UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Commissioner
Noah Joshua Phillips

Prepared Oral Statement of
FTC Commissioner Noah Joshua Phillips
Before the
U.S. Senate Committee on Commerce, Science, and Transportation

Hearing on "Oversight of the Federal Trade Commission"

August 5, 2020[1]

Chairman Wicker, Ranking Member Cantwell, Members of the Committee, thank you for the opportunity to appear before you. I'm honored to testify with my fellow Commissioners about the important work we do at the FTC. I also want to thank you for your flexibility on format. It is always good to be back at the Senate, even if that means virtually.

There is a lot to cover, and I look forward to our discussion; but I want to take a moment to highlight an important issue, which I know is a focus for many of you: data security.

Hardly a week goes by without Americans learning about another major cyberattack, breach, or vulnerability. Accounts on a major social media platform were exploited three weeks ago.[2] Last week, researchers revealed a vulnerability on devices running Windows and Linux operating systems, which could impact *billions* of devices.[3] Consumers get this: a 2018

[1] This written statement, my oral testimony, and my responses to questions reflect my views and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] Euirim Choi and Robert McMillan, *Widespread Twitter Hack Reaches Bill Gates, Kanye West, Elon Musk, Joe Biden, and Barack Obama*, THE WALL STREET JOURNAL (July 15, 2020), https://www.wsj.com/articles/twitter-accounts-of-bill-gates-jeff-bezos-elon-musk-appear-to-have-been-hacked-11594849077.

[3] Tim Starks, *Billions of Windows, Linux devices at risk from vulnerability that could give hackers "near total control," researchers say*, POLITICO (July 29, 2020), https://subscriber.politicopro.com/article/2020/07/billions-of-windows-linux-devices-at-risk-from-vulnerability-that-could-give-hackers-near-total-control-researchers-say-3982874.

Commerce Department study showed identity theft as the number one privacy and security issue concerning Americans.[4] Considering the harms Americans have in mind when they think about privacy, data security legislation is one of best things we can do for privacy.

The endemic use of data in our economy is not going away, and it supports not only the new ways that we all are working, worshiping, learning, and shopping, but countless jobs. Americans are putting an increasing amount of data online, a lot of which is sensitive. My view is that attempts broadly to roll back these trends are unlikely to succeed, and also would hurt consumers and the economy; so we need to focus on how to enjoy the fruits of progress while protecting Americans' data.

The data we put online are targets for criminals and hostile states. While the vast majority of attacks are thwarted, in 2019 there were still over 1,400 reported data breaches in the U.S., exposing over 160 million records.[5] The loss, corruption, and ransoming of these data can pose serious harm to people and businesses, including identity and intellectual property (IP) theft, exposure of sensitive data, years of expensive litigation, and so on. And, of course, inadequate data security is a profound national security issue.

At the FTC, we investigate and bring actions against companies that fail to maintain reasonable data security, or mislead consumers about it. Recent examples include our

[4] Rafi Goldberg, *Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds*, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (Aug. 20, 2018), https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds.

[5] 2019 End-of-Year Data Breach Report, IDENTITY THEFT RESOURCE CENTER (Jan. 28, 2020), https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/.

enforcements against DealerBuilt, an auto dealer software provider[6]; Retina-X, a stalkerware app (which also raised other privacy problems)[7]; and Equifax, the credit bureau we allege neglected to fix an Apache Strutts vulnerability, resulting in the theft of records of over 145 million Americans.[8] We're also imposing new requirements for defendants in data security orders, like certifications of compliance by senior officials and a better third-party assessor process.[9]

Statutes like COPPA[10] and Gramm-Leach-Bliley[11] give us data security authority in areas of heightened sensitivity, like kids' data and financial services; but the regime today has gaps, including in areas of particular vulnerability. Consider the Internet of Things. The proliferation of connected devices is good for consumers and the economy, but it creates risks—the manufacturer of a $15 device may not have an adequate incentive to secure it. We grappled with this issue in our 2017 suit against the wifi router company D-Link[12], and again just a few months ago in our settlement with Tapplock, a maker of smart locks.[13]

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), which builds up cybersecurity defenses in partnership with public and private

---

[6] *Lightyear Dealer Technologies, LLC, d/b/a DealerBuilt*, No. C-4687 (Sept. 6, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3051/lightyear-dealer-technologies-llc-matter-0 ("*DealerBuilt*").

[7] *Retina X Studios, LLC, and James N. Johns Jr.*, No. C-4711 (Mar. 27, 2020), https://www.ftc.gov/enforcement/cases-proceedings/172-3118/retina-x-studios-llc-matter.

[8] *FTC v. Equifax Inc.*, No. 1:19-cv-03297-TWT (N.D. Ga. July 23, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

[9] *See, e.g.,* Statement of the Federal Trade Commission, *Regarding Unizix, Inc. d/b/a/ i-Dressup.com, and Zhijun Liu and Xichen Zhang individually & James V. Grago Jr., d/b/a ClixSense.com* (Apr. 24, 2019), https://www.ftc.gov/system/files/documents/cases/2019-03-19_idressupclixsense_statement_final.pdf; *DealerBuilt*.

[10] 15 U.S.C. §§ 6501-6506.

[11] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

[12] *FTC v. D-Link Systems, Inc.*, No. 3:17-CV-39-JD (N. D. Cal. July 2, 2019), https://www.ftc.gov/enforcement/cases-proceedings/132-3157/d-link.

[13] *Tapplock, Inc.*, No. C-4718 (May 20, 2020), https://www.ftc.gov/enforcement/cases-proceedings/192-3011/tapplock-inc-matter.

entities, is also active on IOT. We regularly consult with CISA, and refer to them as a resource in our consumer and business education.[14] We also view use of CISA's tools, such as those that help businesses identify risks, favorably in our data security investigations. I think we ought to go further, and consider carrots and sticks to encourage participation with CISA through mechanisms like integrating their work into our orders.

Today, though, I want to stress the importance of the Commission's call for data security legislation. We need to be flexible to deal with rapid technological development, and mindful of the fact that defendants in data security cases are often themselves victims of felonies. But a specific congressional mandate and additional incentives to protect data are critical. As a report issued just days ago about many large public companies still failing to patch known vulnerabilities showed,[15] those who could most efficiently address data security problems often fail to do so.

Data privacy is something on which many of you have been working hard; and it's an important part of our mission and a priority. Data security legislation is one of the best things we can do to advance the goal of privacy.

Thank you, and I look forward to addressing your questions.

---

[14] Lisa Weintraub Schifferle, *Free vulnerability scanning for your business*, FEDERAL TRADE COMMISSION (Dec. 4, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/12/free-vulnerability-scanning-your-business.

[15] National/Industry/Cloud Exposure Report (NICER) 2020, RAPID7 (July 2020), https://www.rapid7.com/research/report/nicer-2020/.