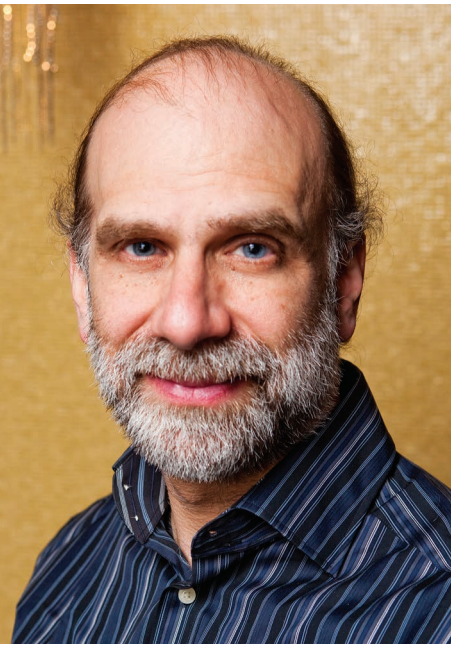

Bruce Schneier
Harvard University

IoT Security: What's Plan B?

In August, four US Senators introduced a bill designed to improve Internet of Things (IoT) security. The IoT Cybersecurity Improvement Act of 2017 is a modest piece of legislation. It doesn't regulate the IoT market. It doesn't single out any industries for particular attention, or force any companies to do anything. It doesn't even modify the liability laws for embedded software. Companies can continue to sell IoT devices with whatever lousy security they want.

What the bill does do is leverage the government's buying power to nudge the market: any IoT product that the government buys must meet minimum security standards. It requires vendors to ensure that devices can not only *be* patched but *are* patched in an authenticated and timely manner, don't have unchangeable default passwords, and are free from known vulnerabilities. It's about as low a security bar as you can set, and that it will considerably improve security speaks volumes about the current state of IoT security. (Full disclosure: I helped draft some of the bill's security requirements.)

The bill would also modify the Computer Fraud and Abuse and the Digital Millennium Copyright Acts to allow security researchers to study the security of IoT devices purchased by the government. It's a far narrower exemption than our industry needs. But it's a good first step, which is probably the best thing you can say about this legislation.

However, it's unlikely this first step will even be taken. I am writing this column in August, and have no doubt that the bill will have gone nowhere by the time you read it in October or later. If hearings are held, they won't matter. The bill won't have been voted on by any committee, and it won't be on any legislative calendar. The odds of this becoming law are zero. And that's not just because of current politics—I'd be equally pessimistic under the Obama administration.

But the situation is critical. The Internet is dangerous—and the IoT gives it not just eyes and ears, but also hands and feet. Security vulnerabilities, exploits, and attacks that once affected only bits and bytes now affect flesh and blood.

Markets, as we've repeatedly learned over the past century, are terrible mechanisms for improving the safety of products and services. It was true for automobile, food, restaurant, airplane, fire, and financial-instrument safety. The reasons are complicated, but basically, sellers don't compete on safety features because buyers can't efficiently differentiate products based on safety considerations. The race-to-the-bottom mechanism that markets use to minimize prices also minimizes quality. Without government intervention, the IoT remains dangerously insecure.

The US government has no appetite for intervention, so we won't see serious safety and security regulations, a new federal agency, or better liability laws. We might have a better chance in the EU. Depending on how the General Data Protection Regulation on data privacy pans out, the EU might pass a similar security law in 5 years. No other country has a large enough market share to make a difference.

Sometimes we can opt out of the IoT, but that option is becoming increasingly rare. Last year, I tried and failed to purchase a new car without an Internet connection. In a few years, it's going to be nearly impossible to not be multiply connected to the IoT. And our biggest IoT security risks will stem not from devices we have a market relationship with, but from everyone else's cars, cameras, routers, drones, and so on.

We can try to shop our ideals and demand more security, but companies don't compete on IoT safety—and we security experts aren't a large enough market force to make a difference.

We need a plan B, although I'm not sure what that is. Email me if you have any ideas. ■

Bruce Schneier is a security technologist and a Fellow at the Berkman Klein Center for Internet and Society at Harvard University. He's also the chief technology officer of IBM Resilient and special advisor to IBM Security. Contact him via www.schneier.com.

Copublished by the IEEE Computer and Reliability Societies