Prepared Oral Statement of
Commissioner Noah Joshua Phillips
Before the
Committee on Commerce, Science, Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
"Oversight of the Federal Trade Commission"
November 27, 2018

Chairman Moran, Ranking Member Blumenthal, distinguished members of the Subcommittee, thank you for the opportunity to appear before you today. I'm honored to be back here with my fellow commissioners to highlight the important work that the FTC and its talented staff do every day on behalf of American consumers.

I'd like briefly to address two international issues, as well as the legislative process you have undertaken on consumer privacy.

While offering incredible opportunities for American consumers, the digital economy poses new challenges for law enforcement, particularly relating to cross-border activities. In 2006, Congress recognized this and passed the U.S. SAFE WEB Act,[1] allowing the FTC to share evidence with and assist foreign authorities in matters involving issues such as privacy violations and data breach. It also confirms our authority to challenge foreign frauds that harm U.S. consumers or involve material conduct in the United States.

[1] Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006.

Using SAFE WEB, the FTC has worked with foreign authorities to stop illegal conduct and secure millions for consumers, and sometimes even obtain criminal convictions. SAFE WEB is a vital tool, but it sunsets in 2020. Congress should reauthorize it, and eliminate the sunset provision.

The FTC works with the Department of Commerce to enable transatlantic data flows and support American business leadership through three cross-border data transfer programs, including the EU-U.S. Privacy Shield.[2] We look for Privacy Shield violations in four ways:

- Referrals from the Department of Commerce;
- Priority consideration of referrals from the European Union;
- Evaluating compliance as part of every privacy investigation; and
- Proactive monitoring of Privacy Shield participants.

We are committed to the success of these cross-border data transfer mechanisms, having brought nearly 50 related actions; and enforcement will remain a priority.

Finally, on the ongoing debate we are having as a nation on consumer privacy, I want to stress three points. First, "privacy" can be a nebulous concept. As you consider legislation, then, it is critical to be clear and frank about the wrongs

[2] The other two are the Swiss-U.S. Privacy Shield, and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (CPBR) System. Before Privacy Shield came into effect, the Commission enforced the predecessor EU-U.S. "Safe Harbor" agreement.

you seek to right. Advocates for new regulation invoke a variety of alleged market failures to justify new rules, from data insecurity to imperfect information about data sharing to 'creepiness' or 'surveillance'. According to the National Telecommunications and Information Administration (NTIA), while online privacy concerns appear generally to be declining, Americans' level of concern about privacy issues varies based on the subject, with people substantially more concerned about issues like identity theft and financial fraud than, for example, the collection of data by firms or the loss of control over data.[3] Reasonable minds can differ on privacy risks, but everyone should agree that the best policy is developed when aimed at clearly-defined harms, with consensus built around how to address them. High-profile incidents and large firms dominate headlines, but legal restrictions have an impact that is broader and more fundamental.

Second, any new rules will come with tradeoffs, to consumers, innovation, and competition. As I've said elsewhere, regulations can chill innovation and competition, including by entrenching incumbents.[4] We need to keep small businesses and startups in mind.

That is not to say that we should not re-evaluate our privacy regime given emerging issues and technologies; but neither can we ignore half a century of our nation's successful experience balancing privacy and other interests, including the tremendous levels of innovation we have seen. On innovation, American remains a

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

[4] Noah Joshua Phillips, Commissioner, Fed. Trade Comm'n, Keep It: Maintaining Competition in the Privacy Debate (July 27, 2018), https://www.ftc.gov/public-statements/2018/07/keep-it-maintaining-competition-privacy-debate.

world leader. I am concerned that early indications about the new European General Data Protection Regulation indicate reduced investment in technology[5] and greater concentration in ad-tech.[6]

The tradeoffs are not easy; and there are no simple answers. So, my third point is that, given the important value judgments that must be made, Congress is the place to make them. Broad delegations to an expert agency are a poor substitute for the lawmaking process our Founders created. I was honored to work here in the Senate for seven years, so I have great faith in the capacity of Congress to listen to the public, build consensus, and reach the right answer. Of course, the FTC, with our talented staff and half-century of experience enforcing privacy law, stands ready to assist in fashioning legislation, and will enforce any new privacy authority Congress deems fit to assign us.

Thank you for your time; I look forward to answering any questions you may have.

[5] *See* Jian Jia, Ginger Zhe Jin & Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment* (Nat'l Bureau of Econ. Research, Working Paper 25248, 2018), https://www.nber.org/papers/w25248.pdf.
[6] *GDPR - What happened?*, WHOTRACKSME BLOG (2018), https://whotracks.me/blog/gdpr-what-happened.html.