iSpy: Threats to Individual and Institutional Privacy in the Digital World

Lori Andrews
fire up my laptop and compose a memo to my co-counsel about a pro bono case we are considering filing against a biotechnology company. I attach it to an email and send it to him, carefully writing “Confidential—Legal Mail” in the subject line and putting a few key ideas in the text of the email. Then I log on to the Southwest Airlines website, enter my credit card information, and buy a ticket for Washington, DC. I check my emails and click through to a website that lists job openings for university professors. One listing is in a town I haven’t heard of, so I Google it to find out if it will be urban enough for me. The town’s name brings up a link to a local newspaper article about a poisoning. I Google that toxin and save the information about it to my hard drive, thinking I might use it in the next mystery book I write. I read an email from my doctor telling me she changed my prescription electronically and the new drug is waiting for me at my neighborhood CVS. I check my Facebook page and see that someone has tagged me in a Halloween
Photo from years ago, when I was a Yale undergrad. I am wearing a belly dancer’s costume and I am with someone dressed like a bottle of Imperial Single Malt Scotch. I untag myself from the photo. If I do interview for a new job, I don’t want someone to say to me, “Well, Ruth Bader Ginsburg would never have shown her navel.”

All in all, I feel good about the security of my morning’s travels across the web. I haven’t responded to any wealthy widows seeking my legal help for their $50 million estates, nor to emails purportedly from friends whose wallets and passports were stolen in London. I haven’t given my credit card to anyone with a sketchy foreign email address who offers me an iPad for $30, nor have I opened the missive that tells me I’ve exceeded my email limit. I’ve only dealt with websites I trust.

However, every action I’ve taken has been surreptitiously chronicled and analyzed by data aggregators—companies that collect information about which websites people visit, what they post on social media, and what internet searches they undertake. The aggregators then sell the information to government and private institutions, including potential employers, insurers, and marketing companies.

**PROTECTING YOUR PRIVACY**

- **Use private browsing.** If you perform a search using Google Search or Microsoft’s Bing, those companies can amass detailed information about your personal interests and browsing habits. StartPage.com and DuckDuckGo.com, on the other hand, are two search engines that do not keep information about your searches. Nevertheless, the websites you visit will know your internet protocol (IP) address, so true privacy cannot be maintained unless that address can be disguised, for example by using Tor, which makes it appear that your search is coming from an IP address that is not your own. Many Massachusetts libraries have installed Tor anonymizing software on their computers. Anne Klinefelter, associate professor of law and director of the law library at the University of North Carolina School of Law, additionally suggests that libraries should be careful not to position security cameras so that patrons’ searches can be seen.

- **Understand what your devices and programs do and use the right privacy settings.** Microsoft 10 eavesdrops on you, keeping your microphone on at all times. However, you can control which apps have access to the device’s microphone in the ‘Privacy’ settings window. Simply click on ‘Microphone’ and slide the master toggle to ‘Off.’ If you want to use Skype or another conferencing app with audio, slide the toggle to the ‘On’ position for just the app for which you would like to use the microphone.

- **Do not use the default password that comes with a device that connects to the internet.** If you buy a modem or baby monitor or other device (even a refrigerator!) that connects to the internet, change the password that comes with it to a new one that you create. Otherwise, hackers can use the default ones to gain access to your device.

- **Use a browser setting that signals that you don’t want to be tracked.** A ‘Do Not Track’ setting is available in Firefox, Chrome, Safari, Edge, and Internet Explorer. This tells the websites you visit that you don’t want to be tracked, but not all websites honor that request.
“Big Brother” Is Watching

Data aggregation is big business. Axiom, which made $850 million in 2016, has data on half a billion people from around the world, including 96 percent of Americans. In The Filter Bubble: What the Internet Is Hiding from You, Eli Pariser notes that the company has an average of 1,500 pieces of data on each person, “everything from their credit scores to whether they’ve bought medication for incontinence.”

Google made $74.54 billion in 2015, 90.4 percent of which was from aggregating people’s private information for advertising. Just imagine how much marketable information Google knows about you. Depending on what services you use, Google knows what you look like (Google+), who your friends are (Google+ and Gmail), your personal appointments (Calendar), correspondence (Gmail), and work and personal documents (Google Docs).

Google knows what videos you watch on YouTube and what search strings you’ve entered into its search engine. If you use an Android phone, Google knows who you call and for how long. With the growing Internet of Things—your devices, programs, and the objects around you—the capability to add to your digital profile has increased. People’s private conversations have been recorded and categorized by their smart TVs and by interactive toys like Hello Barbie. The billboards you drive by have begun tracking you. Clear Channel Outdoor Americas can now lock into your phone’s Bluetooth to assess whether, after you pass a billboard, you go to the liquor store advertised on the billboard. If your phone carrier is the same as your cable company, it can even learn if you later watch the television show advertised on a billboard.

Some third-party use of your information is harmless or even beneficial—an ad for a jacket you’ve already purchased or hotel discount for the trip you’re planning. However, whether you can obtain a scholarship, a job, credit, or insurance can be based on your digital doppelganger—and you may never know why you’ve been turned down.

For example, if you’ve told your sister in an email that you are thinking of getting a divorce, a credit card company may use that information to deny you a card or lower your credit limit because, in the aggregate, people in the midst of a divorce are less likely to be able to pay off their credit cards. With troublesome stereotyping, you are treated not based on your individual actions or interests, but based on aggregate data.

Watch out librarians! Even something seemingly harmless like the fact you like to read a lot can be used against you. Deloitte Consulting LLP advocates using people’s online profiles to make judgments about life insurance underwriting, claiming it could save insurance companies an estimated $2 to $3 million a year and “shorten and reduce the invasive-ness of the underwriting” process. Consultants suggest that if you eat fast food, commute to work, or are an avid reader, you’re not a good candidate for life insurance.

Data Aggregation and Who Uses It

Data aggregation reinforces gender and racial stereotyping. In a 2015 Carnegie-Mellon study, researchers created fake online profiles and used them to apply for jobs. Queries from the 500 male profiles were nearly six times more likely to elicit ads for high paying executive jobs than queries from the 500 female profiles.

Further, private companies are not the only entities that gain access to your digital profile. Government agencies, including the Internal Revenue Service and Homeland Security, judge you based on what you do online. A 2015 study by the International Association of Chiefs of Police surveyed 553 law enforcement agencies from 44 states and found that 88.7 percent of the agencies used social networks in criminal investigations.

Amazingly, courts have said that such data aggregators’ surreptitious snooping doesn’t violate federal laws prohibiting unauthorized access to, or wiretapping of, computers. According to a 2010 New York opinion, the right to privacy “is lost, upon your affirmative keystroke.” Courts have decided that if a website you visit consents to a marketing company secretly putting a cookie on your computer, you can’t sue that company under federal law. The courts have held that the website’s consent is sufficient. However, shouldn’t it be the consent of the person whose personal information is being collected that is considered—not the consent of the entity profiting from that surreptitious activity?

In addition, by agreeing to an app or website’s terms of service or privacy policy stating that the developer sells your information, you are affirmatively giving your consent to be tracked and commodified. Yet who has the time to read (or challenge) those hard-to-access, hard-to-understand legal documents? Lorrie Faith Cranor and Aleecia McDonald of Carnegie-Mellon estimated that it would take 76 work days to read all the privacy statements applicable to the apps, social networks, and digital devices that we commonly use. Nationally, that adds up to $781 billion dollars of opportunity costs due to reading privacy statements.

Is This Legal?

Should we really let companies require us to give up the Constitutional right of privacy to use their services? Would we allow a phone company to require that we give up the right to vote or the right to reproduce to use its services? Moreover, what about the 20 million children under the age of
TOP TIPS FOR PROTECTING YOUR INSTITUTION FROM HACKS

Even if you protect your own privacy and that of your patrons, your institution itself might be hacked. A 2016 article in The Wall Street Journal reported that major law firms, including Cravath and Weil Gotshal, had been hacked. Similarly, universities have been vulnerable to attacks from hackers seeking students’ social security numbers and credit card information. One of their ruses (used at Bucknell): a fake email from the university library.

University of Illinois at Chicago computer science professor Robert H. Sloan and IIT Chicago-Kent College of law professor Richard Warner, authors of Unauthorized Access: The Crisis in Online Privacy and Security, provide this advice for a security risk assessment:

- **Personnel**: Are they adequately trained or easy targets for phishing and other forms of social engineering? Social engineering is the technique of choice for the initial entry into a network.
- **Data**: What data is most likely to be a target for hackers? Concentrate defenses there.
- **Software**: Is all software up to date? What are the known risks of using your software?
- **Network**: What are your defenses? Where are they? Separate your network; for example, social security numbers should be separated from acquisitions information.
- **Third parties**: Make sure there are privacy provisions in contracts so that contractors don’t enable breaches.
- **Consider hiring outside security experts**: Network defense is highly technical and demanding in terms of time and equipment. Outsourcing to an entity such as Cloudflare makes sense in many cases.

18 who have profiles on social networks? How can they even bind themselves to such a contract?

My opinion is that people should have a right to decide whether or not they want their information collected, and that use of a website or an app should not be conditioned on giving up one’s right to privacy. Further, rather than letting the website or app developer contract away your privacy rights, there should be a completely separate digital entity where people can register to be contacted by marketers they value. If you want to get that Macy’s coupon or the latest information about a new beer, you could choose to be contacted directly by the entity, cutting out the expensive marketing middleman and saving the time you otherwise would have spent reading privacy statements.

In other countries, people have a right to advance notice, to control and to correct information. In Europe, when a person’s personal data is collected, the parties responsible for the collection are required to inform the person who they are, why they collected it, and for whom it was collected. If entities use a person’s
data in any way, they are required to supply a copy of the data to the person in an “intelligible form” along with all the available information they have about the source of that data. If any part of the data is inaccurate or unlawfully processed, the person has the right to ask that they make a correction, a deletion, or completely erase the data. The European Union also has a directive that requires that entities not collect more data than they need for a particular transaction; they must ensure that the data is accurate and complete, and that identifiable databases are kept “no longer than is necessary for the purposes for which the data were collected.”

The Future of Internet Privacy

There are no U.S. laws that require data aggregators to reveal what they know about you. I’ve Googled “diabetes” for a friend and “poisons” for my mystery novel; data aggregators assume those searches reflect my own health and proclivities.

The closest analogy to the European approach in U.S. law is the Fair Credit Reporting Act, which allows people to challenge false information in credit reports. In 2016, the U.S. Supreme Court heard the case of Spokeo v. Robins, in which Thomas Robins sued the data aggregator/public search engine Spokeo for distributing false information about him. Spokeo had reported that he was a wealthy 50-year-old with a master’s degree, a wife, and children. None of this was true. Robins alleged he was denied interviews for jobs because employers mistakenly viewed him as overqualified. The Court, in a 6-2 decision, remanded the case for a determination of whether Robins had suffered a “concrete” enough harm. Justices Sotomayor and Ginsburg dissented, arguing that incorrect facts can result in real harm. At oral argument, Justice Sotomayor gave the example of dating, where a woman might choose not to date someone she thinks is married.

With federal statutes providing so little protection, some consumers have turned to state law to protect their rights. In California, consumers sued the company NebuAd, which paid 26 internet service providers to install NebuAd’s hardware on those internet service providers’ networks without ISP users’ consent. The hardware allowed NebuAd to use deep packet inspection—a mechanism to intercept and copy all the online transmissions of the ISPs’ subscribers and transmit them to NebuAd’s headquarters.

In April 2011, a California federal judge considered a suit by consumers against NebuAd. The data aggregator had tried to get the suit dismissed, saying that since it wasn’t liable under federal law, it couldn’t be liable under state law. The judge, though, let the lawsuit go forward under that state’s invasion of privacy law and the state’s computer crime law. In this period of a profound shift in policies with a new presidential administration, state law may be the best legal means to protect one’s privacy.

The internet is not the first technology to challenge privacy. Before 1888, when Kodak introduced a portable camera, taking someone’s photo was a big deal. A person would get dressed up and go to a studio. Photos were not taken without a person’s permission. However, the portable camera changed all that. A newspaper article in the Hawaiian Gazette in 1890 read:

> Have you seen the Kodak fiend? Well, he has seen you. He caught your expression yesterday while you were in recently talking at the Post Office. He has taken you at a disadvantage and transfixied your uncouth position and passed it on to be laughed at by friend and foe alike.

Two lawyers at the time, Samuel Warren and Louis Brandeis, began to assess the impact of the portable camera on modern life. They could have suggested that people no longer had a right to be left alone because technologies could now track and record what they did. Instead, they noted that the intrusiveness of technologies made it even more important for people to have control over information about themselves. Without a right to digital privacy, our freedom of speech and freedom of association cannot be exercised.

AALL 2017 ALERT

Don’t miss the session “Understanding Security Threats to Better Collaborate,” Tuesday, July 18 from 8:30 a.m.–9:30 a.m. For more information visit bit.ly/AALL17Security.

AALL2go EXTRA

Watch the “iSpy: Hot Topics in Internet Privacy” webinar at bit.ly/AALL2goPrivacy.

Lori B. Andrews

UNIVERSITY DISTINGUISHED PROFESSOR OF LAW
DIRECTOR OF THE INSTITUTE FOR SCIENCE, LAW AND TECHNOLOGY
Illinois Institute of Technology (IIT) Chicago-Kent College of Law
Chicago, IL
landrews@kentlaw.iit.edu

Lori B. Andrews is a distinguished professor of law at IIT Chicago-Kent and director of IIT’s Institute for Science, Law and Technology. She received her bachelor’s summa cum laude from Yale College and her JD from Yale Law School. Andrews is an internationally recognized expert on biotechnologies, and was listed as a “Newsmaker of the Year” in the January 2008 issue of the ABA Journal. She is the author of 14 books, including I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy, and more than 100 scholarly articles, monographs, and book chapters on subjects including informed consent, medical genetics, and health policy.