THE CHRONICLE OF HIGHER EDUCATION

Back to Search Results

THE CHRONICLE REVIEW

The Electronic Panopticon

Tim Foley for The Chronicle Review

By Neil Richards | MARCH 16, 2015

Is the web private enough for you? Maybe you're OK with every search you've made, every site visited, every email sent all being stored in databases linked to your name or account by your service provider, your phone carrier, or Google. Maybe you're OK with Amazon knowing not just what's in your Kindle library but also what you've actually read from it, and when. Maybe you're OK with that data not just being stored in the cyberequivalent of a dusty warehouse, but vigorously sought after, bid on, and pursued through coercion by marketers, the police, and spies eager to know you better. Not to mention the aggregated identity and financial information compromised repeatedly by hackers breaching the firewalls of retailers, banks, and government agencies.

It's just the cost of doing business, right? The trade-off for convenience and safety.

Really? The web is little more than 25 years old. Are we already fatalistically resigned to the intrusiveness that accompanies this infant technology? We shouldn't be. We should be outraged that the Internet carries with it so much prying, that it has become an electronic panopticon. But to curb these tendencies, we have to channel our indignation into a unified political voice. We must let policy makers and corporate chiefs know that electronic privacy is a primary concern, one that factors into our values, our votes, and our spending.

Freedom of thought and freedom of speech are our most valuable civil liberties because on them depend our lifelong intellectual and emotional development and satisfaction. Sampling ideas, viewpoints, and aesthetics without being unduly judged by or associated with them are part of

learning, maturing, becoming individuals, figuring out the world on our own terms. We need the free, unmonitored ability to think, read, and speak with confidants before presenting our ideas for public consumption.

That freedom is an idea with very old roots in our law and culture, and it is the basis for democratic self-government, individuality, diversity, and, yes, also the eccentricity, the vibrant weirdness, that often makes life so delectable.

When we are watched, when we even sense that we might be watched, we act differently. Writers and critics from Bentham to Orwell to Foucault have explored how surveillance drives our behavior toward the boring, the bland, the mainstream.

A growing body of empirical evidence supports these insights. One study at a British university measured the money its tea-drinking professors put into a contribution box for shared milk. The reminders to chip in were changed: The words stayed the same, but the background graphic was switched from flowers one week to eyeballs the next. The penetrating gaze of the eyeballs spurred significantly higher contributions. Other studies have documented the normalizing effects of surveillance in such contexts as drug testing and police ethics. Results are unequivocal: When we are watched, we "behave," whatever that means in context.

Surveillance is warranted where it deters police brutality, but we shouldn't deter new or unpopular ideas. In a free society, there is no such thing as a thought crime. Orwell's warnings about surveillance are particularly resonant here. A recent study at MIT found that after the Snowden revelations, Google users searched far less for the sorts of terms ("dirty bomb" or "homeland security") that might raise the attention of the U.S. government. More important, it found, the awareness that web searches might be monitored also apparently led people to search less about things having nothing to do with terrorism but that were just personally sensitive or embarrassing ("body odor," "coming out," "divorce lawyer," "erectile dysfunction"). Being watched deters us from the kind of free and fearless inquiry on which political and personal freedoms depend.

Three aspects of intellectual privacy in particular need to be zealously guarded: freedom of thought, the right to read, and confidential communications. Each of these ancient liberties is threatened by new digital technologies and practices.

Freedom of thought: your ability to think and believe what you want, no matter how radical or weird. If any human right is absolute, it is this one. Supreme Court Justice Benjamin Cardozo once called it "the matrix, the indispensable condition, of nearly every form of freedom." The prohibition on thought crimes is reflected in both the Fourth Amendment's protection of "papers" and the Fifth Amendment's protection against self-incrimination. These foundational Bill of Rights guarantees made it much harder to haul radical diarists or dissenting thinkers into court to answer for their beliefs. But our thoughts, once safely hidden in our heads, have started to be revealed by digital technology. As we increasingly use search engines to ask questions or cloud servers to store our documents, we create digital echoes and copies of those thoughts. When we use search engines, we are thinking with the aid of technology. And when the National Security Agency's surveillance chills our searches, it curbs our freedom of thought.

Protecting free speech is no good if surveillance stops us from thinking up anything new or original to say.

The right to read is equally fundamental. Making sense of the world requires access to the ideas that other people have written down. Librarians have long protected their patrons' reading habits, and those professional ethics have been backed up by law. But new technologies create new kinds of records. When the Supreme Court nominee Robert Bork's movie-rental history was disclosed by a Washington video store, Congress quickly passed the Video Privacy Protection Act, which protects not just old records of VHS rentals but also the confidentiality of your Netflix queue. Bizarrely, though, in most states records of book sales are unprotected. So when *Fifty Shades of Grey* became a best seller on e-books, it happened under an illusion of reader privacy. No one on the subway might have known what you were reading on your Kindle, but Amazon did, down to the time you read each page and which ones you might have reread.

Once we have read and thought, we often want to consult our friends to see if our ideas are important, just a bit crazy, or both. Letters have long been protected by both the Fourth Amendment and ancient laws protecting postal privacy. But most modern communications are electronic. The Supreme Court ruled in 1967 that we have a reasonable expectation of privacy in our phone conversations, and that the police must get a warrant

supported by probable cause before they listen in. Yet there remain open questions about whether the warrant requirement also protects emails or communication metadata. When it comes to digital technology, the confidentiality of our communications is up for grabs.

If we care about intellectual freedom and free speech, we must protect intellectual privacy. Protecting free speech is no good if surveillance stops us from thinking up anything new or original to say. We want to be safe, and we don't want to regulate businesses needlessly, but sensitive data about our mental activities need special protection. We'll have some choices to make as we update our laws, but we can create a world in which we have both intellectual privacy and the many benefits of our digital tools.

First, we should interpret the Fourth Amendment to make search results confidential and to require warrants before the government obtains records of Internet searches. When users can trust that sensitive data regarding their thoughts are held securely, they will search more fearlessly, with more confidence in and greater loyalty to their digital intermediaries. Privacy can be good for business, as companies like Mozilla, DuckDuckGo, Apple, and Microsoft are starting to argue.

We should treat records of both digital and paper reading as confidential, as we have done with library and video-rental records. Companies like Amazon provide a helpful service when they recommend books and movies to us on the basis of information we have shared about our preferences, but such data should be used only to help the customer. The information should not be put toward influencing preferences, or sold to the highest bidder, or potentially used for blackmail, as Uber is alleged to have contemplated to silence its critics.

Communications data, including metadata, should also be better protected. We should be able to trust that our digital communications are secure, and that the government can intrude on private confidences only when it establishes probable cause that the parties are involved in crime. Blanket warrantless surveillance of the conversations or metadata of a free people chills discussion and is ultimately inconsistent with self-government.

We must ensure that intellectual privacy is a basic norm of digital life. We should compel our elected representatives to impose fundamental rules of fairness on the companies whose tools increasingly affect our lives and political freedoms. As consumers, we should encourage companies to protect our privacy against the state through the use of encryption, and we

should reject government calls to weaken encryption through "back doors." A back door to our security services can be used by malicious hackers and criminals as well as by the state. Rather than weaken encryption, we should rely on impartial judges and the tested strengths of the legal process.

Some might argue that intellectual privacy, like other civil liberties, could make us less safe, that we must trade some liberty for security in a dangerous world. We should certainly strike a thoughtful balance — but one that preserves our ability to think, read, and communicate on our own terms. We already have tested methods for investigation and prosecution of crimes, ways that preserve the basic presumption that free people must be trusted with dangerous ideas and dangerous books.

And we already make trade-offs between freedom and safety in other areas. We allow people to drive fast cars and eat unhealthful cheeseburgers. We have chosen to live with the risk of car accidents and heart attacks. Such freedoms matter to us despite their dangers because, on balance, they make life better. In the seductive glow of our electronic age, let's not give away the far more crucial liberties of intellectual privacy.

Neil Richards is a professor of law at Washington University in St. Louis and the author of Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, *just out from Oxford University Press.*

1255 Twenty-Third St., N.W.
Washington, D.C. 20037