DOI:10.1145/2408776.2408784

Eben Moglen

Privacy and Security
The Tangled Web We Have Woven

Seeking to protect the fundamental privacy of network interactions.

THE LAST GENERATION is being born whose brains will develop independently of the Net. From now on, the way the Web works will play a dominant role in the socialization of the human race. But because we have built Web infrastructure without considering privacy, we are also endangering our basic freedoms. We are on the verge of eliminating forever the fundamental right to be alone in our thoughts.

At the beginning of the sixteenth century, moveable-type printing created the experience of private reading, and with it the Western idea of the individual self freely developed, self-made through a private process of reading and thinking. In religion, this led to the revolutionary adoption of individualist forms of Protestant Christianity. Secular society adopted the scientific method, and with it began radically improving the human social condition. The opening of learning also enabled the gradual transformation of the Western political landscape toward democratic self-government and the constitutional protection of freedom of thought.

The Net should now universalize that process throughout the human race, should make it possible for every person on Earth to read, watch, listen, and participate in every form of learning and culture, everywhere, without discrimination between rich and poor, old and young, male and female. This truly universal learning system would immeasurably improve the welfare of humankind. But if we do not protect the fundamental privacy of network interactions, if we permit not only active surveillance but also extensive data mining of personal information in the Net, we will not achieve that promise. Indeed, if the Net is not engineered to protect privacy, it will instead become a jail for the human body and the human soul.

We are on the verge of eliminating forever the fundamental right to be alone in our thoughts.

We are failing at present because our Net is being used to spy on us, constantly, as we use it to enrich our lives. The innovations in surveillance have come from industry. Record-keeping about how we use the Net—what we search for, what we read, who we contact—is intensively and instantaneously "mined" for its value to those who want to sell us something. What we share with our friends and family, even the content of our email and other private communications, is scrutinized to the same end by companies that offer us "services" in return for access to our private data. All this data, assiduously gathered by businesses seeking profit, no matter how responsibly they manage it, is also at the disposal of any government capable—by law, force, or fraud—of gaining their cooperation.

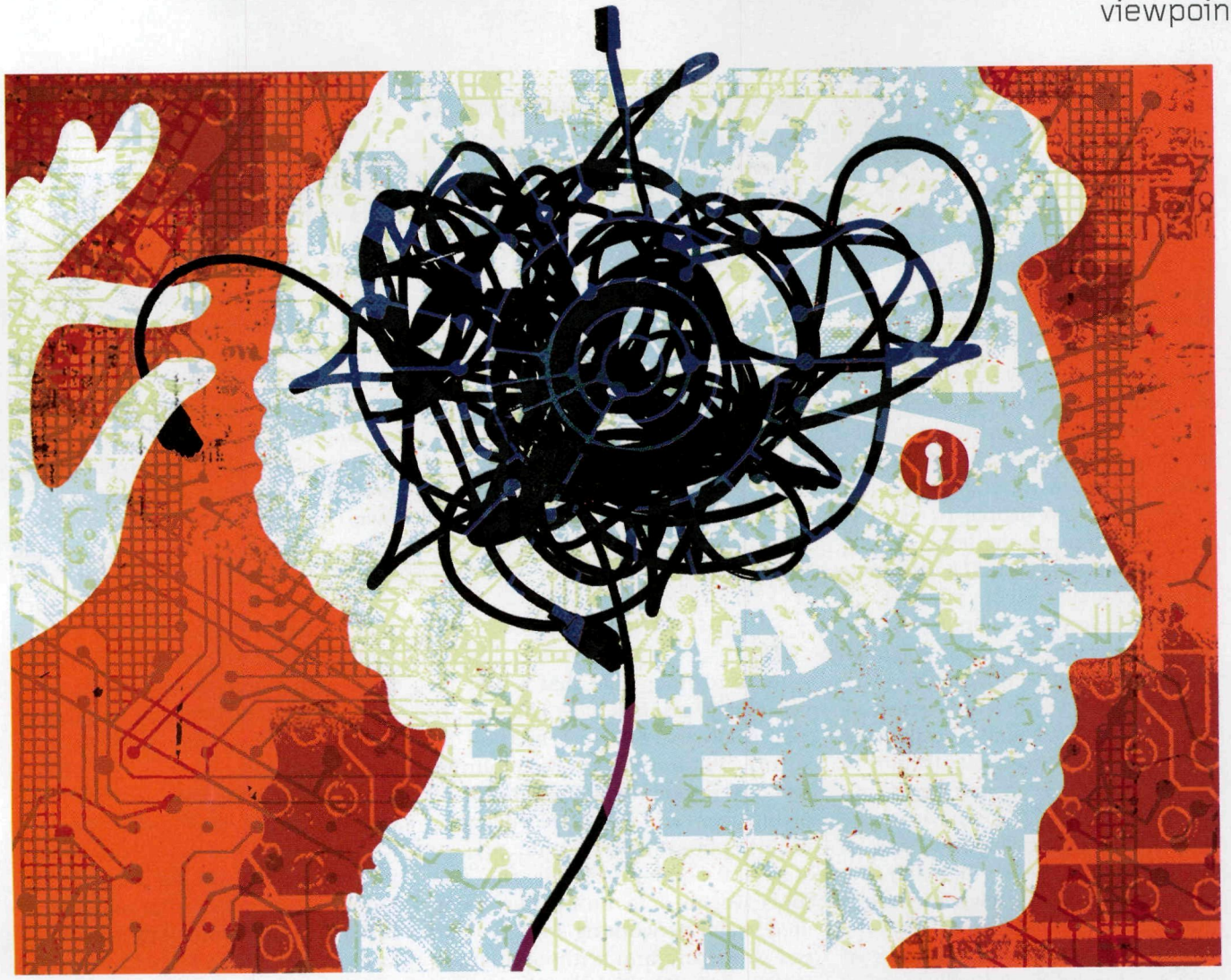

ILLUSTRATION BY GARY NEILL

Beyond the data itself lies the new mathematics of inferring from it. "Data mining," which now politely refers to itself as "data science," is a new subdiscipline of statistics, directed at using all this individually identifiable and aggregated behavioral data to predict human social action. Whether one is selling pharmaceuticals, toys, advertising placement, or a political candidate, data science is now using our personal data to help the seller identify, pursue, and persuade us. Our consumption supplies information that can be used to read our minds.

The situation is made still worse because we are rapidly adopting personal service robots that are not working exclusively in our interests. Unlike the robots living intermixed with humans in the science fiction of our childhoods, these robots have no hands and feet—we are their hands and feet. They see what we point them at; they have ears to hear everything going on around us; they know our location all the time. These robots we call smartphones and tablets often contain software we cannot read or understand, much less change. We do not control them; rather, they offer others the opportunity to control us.

Development in the private market of technologies to surveil, predict, and influence individuals through the Net has of course drawn the attention of states. Governments are rapidly moving, to the fullest extent of their differing means, to harness the power of big personal data to improve their social control. No matter what your politics, somewhere in the world, right now, a government of whose principles you completely disapprove is beginning to use the Net to locate support, influence the population, and find its enemies. Everywhere in the world, from now on, governments that become tyrannical will have immensely powerful new tools for remaining permanently in power.

This privacy crisis is ecological. The unintended consequences of tiny individual activities, aggregated over the vast scope of the Net, are producing a threat to our common human interests on a global scale.

Fortunately, because the parts of this crisis are all our creation, we can remedy the problem. We need to rebuild the operating software of the Net in keeping with certain ethical principles. This does not mean forcing people or businesses to change what they are presently doing. It means providing the equivalent of green technologies, and helping people shift to them.

First, then, we need to build responsible replacement software, providing existing functions in ways that respect users' privacy, to replace systems that are hazardous to privacy. Current webmail and social networking services, for example, put all their users' communications with their respective social circles inside huge centralized databases maintained by the service operator, who in return for doing the storing and providing sophisticated access services to users,

gets the right to mine the data, which is now centralized and vulnerable to government acquisition.

But email and the Web are by design *federated* services, in which individual servers can provide storage and access services cheaply, securely, and with near-perfect reliability for individual users. Users began using centralized services that hurt their privacy because they gained tangible convenience at no apparent cost. No one knew how to run her own mail server or Web server, and we did not make it easy to learn. But we can—and we should—help people to use free software and a coming flood of inexpensive "personal server" hardware to make personal privacy appliances.

The FreedomBox Foundation I am currently advising is an example of an attempt in this direction, making free personal privacy software for creating such appliances. Small, inexpensive, power-miserly devices you just plug in and forget, they keep your communications private, help you navigate the Web without being spied on, and let you share with the world, safely. Let me get technical for a few sentences to describe how.

Much of the implementation of such a software stack involves using existing free software tools. A privacy proxy located in the router between a user's smartphone or PC browser and the public Net can remove advertising and Web bugs, manage cookie flow, and improve browsing privacy and security by providing "HTTPS everywhere." Automating use of SSH proxies and personal VPNs can not only protect the privacy of Web access behind the FreedomBox used as a router, it can also provide secure communications and privacy-protected Web access from a mobile device used on untrusted networks away from home.

Some of the tools needed for personal privacy appliances are combinations of existing functionality. Combining a HTTPS Web server and a XMPP server with OpenPGP-based authentication, for example, along with a method for building the "web of trust" through exchange of public keys embodied in QR codes (the 2D barcodes that smartphones already scan) yields a method for secure text, voice, and video chat that is easy for ordinary users to deploy. That in turn also easily extends to a method for secure communication with journalists and public media outlets for relaying video and audio recorded with mobile phones. Beyond our present stage of development lie the new tools we need to build, like federated social networking software that can smoothly and without disrupting the web of social sharing replace Facebook and similar "services," that have imposed centralized storage, data mining, and control.

When we act to improve our own privacy we are also protecting the privacy of our children, our families, and our friends.

Soon, such privacy servers will be available to replace your home wireless router or other similar device at even lower cost, but with enormous overall social benefit. Think of them as personal coal-scrubbers that cost next to nothing and improve the atmosphere we all breathe.

But this is not all. We must also provide clear, factual, technical public education about privacy and "the cloud." Currently basic technical information is either altogether missing from or else distorted in the public debate. We need to help people understand why they might be better off storing their personal data on physical objects in their possession rather than in other peoples' data centers in "the cloud." We should make the results of "data science" accessible to a public that will never interest itself in the mathematics.

We must help people think ecologically about privacy. Users do not recognize that their correspondents' privacy is also reduced when they use a "free" email service that reads and data mines email sent and received. They do not realize that everyone in the photographs they post on centralized social networking services is being facially identified and tagged. That the social networking service's operator has access to all those pictures and all the tags, and so does anyone with whom the operator "cooperates." We need to explain that every little decision to give away one's own information also gives away other peoples'. We can teach people that when we act to improve our own privacy we are also protecting the privacy of our children, our families, and our friends. If we help people around us to understand the effects their actions have on others, they will decide for themselves what changes they should make.

Untangling the Web, restoring privacy in what we do and anonymity in what we read, will not be easy. Many fine businesses will make a little less money if we do not offer all our personal data to be mined by intermediaries on their behalf. Governments—pretty much all governments of every stripe—are rapidly discovering how much real control they can get without showing their hands if they make use of the currently misconfigured, anti-privacy Net. A consensus of the great and the good against privacy is forming; the one against anonymity is already full-blown. Imagine how different our world would be if all the books in the West for the last half-millennium had reported their readers to headquarters, including informing the Prince or the Pope how many seconds each reader spent on each page. The book, which anyone could read to herself in the privacy of her mind, is being replaced by an appliance that tracks your reading for the bookseller, subject to the Prince's subpoena. It will not be easy to save privacy. But if we believe in liberty, we have absolutely no choice. C

Eben Moglen (moglen@columbia.edu) is a law professor at Columbia Law School and the founding director of the Software Freedom Law Center in New York.