started in 1899, when two brothers created the Retail Credit Company--now known as Equifax--to track the creditworthiness of Atlanta grocery and retail customers. Businesses were encouraged to report which of their customers reliably paid their bills and which did not. Retail Credit collected the information, published it in a book, and sold copies.

Retail Credit and other consumer reporting firms maintained paper files until the 1960s. When they finally started to computerize, they came head to head with a Columbia University political-science professor named Alan Westin.

Westin had uncovered countless cases in which people had been denied credit, insurance, housing, even jobs, because of errors in consumer files--records that many victims didn't even know existed. He feared that computerization would make credit data banks much more widely used, with ominous consequences unless they were properly regulated. In the computer age, he said, privacy is no longer just the right to be left alone; it involves people's right "to determine for themselves when, how, and to what extent information about them is communicated to others." Possession of personal information, Westin said, should not give corporations unlimited rights to use that information.

Westin's research sparked numerous congressional investigations and got him invited to testify before Congress. People were entitled to view their own records, he said. And they needed a way to dispute the records and force an investigation if they thought there was an error.

Retail Credit and others protested that they would be stymied and bankrupted by a flood of requests. And Westin's definition of privacy could put different parties' rights in clear conflict--taken to its extreme today, it would mean that an ex-lover could order you to remove his or her name from your address book and delete all those old e-mails. But Westin and the other privacy advocates won the day, and Congress passed the Fair Credit Reporting Act of 1970. A Nixon administration advisory committee then developed the Code of Fair Information Practice, a guiding set of principles that underlies the majority of U.S. privacy laws passed since.

This code is surprisingly straightforward. There should be no secret data banks; individuals must be able to view their records; there must be a way to correct errors; organizations maintaining data banks must make sure they're reliable and protect them from unauthorized access; and information collected for one purpose must not be used for other purposes.

For example, the Video Privacy Protection Act was passed after Judge Robert Bork's video rental records were obtained by the Washington, DC, weekly *City Paper* in an attempt to dig up embarrassing information while the U.S. Senate was debating his 1987 nomination to the Supreme Court. The Driver's Privacy Protection Act of 1994 was passed after actress Rebecca Schaeffer was murdered in 1989 by a crazed fan, who had hired a private investigator to track down her address. The investigator was able to get the information through the California Department of Motor Vehicles, which had required Schaeffer to provide her home address when she applied for a license.

In both cases, Congress acted to prevent personal information from being reused in certain ways without permission. Score two for the updated concept of privacy.

The Internet

In the 1980s and early 1990s, while lawmakers in Europe and Canada passed comprehensive privacy legislation complete with commissioners and enforcement mechanisms, the United States adopted a piecemeal approach. Some databases had legally mandated privacy guarantees; others didn't. Wiretapping required a warrant--except when companies taped employees for the purpose of "improving customer service." But even if policies weren't consistent, they basically covered most situations that arose.

Then came the Internet's explosive growth--a boon to community, commerce, and surveillance all at the same time. Never before had it been so easy to find out so much, so quickly. But while most Internet users soon became dependent on services from companies like Yahoo and Google, few realized that they themselves were the product these companies were selling.

All activity on the Internet is mediated--by software on your computer and on the remote service; by the remote service itself; and by the Internet service providers that carry the data. Each of these mediators has the ability to record or change the data as it passes through. And each mediator has an incentive to exploit its position for financial gain.

Thousands of different business models bloomed. Companies like Doubleclick realized that they could keep track of which Internet users went to which websites and integrate this information into vast profiles of user preferences, to be used for targeting ads. Some ISPs went further and inserted their own advertisements into the user's data stream. One e-mail provider went further still: it intercepted all the e-mail from Amazon.com to its users and used those messages to market its own online clearinghouse for rare and out-of-print books. *Whoops*. That provider was eventually charged with violating the Federal Wiretap Act. But practically every other intrusive practice was allowed by the law and, ultimately, by Congress, which was never able to muster the will to pass comprehensive Internet privacy legislation.

It's not that Congress was shy about regulating the Internet. It's just that congressional attention in the 1990s was focused on shielding children from online pornography--through laws eventually found unconstitutional by the Supreme Court, because they also limited the rights of adults. The one significant piece of Internet privacy legislation that Congress did manage to pass was the Children's Online Privacy Protection Act (COPPA), which largely prohibited the intentional collection of information from children 12 or younger.

Instead, it fell mostly to the Federal Trade Commission to regulate privacy on the Internet. And here the commission used one primary tool: the FTC Act of 1914 (since updated), which prohibits businesses from engaging in "unfair or deceptive acts or practices." The way this works in connection with online privacy is that companies write "privacy policies" describing what they do with personal information they obtain from their customers. Companies that follow their policies are fine--even if they collect your information and publish it, sell it, or use it to send e-mail or for "any other lawful purpose" (and the law is pretty tolerant). The only way for companies to get in trouble is to claim that they will honor your privacy in a specific manner and then do something different.

Hearings were held at the end of the Clinton administration to pass some online privacy legislation with real teeth. I testified in favor of strong regulations at one of those hearings, but sitting next to me at the witness table were powerful business interests who argued that regulation would be expensive and hard to enforce. The legislation didn't go anywhere. Business groups saw this outcome as the triumph of their "market-based" approach: consumers who weren't happy with a company's privacy stance could always go elsewhere. Privacy activists winced, knowing that legislation would be unlikely to pass if the Republicans won in 2000. We had no idea how right we were.

9/11: The First National Scare of the Computer Age

The terrorist attacks of September 11, 2001, changed the terms of the debate. Suddenly, the issue was no longer whether Congress should protect consumer privacy or let business run wild. Instead, the question became: Should Congress authorize the Bush administration to use the formidable power of state surveillance to find terrorists operating inside the United States and stop them before they could carry out their next attack?

The administration itself had no doubts. Where laws protecting privacy got in the way of its plans to prevent attacks, it set out to change those laws. The pinnacle of this effort was the USA Patriot Act, signed on October 26, 2001, which dramatically expanded government power to investigate suspected terrorism. In the months that followed, representatives for the administration repeatedly denounced those who complained about threats to privacy and liberty; they were, said Attorney General John Ashcroft, "giv[ing] ammunition to America's enemies."

It was a strong, simple, and remarkably effective message--so effective that we know of only a few cases in which Congress pushed back. The first and most public such case involved a Department of Defense research project called Total Information Awareness (TIA).

Soon renamed Terrorism Information Awareness, TIA was the brainchild of the Defense Advanced Research Projects Agency's newly created Information Awareness Office, which was run by retired admiral John Poindexter (a former national security advisor) and his deputy, Robert L. Popp. The idea, which drew heavily on both men's earlier work in undersea surveillance and antisubmarine warfare, was to use new advances in data mining and transactional analysis to catch terrorists while they were planning their attacks.

One way to find submarines is to wire the ocean with listening sensors and then to try to filter the sounds of the sea to reveal the sounds of the subs. The terrorist problem is similar, Poindexter explained at the 2002 DARPATech conference. The key difference is that instead of being in an ocean of water, the terrorists were operating in an ocean of data and transactions. "We must find terrorists in a world of noise, understand what they are planning, and develop options for preventing their attacks," he said in his published remarks.

The approach isn't so far-fetched. Consider that the 1995 Oklahoma City bombing used explosives made of fertilizer and fuel oil, delivered in a rented Ryder truck. One way to stop similar plots in advance might be to look for people other than farmers who are purchasing large quantities of fertilizers used in making bombs--with extra points if the person (or one of his friends) has also rented a moving truck.

That task will be made a bit easier when stores that sell ammonium nitrate are registered with the Department of Homeland Security (a federal law to that effect was passed in 2007). Still: even when we have such registration, the prevention of an attack using fertilizer will require real-time purchase information from every fertilizer seller in the United States.

While I was a graduate student at MIT during the summer of 2003, I got a job working on the TIA project, because I thought that data mining would be a way to objectively look through mountains of personal information without compromising privacy. Congress, however, opposed TIA on the grounds that it treated everyone in the country as a suspect, and because it feared that a massive data surveillance system might be used for purposes other than catching terrorists. This prospect was not so hypothetical: in 1972 Richard Nixon had ordered the IRS to investigate his political opponents, including major contributors to George McGovern's presidential campaign. (Many believe that opposition to TIA was also a kind of payback against Poindexter, who had been convicted of lying to Congress in the Iran-Contra scandal of the 1980s but had his conviction overturned on appeal.) Congress defunded the program in 2003.

TIA was never more than a research project. But other initiatives were moving ahead at the same time.

For example, in 2002 officials from the Transportation Security Administration asked JetBlue Airways to provide detailed passenger information to Torch Concepts, a company in Huntsville, AL, that was developing a data mining system even more invasive than the one envisioned by DARPA. JetBlue was eager to help: five million passenger records were transferred. The records, which included passenger names, addresses, phone numbers, and itineraries, were then combined, or "fused," with a demographic database purchased from a marketing services company called Acxiom. That second database specified passengers' gender, income, occupation, and Social Security number; whether they rented or owned their home; how many years they had lived at their current address; how many children they had; how many adults lived in their household; and how many vehicles they owned.

Torch Concepts identified "several distinctive travel patterns" in the data and concluded that "known airline terrorists appear readily distinguishable from the normal JetBlue passenger patterns," according to a company PowerPoint presentation unearthed by travel writer and privacy activist Edward Hasbrouck and publicized by Wired News on September 18, 2003. A media uproar ensued, but a 2004 report from the Department of Homeland Security ultimately concluded that no criminal laws had been broken, because JetBlue provided the data directly to Torch and not to the federal government. (JetBlue did violate its own privacy policy, however.)

Another data fusion project launched in the wake of 9/11 was the Multistate Anti-Terrorism Information Exchange (Matrix), which was also shut down amid privacy concerns. According to a report by the DHS Privacy Office, the system was designed to allow law enforcement agencies in different states to easily search one another's computers, although the system "was over-sold as a pattern analysis tool for anti-terrorism purposes." The report found that Matrix was late in forming its privacy policy and that it "lacked adequate audit controls." Public support fell off, states pulled out, and the project was terminated.

Since then, a number of states and cities have partnered with DHS to create so-called "fusion centers," with the goal of helping sensitive information flow between federal, state, and even local law enforcement agencies. There were 58 fusion centers around the country by February 2009, according to the department's website, and DHS spent more than $254 million to support them between 2004 and 2007.

Few details of what actually happens at these centers have been made public. But in April 2008, Jack Tomarchio, then the department's principal deputy undersecretary for intelligence and analysis, told the Senate Committee on Homeland Security and Governmental Affairs that information from two U.S. fusion centers had been passed to a foreign government, which set up a terrorism investigation as a result. "DHS received a letter expressing that country's gratitude for the information," he testified. "This information would not have been gleaned without state and local participation."

At least in the eyes of the Bush administration, sacrificing the privacy of Americans to the security of the country had proved well worthwhile. But now the pendulum is swinging back, showing once again that our republic values privacy and will act to protect it from abuses--eventually.

Facebook
Here's a kōan for the information age: Why do so many privacy activists have Facebook pages?

Originally conceived as a place for Harvard undergraduates to post their photos and cell-phone numbers--information that Harvard, because of privacy concerns, wasn't putting online back in 2003--Facebook has grown to be the fourth-most-popular "website" in the world, according to the Web services firm Alexa. But Facebook is really a collection of applications powered by private information: a smart address book that friends and business contacts update themselves; a (mostly) spam-free messaging system; a photo-sharing site. And on Facebook, developers write seamlessly integrated applications.

These applications are troubling from a privacy perspective. Say you want to complete one of those cool Facebook surveys. Click a button and you'll be taken to a page with the headline "Allow Access?" Then you'll be told that using the application allows it to "pull your profile information, photos, your friends' info, and other content that it requires to work." How much information? There's no way to be sure, really--perhaps everything you've put into Facebook.

The roughly one in five Internet users who spend an average of 25 minutes each day on Facebook implicitly face a question every time they type into a Facebook page: Do they trust the site's security and privacy controls? The answer is inevitably yes.

That's the reason privacy activists are on Facebook: it's where the action is. It's easy to imagine a future where most personal messaging is done on such platforms. Activists and organizations that refuse to take part might find themselves irrelevant.

It was in a similar context that Scott McNealy, then CEO of Sun Microsystems, famously said, "You have zero privacy anyway. Get over it." In January 1999, McNealy was trying to promote a new technology for distributed computing that Sun had cooked up--an early version of what we might call "cloud computing" today--and reporters were pestering him about how the system would protect privacy. Four and a half years later, he told the *San Francisco Chronicle*, "The point I was making was someone already has your medical records. Someone has my dental records. Someone has my financial records. Someone knows just about everything about me."

Today it's not just medical and financial records that are stored on remote servers--it's everything. Consider e-mail. If you download it from Post Office Protocol (POP) accounts, as most Internet users still did in 1999, the mail is copied to your computer and then deleted from your ISP's servers. These days, however, most people use Web mail or the Internet Message Access Protocol (IMAP), which leaves a copy on the server until it is explicitly deleted. Most people don't know where that server is--it's just somewhere "in the cloud" of the Internet. [*Editor's note: see our Briefing on cloud computing (http://www.technologyreview.com/briefings/cloud/)* .]

Services like Facebook, Gmail, and Google Docs are becoming wildly popular because they give users the freedom to access their data from home and from work without having to carry it back and forth. But leaving your data on some organization's servers creates all sorts of opportunities for mishap. The organization might have a bad employee who siphons out data for personal profit. Cyberthieves might break into its servers and try to steal lots of people's data at the same time. Or a hacker might specifically target yourdata and contact the organization, claiming to be you. All these are security threats--security threats that become privacy threats because it's *your data*.

Where We Are Now

I have spent a good part of my professional life looking for ways to make computer systems more secure, and I believe that many of the problems we face today are not only tractable--many of them have already been solved. The threat of data theft by insiders can be mitigated by paying employees enough, auditing their work, limiting the amount of authority that any one employee has, and harshly punishing any individual who abuses the employer's trust. Computer systems can be made immune to buffer-overflow attacks, one of the most common security vulnerabilities in recent years, by programming them in modern languages like Java and Python instead of 1980s standards like C and C++. We really do know how to build secure systems. Unfortunately, these systems cost more to develop, and using them would require us to abandon the ones we already have--at least for our critical applications.

But one fundamental problem is harder to solve: identifying people on the Internet. What happens if somebody impersonating you calls up a company and demands access to your data?

If Google or Yahoo were storefronts, they would ask to see a state-issued ID card. They might compare a photo of you that they took when you opened the account with the person now standing in their lobby. Yes, there are phony IDs, and there are scams. Nevertheless, identification technology works pretty well most of the time in the physical world.

It turns out that we essentially have the technology to solve this problem in the digital world as well. Yet the solutions that have been developed aren't politically tenable--not only because of perceived costs but also, ironically, because of perceived privacy concerns.

I understand these fears, but I think they are misplaced. When someone can wreak havoc by misappropriating your personal data, privacy is threatened far more by the lack of a reliable online identification system than it would be by the introduction of one. And it is likely that it would cost society far more money to live with poor security than to address it.

I believe that we will be unable to protect online privacy without a strong electronic identity system that's free to use and backed by the governments of the world--a true passport for online access. One of the fundamental duties of government is to protect the internal security of the nation so that commerce can take place. For hundreds of years, that has meant creating identification documents so that people can prove their citizenship and their identity. But the U.S. government has abdicated its responsibility in the online world, and businesses have made up their own systems--like asking for your Social Security number and address, and perhaps your favorite color.

The difficulty of identifying people in the electronic world is a problem for every single company, every single organization, every single website. And it is especially a problem for Facebook and Google, because at a very basic level, they don't know who their customers are. When you open an account at a bank, U.S. law requires that you prove your identity with some state-issued identification. Bank accounts are linked to an actual identity. But electronic accounts like those on Facebook and Google aren't. They *project* an identity, but they aren't linked, really, to anything. That's a real problem if some hacker takes over your Gmail account and you need to get it back.

One solution would be to make driver's licenses and other state-issued IDs usable online by adding electronic chips. Just imagine: no more passwords to access your bank account, to buy something at Amazon, or to bid on eBay. Just insert your card. And if you lost the card, you could report it missing and get a new one. Instantly, all your online accounts would recognize the new credential and refuse to honor the old one.

Similar proposals have been made in the past: in the 1990s the U.S. Postal Service began working toward a system called the "U.S. Card." But the project never really got off the ground--partly because the technology wasn't quite ready, but also because of significant public opposition. In fact, in the United States every attempt to improve identification credentials has provoked significant public opposition. Many privacy activists see mandatory ID cards as one of the hallmarks of a police state. And many state governments fear the costs.

Though a stronger identification system would undoubtedly harm some citizens through errors, I think the opposition is unfortunate. We're already being identified every time we use an online banking service, or make an online purchase, or even use Facebook. We're just being identified through ad hoc,broken systems that are easy for bad guys to exploit. If we had a single strong identity system, we could adopt legislation to protect it from inappropriate use. A California law enacted in 2003, for example, prevents bars, car dealers, and others from collecting information swiped from a driver's license for any purpose other than age verification or license authentication.

For more than 100 years, American jurisprudence has recognized privacy as a requirement for democracy, social relations, and human dignity. For nearly 50, we've understood that protecting privacy takes more than just controlling intrusions into your home; it also requires being able to control information about you that's available to businesses, government, and society at large. Even though Americans were told after 9/11 that we needed to choose between security and privacy, it's increasingly clear that without one we will never have the other.

We need to learn how to protect privacy by intention, not by accident. Although technology can help, my belief is that such protections need to start with clearly articulated polices. Just as Nixon created the Environmental Protection Agency to protect our environment, we need some kind of Privacy Protection Agency to give our rights a fighting chance. Our piecemeal approach is no longer acceptable.

Simson Garfinkel is an associate professor at the Naval Postgraduate School in Monterey, CA. The views expressed in this article are those of the author and do not necessarily reflect the views of the U.S. government or the Department of Defense.

Upcoming Events

Lab to Market Workshop (http://www.technologyreview.com/emtech/09/workshop.aspx)
Cambridge, MA
Tuesday, September 22, 2009
http://www.technologyreview.com/emtech/09/workshop.aspx (http://www.technologyreview.com/emtech/09/workshop.aspx)

EmTech 09 (http://www.technologyreview.com/emtech)
Cambridge, MA
Tuesday, September 22, 2009 - Thursday, September 24, 2009
http://www.technologyreview.com/emtech (http://www.technologyreview.com/emtech)

Nanotech Europe 2009 (http://www.nanotech.net)
Berlin, Germany
Monday, September 28, 2009 - Wednesday, September 30, 2009
http://www.nanotech.net (http://www.nanotech.net)

2009 Medical Innovation Summit (http://www.ClevelandClinic.org/innovations/summit)
Cleveland, OH