THE FUTURE OF BROADBAND PRIVACY AND THE OPEN INTERNET: WHO WILL PROTECT CONSUMERS?
Open Technology Institute
New America
April 17, 2017[1]

Thank you to the New America Foundation and Public Knowledge for hosting this event today - it is a fascinating and important time to have this conversation. We are close to the First 100 Days mark of the Trump Presidency. This milestone will come with articles and assessments about what has been accomplished and what has not -- which campaign promises have been fulfilled, and which have been missed.

Much of that attention will fall on health care, or the Supreme Court, or maybe international trade or taxes. Very little, if any, will focus on technology policy and the Internet. President Trump hardly mentioned Internet access, privacy, or consumer protection during the campaign.

What was said, wasn't alarming. In fact, much of it was favorable. Protecting the consumer and empowering entrepreneurship have been the foundation of bipartisan policy since the commercialization of the Internet really began in George H.W. Bush's Administration – and led to the passage of laws like the Do Not Call Registry and the Children's Online Privacy Protection Act.

Yet, what the First 100 Days have shown, and what the rest of this Congress and term portend, is that radical change on a host of issues seems likely despite the fact that these changes are deeply unpopular with the American public. The recent passage and enactment of the Congressional Review Act legislation on broadband privacy is the most notable. But we have also seen the first moves against the Open Internet Order; the rescission of rules meant to spur competition in cable boxes; and troubling statements made about encryption and consumer privacy.

All of these, taken together, show a departure from three decades of practice by Democratic and Republican administrations, practices that have helped spur our technological economy, while bringing information and American innovation to every corner of the globe.

Americans understand and value a free and open internet -- 81% support the concept of Internet nondiscrimination and 60% oppose the idea of paid fast lines for data. Not only is an open Internet with privacy protections and competition popular; it has been the status quo for much of the Internet Era- a status quo that has created a virtuous cycle of innovation, trust, adoption, and further innovation.

In fact, most Americans expect their sensitive data to be held securely and not used or shared without their consent -- 91% of Americans want more control over their data, not less. Even as

[1] The views expressed in this speech are my own and do not necessarily reflect those of the Commission or any other Commissioner.

we embrace a ubiquitous always-connected Internet, we also expect to retain meaningful choices over our data. We recognize that these choices are more meaningful as the technology transforming our lives is also clustering us into like-minded communities and offering us increasingly targeted experiences that not only impact how and with whom we communicate but also what opportunities are available to us.

So what is the future of broadband privacy and the Open Internet?

Let's begin with the recent broadband privacy debate.

No Cops On the Beat

One of the real problems with Congress's use of the Congressional Review Act to roll back the FCC privacy rule is that it shifts risk away from multi-billion dollar industry giants and onto American families.

The Federal Trade Commission cannot fill that gap because it does not currently have jurisdiction over the security and privacy practices of broadband, cable and wireless carriers.

What we have at the moment, in my opinion, is the rapid implementation of a "no cops on the beat" approach to privacy and data security in which control over who gets our sensitive information rests in the hands of a few very large companies that are the gatekeepers for our connections to modern life.

That will continue to be the case until Congress acts to fully repeal the common carrier exemption in the Federal Trade Commission Act.

We cannot count on the marketplace or competition to deliver us better options because our broadband markets are highly concentrated. In three-quarters of the country people have only one choice for a high-speed broadband connection.

But let's assume, for arguments sake, that Congress acts and the FTC's jurisdiction is expanded. Is putting privacy, security, and non-discrimination solely under the FTC even the right approach?

Can the FTC do it all?

First, let me underscore the tremendous regard I have for the FTC staff and the agency's 500 plus cases protecting the privacy and security of consumer information.[2] For more than two decades, the FTC has done a remarkable job protecting consumers as they have migrated from an analog world to a digital one.

---

[2] *See* FTC Staff Comment to the FCC: In the Matter of Protecting the Privacy of Consumers of Broadband and Other Telecommunications Services (May 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf

The FTC's efforts have focused on holding companies accountable for the promises they make about the information they use and collect. The agency has consistently focused on transparency, consumer choice, and security.

The FTC has taken the view that consent may be inferred for collection, sharing and use of information – that is consistent with the context of the transaction and conforms to consumers' reasonable expectations. Under this approach, the FTC supports use of opt-in consent for the collection and sharing of sensitive information including content of communications; social security numbers; health, financial, and children's information; and precise geolocation data.[3]

Recent FTC privacy cases have focused on ensuring that consumers' choices about their privacy are honored – and not defeated through clever technological work arounds. For example, in *InMobi* the FTC alleged that the mobile advertising network was using technology to track geolocation even when consumers had denied permission to access their location information.[4] In *Turn*, the FTC settled charges that the mobile ad network – which participated in the Verizon super cookie program - deceived consumers by leading them to believe they could reduce the extent to which the company tracked them online and on their mobile phones.[5] In *Vizio*, the FTC required consent for collection and use of television viewing activity.[6]

The FTC has also taken proactive steps – issuing warning letters to app developers who installed Silverpush software designed to monitor consumers television use through audio beacons[7] and urging companies engaged in cross-device tracking to get affirmative consent before cross-device tracking children or tracking sensitive topics like health, finances, geolocation.[8] Similarly, the FTC has recommended providing consumers with affirmative consent before sensitive information is collected and shared with data brokers – which are the companies that collect consumers personal information and resell it to others.[9]

---

[3] *See id.;* FTC Report, *Privacy & Data Security* (Dec 2016), *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf

[4] United States v. InMobi Pte Ltd., No. 3:16-cv-3474 (N.D. Cal. filed June 22, 2016),

https://www.ftc.gov/enforcement/cases-proceedings/152-3203/inmobi-pte-ltd.

[5] *Turn, Inc.*, Matter No. 1523099 (Dec. 20, 2016) (proposed consent), https://www.ftc.gov/enforcement/casesproceedings/152-3099/turn-inc-matter.

[6] FTC v. VIZIO, Inc., and VIZIO Inscape Services, LLC., No. 2:17-cv-00758 (D.N.J filed Feb 3, 2017) https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc

[7] *See* Press Release, Fed. Trade Comm'n, *FTC Issues Warning Letters to App Developers Using 'Silverpush' Code* (Mar 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code

[8] *See* FTC Report, *Cross-Device Tracking* (Jan 2017), *available at* https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

[9] FTC Report, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

The FTC is at the forefront of these issues because it recognizes that consumer data is both driving valuable innovation to the benefit of consumers – and creating some potential risks. Consumers are concerned about their private information being made public, or falling into the wrong hands, or being used to make important decisions about them. As our connections deepen and widen, it is possible to combine our data in ways that create increasingly intimate profiles about us without our knowledge – to determine, for example, whether we can afford a certain product or offer.

Against this backdrop, the FTC has repeatedly called for more tools to protect consumers - for strong comprehensive privacy and data security legislation that would protect consumers' privacy and data security across the marketplace.[10]

And, importantly, the FTC has worked with states and other government agencies to ensure a consistent approach to privacy and security.

The array of technology raising privacy and security concerns is growing as we connect more devices in our homes and on our bodies to the Internet. Differences between these technologies – and the risks associated with them – may justify some differences in how they are regulated.

The regulations for connected cars, medical devices and drones may vary slightly from those required for, for example, connected toasters. Arguably, an optimal approach would be for the FTC to work with expert industry regulators across government to craft policies that are right for the industry being regulated and consistent with the FTC's long established framework.

That is why the FTC worked with the FCC on its broadband privacy rule – and it is what the FTC is now doing, for example, with NHTSA on connected cars.[11] Privacy and security considerations are too important to be partitioned from core design and regulatory decisions.

I am sympathetic to the concerns raised by those who argue that given the growing complexity of our connectivity we must strive for simplicity and consistency in the area of privacy. Of course, inconsistent standards pervade US privacy and consumer law partly because we have long relied on a sector-based approach. If consistency were truly the goal, then we would likely increase protections for privacy, rather than unraveling them. That is the policy conversation we ought to be having – instead we are fighting a rear-guard action defending basic protections.

---

[10] *See* FTC Staff Comment to the FCC: In the Matter of Protecting the Privacy of Consumers of Broadband and Other Telecommunications Services (May 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf

[11] *See* FTC Comment to the National Highway Traffic Safety Administration Supporting the Inclusion of Consumer Privacy and Cybersecurity Guidance in the Document, "Federal Automated Vehicles Policy" (Nov 2016), *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/comment-jessica-l-rich-director-bureau-consumer-protection-ftc-national-highway-traffic-safety/ntsb_letter_comment112116.pdf ; *See* FTC Workshop, Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles, June 28, 2017, *available at https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected*

Protecting the Open Internet Requires Clear Rules & Strong Regulators

As I have just discussed – I do not think a one-size-fits-all approach to privacy and data security is realistic – and I do not think this approach would adequately protect the Open Internet.

There is not an either-or choice that must be made between FCC regulation and FTC enforcement. By design the agencies have different tools with different features. Both have a role to play when it comes to protecting consumers and ensuring an Internet that fosters innovation – and neither agency alone can do everything that needs to be done to promote competition and fully protect consumers.

First, the open Internet is, overwhelmingly, the status quo in the United Sates. The Internet is not its own sector. It is no longer even just a communications network. Today there are twice as many Internet-connected devices as people on the planet. In three years, that number is expected to triple.[12] By 2025, the value of these devices, and the ecosystem they operate in, is estimated to exceed four *trillion* dollars per year.[13] Thanks to all this connectivity, the Internet is a global, ambient always on system – vital to connect to the conveniences of modern life. It is no longer just a sector of our economy – it now touches nearly every sector. New content, applications and services generate increased consumer broadband demand, which in turn increases broadband infrastructure investment, which spurs innovation, creating ever more new content and applications. We now know this, thanks to the FCC's voluminous record, as the "virtuous cycle."[14]

Protecting the virtuous cycle – ensuring the internet remains a fountain of innovation - is at the heart of an open Internet policy. Eliminating the FCC's Open Internet Order will put us in uncharted territory.

Ex post, case-by-case antitrust enforcement is unable to offer the same protections to innovators as clear, ex ante rules. Under the Open Internet Order, innovators can have confidence that discriminatory network access will not threaten their chances for competitive success. Antitrust enforcement, on the other hand, would require detection, investigation and potentially lengthy rule of reason analysis. Remedying harm years after it occurs may prove challenging – or even impossible.

In fact, just last week, the FTC sent a comment to FERC supporting regulatory action to address competition concerns in electricity generation markets, noting the incentives of vertically integrated incumbents to harm competitors, specifically saying, "it could be costly, difficult and

---

[12] Press Release, Juniper Research, 'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020 (July 28, 2015), https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.

[13] JAMES MANYIKA ET AL., UNLOCKING THE POTENTIAL OF THE INTERNET OF THINGS 7 (McKinsey Global Institute, 2015), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[14] *See United States Telecom Association, et al v. FCC*, No. 15-1063 (D.C. Cir. 2016)

time consuming to detect and document" certain forms of anticompetitive discrimination in the interconnection space.[15]

The FCC also considered First Amendment interests such a free expression, diversity of political discourse and cultural development as a part of its Open Internet proceeding. These are non-economic values that are not generally protected by antitrust laws.

So if antitrust law enforcement alone is not sufficient to protect the Open Internet – is it sufficient to rely on commitments by ISPs to honor Open Internet principles?

I doubt it. Though we still haven't seen the specifics of the proposal, I have some questions. First, the obvious – if ISPs are going to make the same commitments, why roll back the Open Internet order in the first place?

Second, the FTC is a terrific consumer protection agency – but it doesn't have expertise in network engineering. The FCC has the relevant expertise – why not continue to rely on it?

Third, what happens if an ISP simply changes its policies and commitments in the future?

Fourth, how will individual consumers detect and complain about violations? Even if they can, will the available remedies be sufficient – especially after the time it takes to investigate and bring cases?

Finally, what recourse will innovators, entrepreneurs and edge providers have in this new framework? The answer to the last question is particularly critical if we are to preserve the open Internet as a platform and driver of innovation. In markets that are highly concentrated – markets like our broadband markets – adopting policies that strongly favor behemoth incumbents can slow innovation, chill entry, and harm free markets. In these markets, we need all the public policy tools at our disposal – regardless of which agency they reside in – to safeguard an open and nondiscriminatory internet.[16]

Thank you again to the New America Foundation and the Open Technology Institute for having me here at this important time. I look forward to the discussion we are about to have.

---

[15] *See* FTC Staff Comment Before the Federal Energy Regulatory Commission Concerning "Reform of Generator Interconnection Procedures and Agreements" (April 10, 2017), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commission-federal-energy-regulatory-commission-concerning-reform/v170004_ferc_interconnection_ftc_staff_comment.pdf

[16] Jon Sallet, Deputy Assistant Attorney General, Department of Justice, *Broadband Competition Policy: Final Thoughts and First Principles* (Dec 16, 2016), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-jon-sallet-antitrust-division-delivers-remarks-capitol