Written Testimony of Edward W. Felten
Professor of Computer Science and Public Affairs, Emeritus, Princeton University

United States Senate, Committee on Commerce, Science, and Transportation
Hearing on Enhancing Data Security
October 6, 2021

Chair Cantwell, Ranking Member Wicker, and distinguished members of the Committee, thank you for the opportunity to testify.

As you know, data security is an issue that is important to many Americans. More and more data about our lives is captured, stored, and analyzed, with little transparency about what is collected, who has it, what they are doing with it, and how well companies are protecting it. Even the most careful companies may be subject to a data breach, and of course the existence of a breach does not by itself prove security measures were inadequate. But too often companies fail to take common, reasonable steps to ensure data security, and too often these failures lead to breaches that ultimately harm consumers.

At the national level, the Federal Trade Commission plays a primary role in civil enforcement to protect data security in most sectors of the economy, mainly by enforcing Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."

I had the privilege of serving as the FTC's first Chief Technologist from 2011-2012, and I have continued to follow the FTC's data security activities since. My testimony is informed by these experiences and by my academic study of data security and privacy from both technical and

policy perspectives. I am testifying in my personal capacity and not on behalf of any agency or organization.[1]

In this testimony I will cover two main areas. First, I will summarize two examples in which companies' data security failures led to breaches that harmed consumers. Second, I will discuss three things Congress might do to strengthen the FTC's ability to protect consumers: enabling civil penalties for first violations of the FTC Act; creating a statutory or rulemaking framework regulating data security practices; and providing resources to grow and empower the FTC's technology workforce.

Impact on Consumers: An Example

The following example helps illustrate how data security failures put Americans at risk.

Over the last decade or so, cheap Internet of Things devices have proliferated in our homes and offices. For example, a parent might set up a webcam in their home and then, while on a family trip to visit relatives, might use a phone app to turn on the webcam and verify that all is well back at home. This requires a way for the parent's phone to connect over the network to the webcam and send a command to the camera to stream video back to the parent's phone. Security requires that the webcam must only accept commands from the authorized phones of the parents and not from other sources.

In 2015, research revealed that many widely sold webcams had hidden administrative functions that allowed anyone to log in to the webcam and control it from afar, using weak and widely

[1] Although I am a Member of the Privacy and Civil Liberties Oversight Board, I am testifying solely in my individual, non-official capacity.

known username/password combinations such as admin/admin, guest/guest, and administrator/1234. These were not weak passwords chosen by the consumer but rather passwords set up in advance by the manufacturer, without notice to the consumer and without any reasonable way for the consumer to change them.

The consequence was that many Americans had webcams in their homes and offices that could be turned on and viewed across the Internet by bad actors.

In addition to enabling direct exploitation to spy on consumers, these vulnerabilities also opened the door to attackers using webcams as a jumping-off point for cyberattacks on other targets anywhere on the Internet.

This very possibility was exploited by hackers who automated the process of scanning the Internet for vulnerable webcams and similar devices, and installing malware on them. By this means they took control of hundreds of thousands of devices all over the Internet, and operated those compromised devices under centralized control to form what was dubbed the Mirai botnet. Discovered in 2016, Mirai was used to launch some of the largest denial of service attacks seen to that time, including one against an infrastructure provider that knocked many sites, including Twitter, Reddit, and Netflix, offline for several hours. Three young Americans would later plead guilty to these crimes.[2]

There was little if anything that consumers could have done to protect themselves. Nothing on the webcams or their packaging suggested the existence of a minimally protected administrative

[2] More detail about these events is available from the U.S. Department of Justice: *Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant Cyber Attacks*, Dec. 13, 2017. https://www.justice.gov/usao-nj/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases

interface. Few consumers would have had the technical know-how to check or probe the devices themselves. Consumers should have been able to rely on companies to take simple and reasonable precautions to ensure data security.

Consequences of Weak Security: The Equifax Breach

Even large and well-known companies sometimes fail to protect the security of consumer data.

In 2017 the consumer credit reporting company Equifax discovered a series of intrusions into its systems through which the private data of about 150 million people was extracted—including 145 million unencrypted social security numbers. The FTC and other agencies investigated, and Equifax ultimately agreed to a consent order including penalties of about $600 million.

According to the FTC and other sources, the initial breaches occurred because the company failed to apply an available security patch to a component of one of its public-facing servers. The company knew of the problem—the security flaw in the component—and also knew of the availability of the solution—the security patch—but still failed to apply the patch to all of its vulnerable systems. Multiple intruders exploited this failure and gained unauthorized access to Equifax systems.

Because the company did not take other precautions, such as partitioning its network, intruders were able to move laterally from the initially compromised system into other internal Equifax systems. Compounding this failure, the first breached system had access to an unprotected, unencrypted file share that listed administrative passwords for internal systems in plain text, which further helped the intruders expand their access.

The intrusions went undetected for about four months, in part because the company was not consistently using common defensive measures such as file integrity checking and network intrusion detection.

Several of these failures, such as neglecting to apply security patches and storing sensitive data in unencrypted form, were contrary to the company's own internally stated policies, suggesting a broader failure to oversee and manage its internal data security operations. The company's settlement with the FTC required it to establish stronger data security management and accountability structures.

As in the webcam example, there was little if anything that consumers could have done to protect themselves. Equifax, as a consumer credit reporting agency, has data on many Americans who are not its customers, and even those who are customers of an Equifax service would have had no visibility into the company's internal security practices or policies. The affected people could only rely on the company to adopt reasonable measures, and on the FTC and other enforcement bodies to enforce the law when necessary.

Further Empowering the FTC to Protect Data Security

The FTC's staff and leadership have been diligent and dedicated to their data security mission. Yet the agency has sometimes struggled to cope with the sheer scope, scale, and complexity of this mission—and these challenges will only become more difficult as digital technologies continue to proliferate and become even more complex.

Based on my experience at the FTC and my study of the agency, I would point to several factors, listed below, that have contributed to these challenges.

Limitations of the FTC Act: No Civil Penalties for First-time Violations

A first challenge has been the structure of the FTC Act. Section 5 of the Act imposes no civil penalty for a first-time violation, so even companies who commit serious violations can get a free pass if they have not faced an FTC enforcement action before. Often, the most important effect of an enforcement action is merely to enable civil penalties for subsequent violations. Furthermore, civil penalties for a second violation may only be available if the second violation involves behavior covered by the first consent order.

The combination of limited enforcement resources and no first-time penalties can make the FTC Act a weak deterrent, tempting a company to gamble that it won't face enforcement, or even if it does face enforcement, that it can gain an advantage through unfair practices and then clean up its act after the first enforcement. This opens consumers to risk. Congress could strengthen the deterrent effect of the FTC Act by authorizing civil penalties for first-time violations of Section 5, at least for data security related violations.

Many of the FTC's data security enforcements have been under the unfair practices arm of Section 5. The FTC has developed a body of case law through its past data security enforcements, and has offered guidance on some practices it considers unfair.

The case law approach has had some benefits, especially in the early days, but the public and the industry would benefit from a rulemaking that offered more specificity for companies and consumers, while retaining the flexibility needed to enable beneficial innovation in an evolving technological space. I understand that in practice, any data security rulemaking would require a new authorization from Congress.

Need for Comprehensive and Technically Focused Data Security Regulations

If Congress were to enact data security legislation that authorized an FTC rulemaking or that created a statutory framework and directed a rulemaking to fill in further details, it might include provisions such as:

- requiring companies to store and transmit sensitive consumer data in encrypted form;
- requiring strong multi-factor authentication for access to administrative accounts that can access large amounts of consumer data or can grant access to such data;
- requiring reasonable data minimization so that consumer data will be deleted when it is no longer needed for the purpose for which it was collected;
- requiring companies to apply a baseline level of security due diligence to software they build or acquire for use in handling consumer data;
- requiring companies to make reasonable efforts to track and install available security updates in systems that can access consumer data;
- where relevant and feasible, requiring companies to provide a reasonable way for consumers to get security updates for software a company supplies to them, and requiring that those updates be delivered in a secure fashion;
- in relevant cases, requiring a company to make available such security updates for a specified time period, and requiring prominent disclosure of when such security support will no longer be available;
- prohibiting companies from knowingly shipping devices or systems with serious security vulnerabilities that endanger data security;
- prohibiting companies from shipping devices or systems containing old versions of third-party software for which security patches have been issued, without a reasonable mitigation strategy;

- where a company relies on a third-party service provider to store or process consumer data, clarifying the company's responsibility to ensure that the service provider is taking reasonable steps to secure the data;
- prohibiting default settings or behaviors that put consumers at unnecessary risk;
- establishing more stringent requirements for certain sensitive categories of data such as health data, financial data, or information about children, at least when such data is outside the bounds of sector-specific privacy laws such as HIPAA, COPPA, and FERPA; and
- requiring companies handling significant amounts of consumer data to establish internal reporting and accountability structures for data security.

Need for Resources and Expertise for Technology Analysis and Enforcement

Another challenge is the limited resources available to the FTC relative to the scope of its mission—of which data security is just one small part. The limited staff and resources available for data security force the agency to be very selective and strategic in how and when it enforces the law. Companies that stay "under the radar" of the FTC may not see enforcement due to resource limits, and consumers may suffer for it.

When I joined the FTC in 2011 as its first Chief Technologist, the agency was just starting to build its workforce of technologists. The need for more technology expertise seemed clear, especially in technology-related cases. Although the FTC has increased its capacity to hire and work with technologists over the nine years since my term ended, there is still a long way to go.

Technology expertise and analysis play a crucial role in data security investigations and enforcements. Below are a few examples of how technology experts can help the FTC better protect the security of consumers' data.

- Companies that are under investigation often argue in their defense that their practices were required for technical reasons or that they chose their action over the alternatives for valid technical reasons. For instance, a threshold question in any unfairness case is whether the company's relevant behavior was unreasonable under the circumstances. Where a case depends on a company's technology design or practices, technical expertise is required to evaluate claims such as whether the company was following common engineering practices, or whether there were technically feasible alternatives and how much the alternatives would have cost in money or functionality.
- Companies also sometimes argue that they needed to collect more data, or use data more aggressively, or withhold material information about data practices from consumers in order to better protect against cyberattacks or prevent fraudulent activity by their users. Evaluating these claims, and helping enforcers understand how much cybersecurity value these measures might have provided, requires technical expertise.
- Much of the evidence in data security cases will be technological. Technology experts can understand and interpret the evidence, help to draft the Civil Investigative Demands (CIDs) used to get information from a company, and better interpret companies' responses to CIDs.
- Most investigations that lead to enforcement are resolved by a consent decree negotiated with the subject company. These consent decrees often contain forward-looking technology requirements or limitations on a company's technology practices. Technology experts can help agency leaders as they work to negotiate meaningful limits on company behavior that will continue to protect consumers as technology evolves, without unnecessarily constraining a company's ability to improve its products.

Resource limits have been one barrier to expanding the FTC's technologist workforce. Agency leaders, knowing the scope of the agency's mission and the workload facing all of its components, have found it difficult to reduce headcount elsewhere in order to hire more technologists. Congress could lower this hurdle by providing additional resources and directing some of them to building a cohort of technology experts, including people with advanced training in computer science and closely related disciplines, or with equivalent experience in industry.

How to Grow and Empower the FTC's Technology Workforce

Building and leveraging a strong technology team requires more than just a budget. Having worked as the Chief Technologist at the FTC, and having built technology teams in industry and academia, I can offer a perspective on how it might be done.

Government can't match the salaries or working conditions available to top technologists in the private sector, but the FTC can find and recruit outstanding technologists who are motivated by the agency's mission of protecting Americans. Sustaining that strategy, however, relies on keeping the implied promise that a technologist will be able to contribute fully to the agency's work, and that they can aspire to contribute more and take on more responsibility as their career advances. Retaining the best technologists will require having a career path that offers a realistic possibility of reaching the most senior staff positions in the FTC, if their performance merits it. And this will only be possible if experienced technologists are treated as full partners in the agency's internal processes and staff-level decision making, and not merely as consultants or assistants to a legal team.

Although the analogy is not perfect, an interesting comparison is to the role and organization of economists within the FTC. The Bureau of Economics has been a useful vehicle for recruiting the agency's economics workforce and applying its expertise across the FTC's missions. With technology taking on a similarly important role in the FTC's work, the question arises whether it is time to create a Bureau of Technology along similar lines. The best placement of technologists within the FTC is a point for reasonable debate; what is more certain is that the agency can benefit greatly from building up its technology team and including technologists as full partners in the agency's work across the full range of its consumer protection and competition missions.

Conclusion: The Future of Data Security, and the FTC's Role

Data security will only grow in importance as digital technology becomes more prevalent, as new technologies are invented and deployed, and as digital supply chains become more global. With more at stake, and with attackers growing in sophistication, companies need to keep improving their practices to stay ahead of the threats and offer adequate protection for their users.

Civil enforcement by the FTC is an important backstop to protect consumers against unfair or deceptive data security practices. In this testimony, I suggested three steps that Congress might take to empower the FTC in this mission: allowing civil penalties for first-time violators; authorizing data security rulemaking; and enabling the creation of a stronger technology workforce at the FTC.

I thank the Committee members for your attention to data security, and for the work that you have already done to protect the security of Americans' data; and I look forward to your questions.