Thomas B. Pahl, Acting Director, Bureau of Consumer Protection
Federal Trade Commission
Free State Foundation Ninth Annual Telecom Policy Conference
May 31, 2017

Good afternoon. Thank you for the warm introduction and for asking me here today to discuss the FTC's future role with regard to online data security and privacy. 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.

In one generation, the Internet has transformed our lives. When I was a kid, I used encyclopedias to look up information and used a paper map to find my way. I shared a landline with my parents, and could only communicate by telephone with one friend at a time. My parents used travel agents to book vacation plans, endured interminable hold times to buy concert tickets, and hired people to perform home improvement projects we did not know how to do ourselves.

Today, my teenage son cannot even imagine living under these circumstances. He can look up historical trivia, current events, and song lyrics with the click of a button, anywhere, anytime. Through group chats and social media, he can communicate with dozens of friends at the same time. He can book concert tickets through StubHub and find discounts on Groupon. He can look at YouTube videos to learn to mow the lawn, cook dinner, or fix a broken bathroom floor tile. Being a teenager of course means that my son does not actually do any of these projects, but the knowhow is readily available online.

In the 2010s, technology has moved even faster with the rise of the Internet of Things. Almost any product you can imagine is being made now as a connected or "smart" version – from refrigerators and cars to home security systems, baby monitors, and even light bulbs, pillows, and clothing. Yes, smart clothing. Just last month, Amazon announced the new Echo Look, a hands-free, voice-controlled camera that records your looks from every angle and gives you fashion advice. My son will say I need Echo Look. My wife will say I really need it. And I will say: where is the off button!

In any event, these Internet developments have transformed, and will continue to transform, our lives. In large part, a free market, limited regulatory approach has fostered this transformation while protecting consumers from harm.

My boss, Acting FTC Chairman Maureen Ohlhausen has described her approach to governing as "regulatory humility." This means we must recognize the inherent limitations on our knowledge and our ability to predict the future in addressing public policy problems. These limits counsel not abdication but prudence when it comes to the use of governmental power. Let me discuss why I think the FTC applying such an approach to online data security and privacy would serve consumers very well.

It helps to start by going back to the future, specifically, turning the clock back to 2014. The FTC was the federal government's leading agency on privacy and data security matters. The agency was an active law enforcer bringing more than 500 privacy and data security-related cases. We challenged those who violated the prohibition on unfair and deceptive acts and practices in violation of the FTC Act. We also challenged those who violated other laws that specifically address privacy or data security, such as the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Gramm-Leach-Bliley Act.

The FTC's privacy and data security cases involved offline and online information, and companies large and small. They covered all parts of the Internet ecosystem, including social networks, search engines, ad networks, online retailers, mobile apps, and mobile handsets. In 2009, for example, we shut down a rogue ISP we alleged knowingly recruited, hosted, and participated in the distribution of spam, child pornography, and other harmful content. Another example is that we investigated Verizon for issues related to the security of its routers.

The FTC supplemented its enforcement activity with extensive business guidance, consumer education, and policy research and development. For example, in 2014 the FTC hosted a three-part Spring Privacy Series to examine the privacy and security implications of new technologies involving mobile device tracking, alternative scoring products, and connected health and fitness devices. FTC staff also hosted workshops on issues such as Big Data (2014), the Internet of Things (2013), and mobile security (2013). We also released several influential reports, ranging from our landmark 2012 privacy report, to more issue-specific reports on mobile privacy disclosures and data broker practices. And Commission staff released countless consumer and business education materials to provide tips for consumers and businesses to avoid potential privacy and data security harms.

In 2015, however, the FTC's role changed. The FCC issued its Open Internet Order to classify broadband service as a common carrier service under the Communications Act of 1934. Under the long-time views of both the FTC and the

FCC, including in a brief the FCC filed in the Ninth Circuit yesterday, the FTC lacks jurisdiction under the FTC Act with regard to the common carrier activities of common carriers. The FCC's Open Internet Order therefore effectively prevented the FTC from engaging in enforcement, rulemaking, and other consumer protection activities concerning ISPs' online data security and privacy.

In 2016, the FCC followed its Open Internet Order with the issuance of rules restricting and limiting ISPs' data security and privacy practices. In doing so, the FCC chose a more rigid and prescriptive approach to broadband data security and privacy issues than that reflected in the FTC's traditional case-by-case approach. The FCC's rules also set data security and privacy standards for broadband providers separate and apart from the standards applicable to others in the online space, eschewing the FTC's more holistic and comprehensive approach.

Under the leadership of Chairman Pai, the FCC in 2017 has taken a different tack. In March, the FCC stayed its privacy and data security broadband rules. Congress followed by using the Congressional Review Act to invalidate them and preclude the FCC from adopting substantially similar rules in the future. Earlier this month, the FCC also issued a Notice of Proposed Rulemaking under which it proposes to no longer classify broadband service as a common carrier service. This proceeding of course is ongoing. If the FCC were to make this proposed change final, the FTC likely would be able to use enforcement, rulemaking, and other activities to address broadband data security and privacy.

The FTC is ready, willing, and able to protect the data security and privacy of broadband subscribers. The FTC continues to be the leading federal government agency on data security and privacy issues. We have a wealth of consumer protection and competition experience and expertise that we bring to bear on online data security and privacy issues. We would apply data security and privacy standards to all companies that compete in online space, regardless of whether the companies provide broadband services, data analytics, social media, or other services. Our approach would ensure that the standards the government applies are comprehensive, consistent, and pro-competitive.

At the heart of the FTC's approach to online data security and privacy is tough but measured law enforcement, focused mainly on combatting unfair and deceptive acts and practices in violation of the FTC Act. We hold companies responsible for the privacy promises they make to consumers. We hold companies

accountable for their misuse of sensitive consumer data.[1] We hold companies responsible for not having reasonable data security practices.[2] As aptly illustrated by the FTC's track record, we use effective case-by-case enforcement to protect consumers, including those on online.

Some have argued it would be better for the government to address online data security and privacy through regulation rather than through case-by-case enforcement. Rulemaking imposes standards based on a prediction that they will be necessary and appropriate to address future conduct. Case-by-case enforcement, by contrast, involves no such prediction, because it challenges and remedies conduct that occurred in the past. Of course, such enforcement also has a prophylactic effect, as companies look at past enforcement to guide their conduct.

The Internet has evolved in ways we could not have predicted and it is likely to continue to do so. Given the challenges of making predictions about the Internet's future, we need case-by-case enforcement, which is strong yet flexible like steel guardrails. We do not need prescriptive regulation, which would be an iron cage.

Some of the advocates of regulating online data security and privacy emphasize the clarity and certainty that rules purportedly would bring. Yet this underestimates the guidance that companies can derive from other FTC activities. The complaints and orders in the FTC's more than 500 data security and privacy-related cases provide firms with critical information as to what conduct the FTC is likely to challenge. The FTC also has a long and successful history of educating businesses about their data security and privacy obligations. We continue to build on that work, focusing in particular on guidance for small businesses. For example, 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. Given the FTC's demonstrated ability to inform

[1] For instance, we recently brought a case against mobile app developer 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.

[2] For example, in our recent settlement 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.

companies what the law requires of them, there is no need to issue prescriptive rules governing online data security and privacy to convey guidance.

The call for rules to provide guidance on online data security and privacy also overestimates the guidance provided by prescriptive regulation. Prescriptive regulation can provide some certainty in the short term. But in fast-changing areas like online privacy and data security, regulations would need to be amended very often to remain current. Amending regulations is cumbersome and time-consuming, even where agencies can use APA notice and comment rulemaking procedures, and so such amendments are not likely to keep up. Out-of-date rules can be very unclear in their application to new technologies and cause confusion and unintended consequences in the marketplace.

The FTC knows that its approach to online data security and privacy must always look forward. Because the Internet continues to evolve, we need to evolve with it. At the FTC, we have demonstrated our commitment to learning about newer technologies, including new online technologies. We have an Office of Technology, Research, and Investigation – "OTech." Its technologists work with our investigators and prosecutors in developing and bringing cases involving newer technologies. They also encourage researchers to undertake projects at the intersection of technology and consumer protection.

We also have an active research agenda on data security and privacy issues. Just last week, we hosted a workshop on identity theft, where we explored new types of harm and called on stakeholders to conduct new research. Next month, we are hosting a workshop with the National Highway Transportation Safety Agency on connected cars, where we will discuss technology, privacy, and security issues. Finally, over the longer-term, the FTC is conducting and encouraging new research into the economics of privacy.

Note that this is the FTC's *current* data security and privacy research agenda – it is not carved in stone. Our agenda will respond to changes in technology and the marketplace, including those relating to online privacy and data security.

In conclusion, the law, the market, and the technology relating to online data security and privacy are always evolving. The FTC is ready, willing, and able to act to protect consumers who are online (including broadband subscribers) without

imposing unnecessary or undue burdens on industry. Thank you very much for having me here today, and I am happy to take any questions you have.