Bruce Schneier
Harvard University

Technologists vs. Policy Makers

Sometime around 1993 or 1994, during the first Crypto Wars, I was part of a group of cryptography experts that went to Washington to advocate for strong encryption. Matt Blaze and Ron Rivest were with me; I don't remember who else. We met with then Massachusetts Representative Ed Markey. (He didn't become a senator until 2013.) Back then, he and Vermont Senator Patrick Leahy were the most knowledgeable on this issue and our biggest supporters against government backdoors. They still are.

Markey was against forcing encrypted phone providers to implement the NSA's Clipper Chip in their devices, but wanted us to reach a compromise with the FBI regardless. This completely startled us techies, who thought having the right answer was enough. It was at that moment that I learned an important difference between technologists and policy makers. Technologists want solutions; policy makers want consensus.

Since then, I have become more immersed in policy discussions. I have spent more time with legislators, advised advocacy organizations like EFF and EPIC, and worked with policy-minded think tanks in the United States and around the world. I teach cybersecurity policy and technology at the Harvard Kennedy School of Government. My most recent two books, *Data and Goliath*—about surveillance—and *Click Here to Kill Everybody*—about IoT security—are really about the policy implications of technology.

Over that time, I have observed many other differences between technologists and policy makers—differences that we in cybersecurity need to understand if we are to translate our technological solutions into viable policy outcomes.

Technologists don't try to consider all of the use cases of a given technology. We tend to build something for the uses we envision, and hope that others can figure out new and innovative ways to extend what we created. We love it when there is a new use for a technology that we never considered and that changes the world. And while we might be good at security around the use cases we envision, we are regularly blindsided when it comes to new uses or edge cases. (Authentication risks surrounding someone's intimate partner is a good example.) Policy doesn't work that way; it's specifically focused on use. It focuses on people and what they do. Policy makers can't create policy around a piece of technology without understanding how it is used—how all of it's used.

Policy is often driven by exceptional events, like the FBI's desire to break the encryption on the San Bernardino shooter's iPhone. (The PATRIOT Act is the most egregious example I can think of.) Technologists tend to look at more general use cases, like the overall value of strong encryption to societal security. Policy tends to focus on the past, making existing systems work or correcting wrongs that have happened. It's hard to imagine policy makers creating laws around VR systems, because they don't yet exist in any meaningful way. Technology is inherently future focused. Technologists try to imagine better systems, or future flaws in present systems, and work to improve things.

As technologists, we iterate. It's how we write software. It's how we field products. We know we can't get it right the first time, so we have developed all sorts of agile systems to deal with that fact. Policy making is often the opposite. U.S. federal laws take months or years to negotiate and pass, and after that the issue doesn't get addressed again for a decade or more. It is much more critical to get it right the first time, because the effects of getting it wrong are long lasting. (See, for example, parts of the GDPR.) Sometimes regulatory agencies can be more agile. The courts can also iterate policy, but it's slower.

Along similar lines, the two groups work in very different time frames. Engineers, conditioned by Moore's law, have long thought of 18 months as the maximum time to roll out a

Digital Object Identifier 10.1109/MSEC.2019.2951825
Date of current version: 23 January 2020

continued on p. 71

 Copublished by the IEEE Computer and Reliability Societies

 continued from p. 72

new product, and now think in terms of continuous deployment of new features. As I said previously, policy makers tend to think in terms of multiple years to get a law or regulation in place, and then more years as the case law builds up around it so everyone knows what it really means. It's like tortoises and hummingbirds.

Technology is inherently global. It is often developed with local sensibilities according to local laws, but it necessarily has global reach. Policy is always jurisdictional. This difference is causing all sorts of problems for the global cloud services we use every day. The providers are unable to operate their global systems in compliance with more than 200 different—and sometimes conflicting—national requirements. Policy makers are often unimpressed with claims of inability; laws are laws, they say, and if Facebook can translate its website into French for the French, it can also implement their national laws.

Technology and policy both use concepts of trust, but differently. Technologists tend to think of trust in terms of controls on behavior. We're getting better (at what?)—NIST's recent work on trust is a good example—but we have a long way to go. For example, Google's Trust and Safety Department does a lot of AI and ethics work largely focused on technological controls. Policy makers think of trust in more holistic societal terms: trust in institutions, trust as the ability not to worry about adverse outcomes, consumer confidence. This dichotomy explains how techies can claim bitcoin is trusted because of the strong cryptography, but policy makers can't imagine calling a system trustworthy when you lose all your money if you forget your encryption key.

Policy is how society mediates how individuals interact with society. Technology has the potential to change how individuals interact with society. The conflict between these two causes considerable friction, as technologists want policy makers to get out of the way and not stifle innovation, and policy makers want technologists to stop moving fast and breaking so many things.

Finally, techies know that code is law—that the restrictions and limitations of a technology are more fundamental than any human-created legal anything. Policy makers know that law is law, and tech is just tech. We can see this in the tension between applying existing law to new technologies and creating new law specifically for those new technologies.

Technology and policy both use concepts of trust, but differently.

Yes, these are all generalizations and there are exceptions. It's also not all either/or. Great technologists and policy makers can see the other perspectives. The best policy makers know that for all their work toward consensus, they won't make progress by redefining pi as three. Thoughtful technologists look beyond the immediate user demands to the ways attackers might abuse their systems, and design against those adversaries as well. These aren't two alien species engaging in first contact, but cohorts who can each learn and borrow tools from the other. Too often, though, neither party tries.

In October, I attended the first ACM Symposium on Computer Science and the Law. Google counsel Brian Carver talked about his experience with the few computer science grad students who would attend his Intellectual Property and Cyberlaw classes every year at UC Berkeley. One of the first things he would do was give the students two different cases to read. The cases had nearly identical facts, and the judges who'd ruled on them came to exactly opposite conclusions. The law students took this in stride; it's the way the legal system works when it's wrestling with a new concept or idea. But it shook the computer science students. They were appalled that there wasn't a single correct answer.

But that's not how law works, and that's not how policy works. As the technologies we're creating become more central to society, and as we in technology continue to move into the public sphere and become part of the increasingly important policy debates, it is essential that we learn these lessons. Gone are the days when we were creating purely technical systems and our work ended at the keyboard and screen. Now we're building complex socio-technical systems that are literally creating a new world. And while it's easy to dismiss policy makers as doing it wrong, it's important to understand that they're not (Qualify this somehow? From their point of view?). Policy making has been around a lot longer than the Internet or computers or any technology. And the essential challenges of this century will require both groups to work together. ■

Bruce Schneier is a lecturer and fellow at the Harvard Kennedy School and special advisor to IBM Security. His new book is *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. He organized a one-day track on public-interest technology at the RSA Conference in March 2019 in San Francisco. He maintains a resources page at www.public-interest-tech.com. Contact him via www.schneier.com.