

Whose Life Is It Anyway?

An enterprising reporter tries—and mostly fails—to regain privacy online

CLIVE THOMPSON

DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE

BY JULIA ANGWIN NEW YORK: TIMES BOOKS. 304 PAGES. \$28.

Let's imagine you wanted to instant message with someone in a completely secure way. You don't want the National Security Agency to listen in, and you don't want a company like Google scooping up and analyzing your words so it can tailor ads to you. How would you do it?

You'd have to follow Julia Angwin's lead. In *Dragnet Nation* she spends a year trying to communicate digitally without being snooped upon by these powerful forces. As she discovers, it isn't easy.

To create private instant messaging, for example, you need to use a great deal of encryption technology to scramble the IMs as they travel between you and your correspondent. To ensure that she can chat in conditions of actual privacy, Angwin finally has to configure three separate pieces of software so they work in concert. It is a task of sufficient complexity that Angwin—who, as a digital-privacy reporter for the *Wall Street Journal*, is no high-tech neophyte—can only accomplish it with the help of a computer-security researcher at her shoulder, guiding her through each step.

Why is the encryption software so convoluted? Why can't you simply click on a box somewhere to shield your digital correspondence from prying eyes or consumer-monitoring commerce bots? It turns out that the cumbersome design of encryption safeguards is partially a side effect of their creators' virtuous intent. Each piece is an open-source work created by volunteer programmers. They're public spirited and devoted to the cause of privacy, but most of them aren't being paid for their work. So they struggle to find the time to update their tools and make them user friendly. One key piece of software that Angwin employs—the chat program Adium—was coded by Evan Schoenberg, “an ophthalmologist finishing his fourth year of medical residency,” who tells her, apologetically, “I simply haven't had time and a lot of our core development team has moved on to jobs that pay.” He improves the program in his spare time. When she calls him, he is at the hospital, working his day job. “On this fragile foundation,” Angwin writes, “rested my most robust hope of encryption.”

In a way, *Dragnet Nation* fits into the now-familiar genre of “stunt” books, in which authors take it upon themselves to try something kooky for a year. But *Dragnet Nation*'s high-wire concept—disappearing from the surveillance-sphere—is much more serious and ambitious. As she documents, corporate and government spying has been woven, creepily, into the fabric of our everyday lives online.

Angwin traces the rise of modern corporate surveillance to 2001, when Web companies—desperate for new business models after the dot-com collapse—launched ambitious software dedicated to hoovering up people's online activities and selling them to advertisers eager to “microtarget” the potential consumer base for their products. This quiet, behind-the-cursor revolution created today's ecosystem of browser “cookies”—the digital files that websites place on your

computer to track your online roamings. Meanwhile, as digital tools became cheaper in the aughts, routine surveillance grew increasingly tempting for more and more organizations pursuing an expansive array of commercial, behavioral, or just plain invasive agendas. Schools put webcam spyware on kids' laptops at home, marketers rolled out face-recognition systems, and repo men began scanning the images of license plates they had captured as they drove about to identify debt-racked car owners. (One repo outfit that Angwin profiles here scans photos of one million such plates a month.)

On the government side, 2001 was also a seminal year: The federal response to the September 11 terrorist attacks outfitted the NSA with a new mandate to start collecting

In the former East Germany, Angwin shows her LinkedIn network to an archivist, who marvels at the social map. “The Stasi,” he says, “would have loved this.”

phone-call and e-mail records en masse and without warrants. The NSA won a wide berth for such surveillance from Congress in the Patriot Act, and the Bush administration bolstered that with a battery of secret legal memos.

But sinister government surveillance was just one prong of the new data-sweeping regime: We, the spied-upon, made the job easier as we began using large services—like Twitter, Facebook, and Gmail—that offer one-stop shopping for spy agencies eager to map our connections. When Angwin visits the Stasi archives, she shows her LinkedIn network to the archivist, who marvels at the social map. “The Stasi,” he says, “would have loved this.”

Invasive surveillance deforms civic life. Citizens who were visited by the Stasi were so terrified by the reach of the surveillance into their personal lives that they either became “model citizens” or withdrew from public life. Today's panopticism (in the West, at least) hasn't had anything like this effect, as Angwin notes, because it can be quite crude in displaying its own invasive footprints: You shop for cameras online, and then find yourself haunted for weeks by camera ads each time you visit a new website. We thus tend to see the incipient danger not in the everyday but in the extraordinary—the screwups and errors of spy agencies and corporations.

These depredations of our dragnet world, Angwin argues, will grow and grow, though the public may not perceive the hazard until it's too late. The challenge of privacy is thus comparable to pollution or global warming. These crises grew slowly, created by a billion tiny, daily uses of energy that individually seemed harmless, but in aggregate cooked the planet. “The harm of both pollution and privacy is collective,” Angwin writes:

No one person bears the burden of pollution; all of society suffers when the air is dirty and the water undrinkable. Similarly, we all suffer

when we live in fear that our data will be used against us by companies trying to exploit us or police officers sweeping us into a lineup.

Angwin elegantly chronicles this tragedy of the digital commons at the level of policy and our individual civil liberties. But *Dragnet Nation* really kicks in—and becomes a blast to read—when she fights back. As she transforms herself into the invisible woman online, the book becomes by turns a spy novel, a how-to guide, and a rumination on the politics of software.

She stops using “cloud” programs that lack strong encryption, storing her files instead with services with names like SpiderOak. She analyzes the entropy levels of her passwords, discovering how weak many of them

are (her blog password can be broken in an instant), and uses a dice-throwing mechanism to generate much stronger ones. She puts tape over her laptop's webcam and wraps her mobile phone in tinfoil (because even when it's turned off, it still generates geolocatable signals). Like the drug dealers in *The Wire*, Angwin becomes adept at using “burners,” mobile phones you can pay for in full anonymity. She even gets another copy of her credit card issued with a fake name—surprisingly legal, so long as the main card is still billed to her real name at home—since this lets her confuse the trackers by making it harder to match her purchases to any name-based files. She wrangles cookie-blocking technologies and pays privacy concerns to render her more or less invisible on search sites.

But Angwin comes to realize that her success is always incomplete. Hiding files is one thing; communicating online with other people is what proves truly bedeviling. Encryption works only if both parties carefully use the same encryption software, and it's still pretty obtuse stuff. Angwin valiantly tries to use it in her e-mail and chat programs and to convince others to do so, but she gets thwarted by human error (she or her opposite number will misconfigure things, and their cover is instantly blown) or the sheer ungainliness of the software. “There is not really a market for consumer privacy software,” as one maker of the tools admits. “All this stuff is unusable. All of the tools we have are awful. We have to acknowledge that.”

Nor does it seem likely that Silicon Valley's ballyhooed and innovation-happy private sector will ever come to the rescue of privacy seekers, because the demand isn't there. Most casual computer users are simply injured at this point to trading off user convenience for consumer privacy, and as a result, profitable security fixes are never able to get much of a market footing. Worse, the few companies that have made genuinely easy-to-use encryption tools have been aggressively targeted by the government. Two

encrypted e-mail services—Lavabit and Silent Circle—recently shut down after federal spy agencies essentially threatened to hound them into oblivion.

This all serves to reinforce Angwin's larger argument: The real solution for privacy, she concludes, isn't technological—it's political. Bad laws like the Patriot Act enabled today's dragnet-spying complex. So in order to rein in its well-documented abuses, Congress will have to pass better laws. We need regulations that limit what data can be collected, whom it can be shared with, and what rights we have to examine, and to amend, the files held in the darker reaches of the federal intelligence bureaucracy. We need political pressure—at voting booths, in the media, and in the courts—to keep the government from threatening those who make pro-privacy tools.

Angwin is cautiously optimistic this balance is attainable. “We didn't shut down the industrial economy to stop pollution,” she writes:

We simply asked the polluters to be more accountable for their actions. We passed laws and created a new governmental agency and forced polluters to be transparent. Similarly, we don't need to shut down the data economy. We just need to make the data handlers let us see what they have about us and be accountable for any harm caused by their use of our data.

Angwin doesn't want people to stop going online: “Technology allows us to find people who share our inner thoughts; to realize we're not alone,” she writes. What she wants is a deceptively modest safeguard within this system of online exposure: the clearing out of some “room in the digital world for letters sealed with hot wax.”

I would like to share her hope for a better legal regime here, but it's tough to see just how it might be grounded in the present arrangement of our national politics. The regulatory capture of Congress by spies—both state and commercial—seems awfully complete.

Still, her pioneering experiment to forge a less readily detectable online presence is admirable, and as she convincingly argues, it created its own ripple effect in the spread of greater privacy consciousness. Each time she insisted on trying to use encrypted chat with a friend or colleague or showed off a burner phone, it prompted her acquaintances and chat partners to ponder the politics of online privacy.

If we're lucky, this could be another way that the brewing crusade for online privacy mirrors the environmental movement. Americans once thought nothing of hurling garbage out their car windows; it took decades of shifting social expectations and face-to-face peer pressure to slowly change their conduct. Better behavior spread incrementally, as one person's moral acts encouraged another's. If enough people followed Angwin's lead, new networks of computer users might manage to open up ever larger holes in the dragnet world. □

Clive Thompson is the author of *Smarter than You Think: How Technology Is Changing Our Minds for the Better* (Penguin Press, 2013). (See Contributors.)