Thomas B. Pahl, Acting Director, Bureau of Consumer Protection
Federal Trade Commission
ABA/FCBA Privacy and Data Security Symposium
March 21, 2017

Good afternoon. Thank you for asking me here today to address what to expect from the Federal Trade Commission on privacy and security issues during the Trump Administration. Before I begin, I need to say that the views I express are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

As you know, President Trump recently selected Maureen Ohlhausen as Acting Chairman of the FTC. Acting Chairman Ohlhausen supports a free market approach to public policy. She is a practitioner of an approach to governing she describes as "regulatory humility" as well as being an ardent proponent of individual liberty.

Shortly after her selection, Acting Chairman Ohlhausen set forth her positive consumer protection agenda. Her agenda calls for the agency to focus its law enforcement work on addressing fraud and other unlawful conduct that causes concrete consumer injury. Further, it calls for more transparency as to how the agency operates and more clarity in standards for industry. Finally, her agenda calls for the agency to reduce undue and unnecessary burdens on industry, both through decreasing the burdens of FTC law enforcement investigations and decreasing the burdens of FTC regulations and orders.

My task as the Acting Director of the FTC's Bureau of Consumer Protection is to apply these principles to the work of the bureau. We need to be mindful of the legal and prudential limits on our use of governmental power, including in our enforcement work. At the same time, we need to be effective in our enforcement work to fulfill our core mission of protecting American consumers from harm.

Law Enforcement Priorities

Before turning specifically to privacy and data security, let me speak more generally about our plans for law enforcement, a critical focus given that the FTC is fundamentally a law enforcement agency. At the top of our agenda is refocusing on practices that cause the most harm to consumers. We will be increasing our focus on investigating and prosecuting those who engage in fraud. Indeed, stopping fraudulent schemes has long been an FTC's consumer protection priority, and it will be an even greater priority going forward.

We similarly will place an increased emphasis on investigating and prosecuting cases (including many fraud cases) in which the injury to consumers is concrete. Concrete harms include not only monetary injury, but also, for example, unwarranted health and safety risks. By focusing on practices that are actually harming or likely to harm consumers, the FTC can best use its limited resources. History further teaches that the FTC gets in trouble both in the courts and on

Capitol Hill if the agency is not focused like a laser on attacking fraud and other conduct that causes concrete harm.

In addition to identifying and pursuing appropriate targets, we are considering measures to make our law enforcement work more efficient. Part of making FTC law enforcement more efficient is reducing unnecessary investigations. We are exploring ways to provide more and even better guidance to industry. Guidance ensures that companies who want to comply with the law can do so. Not only does this save companies money, but it conserves FTC resources as well. Issuing guidance is far less expensive than litigation for bring legitimate companies into compliance.

We also are considering ways to make FTC investigations more efficient. For example, the recent ABA Antitrust Section's Presidential Transition Report stated there had been a recent trend towards generic and overbroad requests for documents and information in FTC civil investigative demands. The report asserted that such requests impose large and unnecessary compliance costs on companies. We are evaluating our civil investigative demands to determine if we can do a better of job of obtaining what we need without imposing unnecessary or undue costs on recipients.

Privacy and Data Security

So how does Acting Chairman Ohlhausen's positive consumer protection agenda specifically affect the FTC's privacy and data security program? The Commission will continue its active and leading role on privacy and data security. Most of the FTC's efforts relating to privacy and data security involve law enforcement, and the agency's enforcement authority derives from two main sources. First, the FTC enforces the FTC Act's prohibition on unfair and deceptive acts and practices, including enforcing them in the context of privacy and data security. Second, the FTC enforces statutes and rules that specifically address privacy or data security, such as the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the GLBA Safeguards Rule.

Over the years, the FTC has brought over 500 enforcement actions protecting the privacy of consumer information. These privacy cases have involved offline and online information, and companies large and small. These privacy cases also cover all parts of the Internet ecosystem, including social networks, search engines, ad networks, online retailers, mobile apps, and mobile handsets, as well as a vast array of deceptive claims and unfair conduct. In addition to these privacy cases, the FTC has brought approximately 60 data security cases over many years.

Consistent with the agency's overall consumer protection agenda, we will target our future privacy and data security enforcement on companies who engage in conduct that causes, or is likely to cause, harm to consumers, and on companies who do not keep their promises. For example, in our recent settlements with infidelity–promoting website Ashley Madison, there was evidence that several people committed suicide after their names and other information were exposed. Another example is our recent settlement with router manufacturer ASUS, whose products' critical security flaws put the home networks of hundreds of thousands of consumers at risk.

We also will continue to target for enforcement activity on companies who misuse sensitive data. For instance, we recently brought a case against inMobi for deceptively tracking the locations of hundreds of millions of consumers – including children – without their knowledge or consent and then serving them geo-targeted advertising. Likewise, we brought a case against Practice Fusion, a cloud-based electronic health record company, for soliciting patient reviews of their doctors without disclosing adequately that the company would post publicly the reviews on the Internet, thereby disclosing patients' sensitive personal and medical information.

Finally, we will continue to investigate and challenge conduct which violates the specific data security and privacy statutes, such as the GLBA, COPPA, and the FCRA, the Commission enforces.

I would be remiss not to mention the FTC's vigorous and extensive program of research and policy development which always has informed our law enforcement work. Acting Chairman Ohlhausen has directed FTC staff to conduct further research on the economics of privacy. Among other things, we will examine consumer privacy preferences and the relationship between access to consumer information and innovation. While this research is in its embryonic stages, it is the sort of undertaking that may have a significant impact over the long term on how the FTC and others address privacy issues, including through law enforcement.

Business Outreach and Consumer Education on Data Security and Privacy

Consumer education is critical in our efforts to empower consumers to protect themselves. Our business education efforts also help companies understand the law so they can comply with it. We will expand on our current, extensive consumer and business education and outreach efforts relating to privacy and data security.

For example, we are making a stepped up effort to educate small businesses. We are creating a one-stop shop on our website with data security

and privacy materials specifically for them. In addition, in the coming months, we will expand our business outreach on data security issues, with a focus on helping businesses identify risks and develop data security plans.

Much of the Commission's business education efforts have emphasized reviewing FTC complaints and orders to understand what businesses should not do. While these materials provide valuable information, businesses would benefit from even greater transparency. We therefore are undertaking a project to disclose more information about the data security investigations we close. This will help illustrate how the FTC staff has applied the principles in its long-standing data security guidance materials to decide when not to take enforcement action. We hope this information will provide businesses with an even better idea of what they should do when it comes to data security. Moreover, we hope this information will be especially useful to smaller businesses that are more likely to be reliant on such FTC guidance materials.

Cooperation with Partners on Data Security and Privacy

FTC and FCC cooperation will continue to be an agency priority under Acting Chairman Ohlhausen's leadership. The Commission has a long history of successful cooperation with all of our state and federal partners, including the FCC. For example, the FCC and FTC cooperated extensively in the implementation of the National Do Not Call Registry. We also continue to

cooperate in enforcement of the Do Not Call rules under a Memorandum of Understanding. In addition, in 2015, the FCC and the FTC affirmed and formalized their ongoing cooperation and coordination on consumer protection matters generally, and privacy and data security particularly, by entering into a second Memorandum of Understanding.

Let me give you some practical examples of FTC and FCC cooperation. The FTC recently provided input to support the FCC-initiated and industry-led Robocall Strike Force, which is working to deliver comprehensive solutions to prevent, detect, and filter unwanted robocalls. In tandem with this effort, the FTC worked with a major carrier and federal law enforcement partners to help block scam calls that were spoofing well-known IRS telephone numbers. We are continuing to support the Robocall Strike Force, particularly in its efforts to move forward with Caller ID authentication standards and to enhance industry traceback efforts. And FTC staff continues to work with its federal law enforcement partners and major carriers to encourage network-level blocking of mass robocall campaigns.

Another practical example of FTC and FCC cooperation arose from the FCC's implementation of the 2015 Budget Act amendments to the Telephone Consumer Protection Act (TCPA). These amendments directed the FCC to amend its rules implementing the TCPA to allow the federal government to robocall

consumers to collect federal government debts. In May 2016, the FCC issued a Notice of Proposed Rulemaking seeking public comment. In June 2016, FTC staff submitted a comment, urging caution with any expansion of permissible robocalling and recommending that the FCC create standards for collecting government debt consistent with the Fair Debt Collection Practices Act (FDCPA) and the Telemarketing Sales Rule (TSR). In August 2016, the FCC adopted several of the key recommendations made by FTC staff, including: (1) limiting covered calls to those directed at debtors; (2) prohibiting calls with advertising or marketing content; and (3) requiring callers to inform debtors of their right to request that calls stop.

The FTC's Jurisdiction over Common Carriers

One hot topic is the FCC and FTC's activities relating to broadband privacy. Before we get to the FCC's broadband privacy rule, it would be useful to provide a brief outline of the FTC's jurisdiction.

As I mentioned, the FTC has broad jurisdiction under the FTC Act to protect against unfair and deceptive practices. "Common carriers" subject to the Communications Act, however, are excepted from the FTC Act. The FTC has long called for Congress to repeal this exception, which dates from the time that phone companies engaged only in conduct that was common carriage.

Even with this exception, however, the FTC has jurisdiction over some

activities of common carriers under the FTC Act. The FTC and the FCC have for decades viewed the common carrier exception as "activity based," meaning the FTC *doesn't* have FTC Act jurisdiction over common carriers' provision of common carrier service ("the pipes") but *does* have FTC Act jurisdiction over their non-common carrier activities. Using this approach, the FTC has protected consumers from many activities of telecommunications common carriers. For example, we have challenged T-Mobile and AT&T's conduct in cramming charges on to the bills of consumers as well as challenged AT&T and TracFone's claims that they provide "unlimited data."

Reclassification of Broadband

As you know, in February 2015, the FCC adopted the Open Internet Order, which classified broadband as a common carrier service subject to Title II of the Communications Act. This Order had the effect of carving out broadband services from the FTC's jurisdiction. In October, after receiving extensive comments from FTC staff, the FCC adopted final privacy and security rules governing broadband. Earlier this month, the FCC decided to stay part of these broadband privacy rules. Acting Chairman Ohlhausen of the FTC issued a statement with Chairman Pai of the FCC supporting the FCC's decision. In the statement, the FTC and FCC heads explained that their goal is to ensure that the federal government applies consistent and cohesive privacy and data security rules for all companies. The way to achieve

this goal is for the FTC to set standards for privacy and data security. I agree that the same privacy and data security rules of the road should apply regardless of whether companies provide broadband services, data analytics, social media, or other so-called edge services.

Some argue that the FTC's approach to privacy and data security is somehow "too soft" or will not lead to robust consumer protection. I disagree. We are the iron fist inside a velvet glove. Let me mention a few examples of how the FTC has achieved strong privacy protections for consumers without imposing unnecessary or undue burdens on industry.

First, the FTC has ensured strong protections for sensitive information. Children's information is a prime example. The Rule the FTC promulgated under the Children's Online Privacy Protection Act is robust, covering a broad range of personal information and a broad range of entities, including kid-directed websites, as well as apps and third parties that collect children's data through these websites and apps. It clearly requires parental consent before kid-directed entities can collect information from children under 13. Because, however, the FTC can only enforce the COPPA rule against entities for which it has jurisdiction under the FTC Act, ISPs are not subject to the COPPA Rule when they provide broadband service. If the FTC had jurisdiction over these services, ISPs would be subject to important COPPA requirements that they are not subject to now.

Second, the FTC has aggressively used its authority under the FTC Act to require companies to maintain reasonable data security. As I mentioned above, we have brought approximately 60 data security cases over many years. Each of our orders in these cases require companies to maintain robust data security policies and procedures, similar to those enumerated in the FCC broadband rulemaking. And the orders go further – they require companies to get third-party audits of their data security program. Through these enforcement actions, as well as its strong education efforts, the FTC has delivered the message to entities in a range of fields – retailers, apps, data brokers, health companies, financial institutions, third party service providers, and others -- that they need to adopt and implement reasonable data security measures. The same approach and oversight should apply to broadband providers and traditional common carriers.

Finally, prior to the 2015 Open Internet Order, the FTC did investigate broadband providers. In 2009, we shut down a rogue ISP we alleged knowingly recruited, hosted, and participated in the distribution of spam, child pornography, and other harmful content. We investigated Verizon for issues related to the security of its routers, closing our investigation and issuing a closing letter in 2014.

As these examples aptly demonstrate, the FTC has a long and deep understanding of broadband. We stand ready to protect consumers in the broadband ecosystem if we have the opportunity to do so.

Conclusion

American philosopher Yogi Berra once explained, "It is hard to make predictions . . . especially about the future." The future of the FTC on data security and privacy matters generally will bear the imprint of Acting Chairman Ohlhausen' s positive consumer protection agenda. Despite the perils of forecasting, I have given you my predictions of what I think the future holds. Thank you for having me here today. I am happy to take any questions you have.