PREPARED STATEMENT OF THE

FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Permanent Subcommittee on Investigations

UNITED STATES SENATE

WASHINGTON, DC

MARCH 7, 2019

I. INTRODUCTION

Chairman Portman, Ranking Member Carper, and members of the Subcommittee, I am Andrew Smith, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on data security.

For nearly two decades, the FTC has been the nation's leading data security enforcement agency. In that role, the Commission has settled or litigated more than 60 law enforcement actions against businesses that allegedly failed to take reasonable precautions to protect consumers' personal information. The FTC vigorously pursues data security cases in a variety of areas, including against manufacturers of consumer products like smartphones, computers, routers, and connected toys as well as against companies that collect consumers' most sensitive personal information.

Data security is critically important both to consumers and to businesses. When a failure to reasonably safeguard consumers' personal information results in a data breach, consumers can suffer fraud and other harm. Moreover, the specter of data breaches not only affects those individual victims; it can engender a loss of consumer trust in companies, products, technologies, or even business sectors—with an adverse impact on consumers and businesses alike. To combat these harms, the Commission has, for nearly two decades, taken a three-pronged approach to data security: law enforcement, policy initiatives, and consumer and business education. The FTC has also coordinated efforts and resources in this area with other government actors, including the Department of Justice, criminal investigative agencies, and state Attorneys General.

[1] This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

Today, the Commission reiterates its longstanding bipartisan call for enactment of a comprehensive federal data security law. This testimony provides an overview of the Commission's efforts to promote data security, and explains further the Commission's support for data security legislation.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

Although it does not enforce a comprehensive data security law, the Commission does enforce a number of statutes related to data security. First, it enforces statutes and rules that pertain to specific types of entities and covered data. For example, the Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), requires non-bank financial institutions to safeguard nonpublic personal information by developing, implementing, and maintaining a comprehensive information security program..[2] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to verify that recipients of sensitive consumer information act with a permissible purpose,[3] and requires entities that maintain consumer report information to use safe disposal procedures.[4] Finally, the Commission enforces the Children's Online Privacy Protection Act ("COPPA"), which requires website operators to use reasonable security for the personal information they collect from children online.[5]

---

[2] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).
[3] 15 U.S.C. § 1681e.
[4] *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.
[5] 15 U.S.C. §§ 6501-6506. The FTC's implementing rule is at 16 C.F.R. Part 312. As part of its vigorous enforcement of COPPA, the FTC announced last week that video social networking app Musical.ly (now known as TikTok) has agreed to pay a record $5.7 million civil penalty to settle allegations that it illegally collected personal information from children. Press Release, FTC, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That It Violated Children's Privacy Law* (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.

Second, the Commission enforces Section 5 of the FTC Act, which prohibits unfair or deceptive practices.[6] Although not a data security statute *per se*, the FTC Act empowers the Commission to stop companies from making misleading statements or omissions about data security, where such material statements or omissions are likely to mislead reasonable consumers.[7] Indeed, the Commission has settled more than 30 matters challenging companies' express and implied claims that they provide reasonable security for consumers' personal data when they allegedly failed to use readily available, cost-effective measures to reduce data security risks.[8] And the Commission is currently litigating a case in federal district court against a device manufacturer that allegedly deceived consumers about the security of its routers and internet cameras.

The Commission has similarly used the FTC Act's prohibition on unfair practices to stop unreasonable data security practices. Under the statute, if a company's data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices are "unfair."[9] The Commission has settled over 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.[10]

As described above, the Commission has used its authority under these laws to litigate or settle more than 60 data security cases. In each of these instances, the security failures were not merely isolated mistakes. Indeed, the Commission has made clear that it does not require perfect security. There is no one-size-fits-all data security program, and the fact of a breach does not

---

[6] 15 U.S.C. § 45(a).
[7] *See* Federal Trade Commission Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).
[8] *See* FTC, Cases Tagged with Data Security, https://www.ftc.gov/enforcement/cases-proceedings/terms/249 (last visited Feb. 14, 2019).
[9] *See* Federal Trade Commission Policy Statement on Unfairness, *appended to Int'l Harvester Co*., 104 F.T.C. 949, 1070 (1984); 15 U.S.C. § 5(n).
[10] *See supra* note 8. Some cases have alleged both deception and unfairness.

necessarily mean that a company's security was unreasonable. Rather, reasonable security requires an ongoing process of assessing and addressing risks. When deciding whether to pursue an action, the Commission considers whether a company's data security measures are reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its operations, and the cost of tools available to reduce data security risks.

Several recent cases illustrate this approach. In a revised settlement with Uber Technologies, Inc.,[11] the FTC charged that the popular ride-sharing company deceived consumers by failing to reasonably secure sensitive consumer data stored in the cloud, despite promises of secure storage. Uber's alleged security failures were numerous: using a single key for full administrative access to consumer data, not requiring multi-factor authentication (a widely used, readily available safeguard in this area), and storing sensitive consumer information in plain readable text in database back-ups stored in the cloud. In light of these alleged pervasive, basic security failures, breaches of personal information in 2014 and 2016 were no surprise—and an FTC action to require reasonable security was necessary.

In another case, the FTC settled allegations that mobile phone manufacturer BLU Products, Inc. failed to implement the "appropriate" security procedures it promised.[12] As a result of BLU's security failures, the complaint charged, a third party service provider located in China collected an enormous amount of information from consumers' devices (far more than it needed), including the full contents of consumers' text messages. According to the complaint, had BLU implemented

[11] *See* Press Release, *Federal Trade Commission Gives Final Approval to Settlement with Uber* (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber.
[12] Press Release, *FTC Gives Final Approval to Settlement with Phone Maker BLU* (Sept. 10, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/ftc-gives-final-approval-settlement-phone-maker-blu.

reasonable technical security measures or engaged in reasonable oversight of its service provider, the third party would not have been able to access such sensitive information.

The FTC is currently litigating an action against computer networking equipment manufacturer D-Link, whose alleged inadequate security measures left consumers' wireless routers and internet cameras vulnerable to hackers.[13] Here, too, the FTC is challenging multiple alleged security failures: shipping software with well-known flaws, mishandling a private code-signing key, and storing login credentials in clear text. This action, like the FTC's other data security cases, sends a clear message: the FTC uses its existing tools to the fullest extent to stop unreasonable data security practices.

B. Policy Initiatives

Law enforcement is not the Commission's only tool; the FTC also uses policy initiatives, such as workshops, reports, and rulemaking, to promote data security. For example, in October 2018, the Commission's legal and economic staff issued their perspective on the FTC's December 2017 Informational Injury Workshop, which explored the injuries consumers may suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[14] The staff perspective was the second security-related report that the FTC issued in 2018. A report issued earlier in the year, *Mobile Security Updates: Understanding the Issues*, provided in-depth analysis of mobile security update data submitted by eight mobile device manufacturers in response to Commission orders.[15] The report's policy recommendations were grounded in that empirical work.

---

[13] Press Release, *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras* (Jan. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.

[14] FTC Report, *FTC Informational Injury Workshop: BE and BCP Staff Perspective* (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

[15] FTC Report, *Mobile Security Updates: Understanding the Issues* (Feb. 2018), https://www.ftc.gov/reports/mobile-security-updates-understanding-issues.

In November, the FTC held a hearing on data security as part of its series of *Hearings on Competition and Consumer Protection in the 21st Century*.[16] Participants included academics, industry representatives, practitioners, and consumer advocates who discussed a variety of data security-related topics, including the prevalence and consequences of data breaches, incentives to invest in data security, consumer demand for security, data security assessments, and whether the FTC's current toolkit is sufficient to address data security harms.[17] This hearing, like the others in the series, has yielded important information about business and technological changes that affect pressing consumer protection issues.

C. Business Guidance and Consumer Education

The Commission also creates extensive business and consumer education on data security. A recent focus has been cybersecurity guidance for small businesses. In April 2018, the FTC issued *Engage, Connect, Protect*, a staff perspective on the agency's projects and plans in this area.[18] As part of this initiative, the FTC has issued a variety of cybersecurity guidance for small businesses, such as fact sheets, videos, and other materials on dozens of cybersecurity topics.[19] For

[16] *See* Press Release, *FTC Announces Sessions on Consumer Privacy and Data Security as Part of Its Hearings on Competition and Consumer Protection in the 21st Century* (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its.
[17] *FTC Hearing on Competition and Consumer Protection in the 21st Century* – December 2018, https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018 (last visited Feb. 20, 2019).
[18] FTC Staff Perspective, *Engage, Connect, Protect: The FTC's Projects and Plans to Foster Small Business Cybersecurity* (Apr. 2018), https://www.ftc.gov/system/files/documents/reports/engage-connect-protect-ftcs-projects-plans-foster-small-business-cybersecurity-federal-trade/ecp_staffperspective_2.pdf.
[19] *See* FTC, *Protecting Small Businesses*, https://www.ftc.gov/tips-advice/business-center/small-businesses (last visited Feb. 14, 2019); *see also* Press Release, *FTC Launches National Campaign with Resources to Assist Small Businesses with Cybersecurity* (Oct. 18, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-launches-national-campaign-resources-assist-small-businesses.

example, recent business guides have covered topics such as email authentication,[20] vendor security,[21] and tech support scams.[22]

This guidance builds on the success of the 2017 business education series *Stick with Security*,[23] which offers advice on key security principles based in part on the FTC's closed investigations. The *Stick with Security* series itself expands on *Start with Security*, an earlier Commission initiative on data security that includes a written guide for businesses[24] and 11 short videos[25] that discuss ten important security topics and give advice about specific security practices for each. The advice in the guide and videos is drawn directly from lessons learned in FTC cases.

The Commission also educates consumers on data security in a variety of ways, such as through its website, videos, and pamphlets. For example, the FTC website highlights timely security issues, like tax identity theft, a Netflix phishing scam, tips on buying internet-connected smart toys, and the aftermath of the Marriott data breach.[26] At times, the FTC provides in-depth materials on a data security topic of particular concern to consumers. For example, immediately following the Equifax data breach, the agency created a dedicated page on its website, with information about fraud alerts, active duty alerts, credit freezes and locks, credit monitoring, and how to reduce the risk of identity theft.[27] Finally, the FTC assists consumers affected by data breaches through identitytheft.gov, a website that allows victims of data breaches to get

---

[20] FTC Business Blog, *Cybersecurity for small business: Email authentication* (Feb. 8, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/02/cybersecurity-small-business-email-authentication.
[21] FTC Business Blog, *Cybersecurity for small business: Vendor security* (Dec. 21, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/12/cybersecurity-small-business-vendor-security.
[22] FTC Business Blog, *Cybersecurity for small business: Tech support scams* (Dec. 14, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/12/cybersecurity-small-business-tech-support-scams.
[23] FTC, *Stick with Security: A Business Blog Series* (2017), https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.
[24] FTC, *Start with Security: A Guide for Business* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[25] FTC Videos, *Start with Security* (2015-2016), https://www.ftc.gov/news-events/audio-video/business.
[26] *See generally* FTC Consumer Blog, https://www.consumer.ftc.gov/blog (last visited Feb. 14, 2019).
[27] FTC, *The Equifax Data Breach*, https://www.ftc.gov/equifax-data-breach (last visited Feb. 14, 2019).

information on how to protect their personal information, and enables identity theft victims to easily file a complaint with the FTC and get a personalized Identity Theft report that can be used to help communicate with financial companies and credit reporting agencies. For victims of tax identity theft, identitytheft.gov helps people file the IRS Identity Theft Affidavit with the IRS – the first-ever digital pathway to do so.

III. DATA SECURITY LEGISLATION

While the Commission uses its existing authorities aggressively, the FTC reiterates its longstanding bipartisan call for comprehensive data security legislation. In particular, the FTC supports data security legislation that would provide the agency with three essential additional authorities: (1) the ability to seek civil penalties to effectively deter unlawful conduct, (2) jurisdiction over non-profits and common carriers, and (3) the authority to issue implementing rules under the Administrative Procedure Act ("APA"), as appropriate.[28]

Each of these additional authorities is important to the Commission's efforts to combat unreasonable security. Under current laws, the FTC only has the authority to seek civil penalties for data security violations related to children's online information (under COPPA) or credit report information (under the FCRA).[29] When the FTC brings data security cases under the FTC Act or the GLB Safeguards Rule, it cannot obtain civil penalties for first-time violations. To help ensure effective deterrence, we urge Congress to enact security-specific legislation to allow the FTC to seek civil penalties for data security violations in appropriate circumstances. Likewise, enabling the FTC to bring cases against non-profits and common carriers is important because these entities often collect sensitive consumer information. For example, educational institutions often collect

[28] While today's hearing focuses on data security, the Commission recognizes that many aspects of data security intersect with broader questions about consumer data privacy. The Commission urges Congress to consider enacting privacy legislation that would be enforced by the FTC.
[29] The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(*l*).

Social Security numbers and common carriers often collect the contents of consumer communications. Significant breaches have been reported in each of these sectors.[30]

Finally, the ability to engage in targeted APA rulemaking authority would enable legal requirements to keep up with business and technological changes. For example, in 2012, the FTC used its APA rulemaking authority under COPPA to update its implementing Rule (after giving notice and seeking public comment) to account for the rise of social media and the collection of geolocation information—practices that developed after Congress passed COPPA in 1998.[31]

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on data security. The FTC remains committed to promoting reasonable security for consumers and data, and we look forward to working with the Subcommittee as it considers these important issues.

---

[30] *See, e.g.*, Andy Segedin, *Hacked! Crooks are Grabbing Nonprofit Websites and Demanding Ransom*, THE NONPROFIT TIMES (Mar. 30, 2017), http://www.thenonprofittimes.com/news-articles/hacked-crooks-grabbing-nonprofit-websites-demanding-ransom/; *Spanish Telecom Provider Suffers Massive Data Breach*, SECURITY NEWSPAPER (July 19, 2018), https://www.securitynewspaper.com/2018/07/19/spanish-telecom-provider-suffers-massive-data-breach/.

[31] Press Release, *FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Childrens Online Privacy Protection Rule* (Dec. 19, 2012) https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.