Whose Life Is It Anyway?

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

CLIVE THOMPSON

Let's imagine you wanted to instant message with someone who was completely secure. You don't want the National Security Agency to listen in. 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 catch in conditions of actual privacy, Angwin finally has to negotiate three separate pieces of software so they work in concert. It is of sufficient complexity that Angwin—who, as a digital-privacy reporter for the Wall Street Journal, is a 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 a computer monitoring commerce bots? It turns out that the cumbersome design of encryption safeguards is partly a side effect of the creation of its 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 Schoner, 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 it in his spare time. When she calls him, he is at the hospital, working his day job. "On this fragile foundation," Angwin writes, "we must rely on my most robust brother, who is a brilliant student.

In a way, Dragnet Nation fits into the now-familiar genre of "trust" books, in which authors lay 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 the documents, corporate and government spying has been woven, crept, into the fabric of our everyday lives online. Angwin traces the rise of modern corporate spying back 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 quick, behind-the-scenes creation revealed today's ecosystem of browser "cookies"—the digital files that websites place on your computer to track your online readings. Moreover, it became clear that in the arts, routine surveillance grew increasingly tempting for more and more companies pursuing an expansive array of customers, beliefs, or even just plain invasive agendas. Schools put webcam software on kids' laptops at home, marketeers rolled out face-recognition software, 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 soul that Angwin profiles here scans photos of one million such plates a month.)

On the government side, 2011 was also a seminal year: The federal response to the September 11 terrorist attacks outfitted the NSA with a new mandate to start collecting phone-call and e-mail records in 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 programs. 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 buying 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 defies a civic life. Citizens who were visited by the Stasi were so terrorized by the reach of the surveillance into their personal lives that they either became "model citizens" or withdrew from public life. Today's panopticon (in the West, at least) hasn't had the impact of this effect, as Angwin notes, because it can be quite crude in displaying its own invasive forces. You shop for cameras online, and then find yourself haunted for weeks by 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 screwdrivers and errors of spy agencies and corporations.

These depredations of our digital 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 grow slowly, created by a billion, daily uses of energy that individually seemed harmless, but in aggregate cooked the climate. The "harm of both pollution and privacy is collective," Angwin writes.

No one person bears the burden of pollution, oil spills, and the slow shift to dirtier, more perilous and dangerous waste undrinkable. Similarly, 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 large carpet.

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 tin foil (because even when it's turned off, it still generates geolocational signals). Like the drug dealers in The Wire, Angwin becomes adept at using "burners," mobile phones you can pay for in small amounts. 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 confer the trackers by making it harder to match her purchases to any name-based files. She wrangles codec-based 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. Hiring files is one thing; communicating online with other people is what proves truly bewildering. Encryption works only if both parties carefully use the same encryption software; it's still pretty brute force stuff. Angwin valiantly tries to use it in e-mail and chat programs and to continue to do so, but she gets thwarted by human error (she or her correspondents will mess up the critical variables, or be compromised by phishers) or the sheer unavailability of the software. "There is not really a market for consumer privacy software," as one maker of the tools admits. "All this stuff is useless. All of the tools we have are useless. We have to acknowledge that." But 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 insured at this point to trading off user convenience for consumer privacy, and as a result, profitable security flaws 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.

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. We might want a deceivingly 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 too late to see just how it might be grounded in the present arrangement of our national politics. The regulatory capture of Congress by spooks—both state and corporate—seems woefully complete.

Still, her pioneering experiment to forge a little more readable 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 applications or to send a file encrypted to safeguard her privacy, 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 crucible for online privacy mirrors the environmental movement. Americans once thought nothing of hurling garbage out of their car windows; it took decades of shifting social expectations and face-to-face peer pressure to slowly change our behavior. Did-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 digital world.