Steven M. Bellovin
Columbia University

Security, Privacy, and Scale

How should we decide what problems to focus on? After all, there is no shortage of security and privacy challenges. For me, the answer is "scale"; oddly enough, that answer grew out of my early policy work rather than anything technical.

I first started getting professionally involved in law and policy issues around 1993. I was working at Bell Labs at the time, and three different tech policy issues arose that AT&T was interested in: the bill that became the Digital Millennium Copyright Act, government access to encrypted communications in the form of the Clipper chip, and the bill that became the Communications Assistance to Law Enforcement Act (CALEA). I was one of two people in research who knew the relevant technical issues and wanted to get involved with lawyers. This probably led to the legal chapter in my first book, *Firewalls and Internet Security*; it also led to my current professional focus, where I spend as much effort on the law and policy side as on purely technical issues. But it also forced me to confront a difficult question: assuming that CALEA and the Clipper chip actually help law enforcement (itself a questionable assumption, but that's for another time), what is there about these technologies that makes them objectionable? That is, under the assumption that not all technology that law enforcement finds helpful is bad—and I think that that's a valid assumption—what is my metric for distinguishing between good and bad mechanisms?

My answer, back then, was that I didn't like mechanisms that "scaled to oppression." That is, I objected to schemes that could be abused not just to solve individual crimes but to engage in mass surveillance of the population. In her concurrence in *United States v. Jones*, Justice Sotomayor expressed it more precisely:

And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously,

it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility."

In other words, invisible technologies are problematic, as are ones that are too cheap. She noted, I think correctly, that it's a feature if law enforcement has to exert a reasonable amount of effort to invade someone's privacy. Otherwise, there will be too much temptation for abuse of authority.

The same applies to security. In fact, defense at scale was a major motivation for firewalls. Back in 1994, I wrote that "firewalls are *not* a solution to network problems. They are a network response to a host security problem"—to ubiquitous buggy code. In other words, we saw firewalls as a scalable solution to host insecurity.

It is important to realize that I'm not speaking of something as simplistic and as hard to get right as "the greatest good for the greatest number." Rather, it's an economic issue: defenders have limited resources; it pays to see out leverage where a comparatively small effort can have a large payoff.

Operating system designers have long understood this. Consider how the advent of universal face masks has inconvenienced the

Digital Object Identifier 10.1109/MSEC.2020.3019709
Date of current version: 29 October 2020

continued on p. 63

 continued from p. 64

users of newer iPhones, which are unlocked by facial recognition. Why must I enter a PIN to, say, see where I am on a map? Map apps can reveal all sorts of sensitive information about a person's travels; permitting unauthenticated access to the map program would require that it implement access control. The same, of course, is true for many other apps—which is why the operating system does it in one place. This is a *scalable* solution.

Of course, scale cuts both ways. Viruses and worms exploit monocultures. Too many people run too few different kinds of software. For example, for all practical purposes there are four web browsers: Google's Chrome, Apple's Safari, Microsoft's Edge, and Mozilla's Firefox, and in the U.S. the first two dominate. This means that a single browser bug can be used to hack platforms at scale. Conversely, some of our defenses, e.g., address space layout randomization, are intended to deny scale to the attackers.

Scale isn't the only property to consider when designing defenses—but it is an important one. ■

Steven M. Bellovin is a professor of computer science and affiliate law faculty at Columbia University. Contact him via https://www.cs.columbia.edu/~smb.

Digital Object Identifier 10.1109/MSEC.2020.3028712