THE CHALLENGE OF NEW TECHNOLOGIES AT A TIME OF TRANSITION
FEDERAL COMMUNICATIONS BAR ASSOCIATION
Practicing Law Institute
December 1, 2016
Keynote Remarks by Commissioner Terrell McSweeny[1]

Good afternoon everyone. I want to thank the Practicing Law Institute and the Federal Communications Bar Association for having me here today, and allowing me to speak on how the FTC is approaching new and transformational technologies.

This morning you've already spent some time exploring the FTC's recent privacy and security enforcement and education initiatives, big data, IoT, advertising, breach legislation – all incredibly important topics. So I thought I'd take a few minutes of your time to address why getting consumer protection right at this time of rapid change really matters – not just to protect the little guy – but also to foster innovation.

Technology is producing changes in our lives and changes in the economy at a rate not seen since the Industrial Revolution.

Fifty years ago, Gordon Moore published his seminal work predicting an ever increasing capacity to "cram more and more components onto integrated circuits." He further quantified this "cramming" into what we now know as Moore's Law – the regular doubling of the components in an integrated circuit.

Since that paper was published, we've seen the processing capacity of computers double nearly every two years.

What that means in real terms is a regular doubling of the processing power of a microchip.

Computers have gone from desktops, to laptops, to handheld smartphones – each with more power, memory, and capability than the one preceding it. Our connected technology is getting smarter, faster and more ubiquitous. Today 90% of American adults use the Internet, 81% of Americans use smartphones.

And smartphones are just the beginning.

Two years ago self-driving cars were an oddity on the back lots of tech companies in the Valley – this Fall they were out on the streets of Pittsburgh picking up Uber passengers.

There has also been an explosion of sensors and Internet connected devices at increasingly lower and lower prices.

[1] I would like to thank Joshua Tzuker for his contributions to this speech. The views expressed in this speech are my own and do not necessarily reflect those of the Commission or any other Commissioner.

Today, there are twice as many Internet-connected devices in the world as there are people.[2] That number is projected to triple within the next five years.

By 2020, there will be an estimated 38 billion Internet-connected devices in use worldwide.[3]

The impact of increased connectivity on our economies cannot be overstated. In 1995, almost at the dawn of the commercial Internet, the total market capitalization of public Internet companies was $16 billion. Last year the total market cap of just the top 15 firms was $2.4 trillion.

From McKinsey "by 2025, the total value of the Internet of Things space (including industrial and municipal IoT) will at minimum be $4 trillion/yr.[4]

The growth in value, the growth in new types of work, and the impact of these new services is predicated on the flow of information – of data.

Last year, Cisco released a report predicting that the Internet of Things will generate more than 500 zettabytes of data a year by 2019 – or the rough equivalent of all the data created from the dawn of the written word to the dawn of the Internet.[5]

This data – and the increasingly smart technology (algorithms, machine learning, AI) operating on it - is creating new opportunities for better products, lower prices, more personalization, and stronger networks. It is fostering not only new jobs and new businesses but also entirely new industries.

The Internet is no longer a communications network or even a sector of our economy – it is becoming a global, immersive ambient system. We have never seen this much change in this short a period of time on this many fronts. All this connectivity poses some real challenges for policy makers, regulators and enforcers.

How do we optimize for rapid innovation to remain a world leader in the development of new technology while mitigating some of the consequences of all this change – addressing digital divides, insuring data sets are high-quality and representative, increasing digital readiness, and protecting jobs, privacy and security? How do we respond to changing social norms around data sharing? How do we make sure consumers, who want to benefit from all of this innovation, have choices and transparency? What additional protections do consumers need? As the technology gets smarter, how and when do we protect human agency?

---

[2] *See* Juniper Research, Internet of Things Connected Devices to Almost Triple to Over 38 Billion Units by 2020, July 28, 2015, http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.

[3] *See id*.

[4] James Manyika et al., MCKINSEY GLOBAL INSTITUTE, THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE, June 2015, at 7, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

[5] Cisco Global Cloud Index: Forecast and Methodology, 2014–2019 White Paper (April 21, 2016) at 17, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf

Policy makers often wrestle with whether an enforcement-based, voluntary best-practices approach can adequately protect innovators and consumers – and whether, in the face of dynamism, regulations are appropriate or can keep pace with rapid market changes.

These are legitimate questions – I'd argue that smart government requires a combination of tech-neutral, tech-informed enforcement, engagement between regulators and enforcers across the government and narrowly tailored regulation in key areas in order to insure that consumers are protected and that markets are competitive.

I feel fortunate to be at the Federal Trade Commission during this era of rapid change. As independent agencies go, we are a fairly old one. We were established by the Wilson Administration to address one of the central economic questions of that period – how to restore competition and protect consumers against the unregulated economic power of concentrated wealth and monopolies. Themes that, a hundred years later, sound awfully familiar.

The FTC was given the broad mandate that we should make the marketplace fair for competition and for consumers. We were instructed also, importantly, to study trends in the marketplace to inform both our enforcement and policy makers – and given a relatively flexible mandate to keep pace with a dynamic market.

Fascinatingly – the role of data (and the data advantages conferred by scale) – were an issue even then. Louis Brandeis, one of the architects of the FTC, noted "there is one respect in which the great industry has an important advantage, that is in the collection, the getting of knowledge for which great concerns extend their bases of inquiry all over the world." He argued that the FTC could serve to help small business get access to the same information in order to compete in new markets.[6]

It's actually pretty impressive how prescient the FTC's founders were – and I think they would be pleased to see that the FTC has evolved to keep pace with the American marketplace – fostering innovation, advocating for disruptive competitive and ensuring that new technologies enter the market – while the same time acting to protect consumers.

As the economy has transitioned to the Digital Age, so has the FTC. More and more, the Federal Trade Commission moves in a world of data and disruptors, Internet connected devices, privacy policies, and international data flows.

In recent years, much of our mission has been protecting the digital consumer and the digital marketplace – and bringing hundreds of general privacy and data security cases.

As new digital and online products and services made their way into the marketplace, the FTC has been an advocate for their disruption. When Internet retailers first began making sales to consumers, incumbent brick and mortar retailers sought to block these entrants in a number of markets. The FTC advocated against regulatory barriers to online entry in markets ranging from

[6] JEFFERY ROSEN, LOUIS D. BRANDEIS: AMERICAN PROPHET, 65 (2016).

contact lenses to wine shipments.[7] We continue to be a forceful advocate for the competition introduced by innovators.

But we are also mindful that the explosion of connectivity is creating new risks for consumers, new enterprises for criminals, new opportunities for prejudice and discrimination, new risks for consumer privacy, and potentially new impediments for innovators to enter the marketplace.

When the FTC first began to look at online privacy, it did so in order to build consumer trust in making purchases on a new-fangled thing called the world wide web. This was less than 20 years ago in a time when the chirp "you've got mail" was still an exciting thing to hear – while that all seems quaint in 2016 – consumer trust is still central to demand and adoption of new technology.

Earlier this year, the National Telecommunications and Information Administration released a survey finding 84% of households expressed concern about online privacy or security and 45% of Internet users chose to avoid an online product, service, or device because of safety or security concerns.

The FTC's enforcement, business education, and consumer outreach programs are vital to reverse this trend. But alone, they aren't enough – because our connectivity is rapidly extending to every part of our lives – our cars, our bodies, our homes, our children's toys.

I suspect we are only at the beginning of a deepening of consumer distrust – which may harm adoption and demand for all these wonderful connected innovations.

As our connectivity deepens and becomes more intimate – so too does our vulnerability.

Last year, the FTC issued a report on the rapidly growing Internet of Things. The report highlighted the very real security issues the adoption of Internet connected devices present to consumers and developers. Lightbulbs, thermostats, and ovens that can be turned on from a phone can also be entry points for attacks, surveillance and data breaches.

We are already seeing Internet connected devices used as vectors for massive denial of service attacks. These attacks have the potential not just to disable websites but also critical infrastructure. Insecure devices connected to the Internet can be exploited in a matter of minutes.[8]

This Fall, our focus at the FTC has turned to the challenging problem of ransomware. Ransomware will increasingly be a problem for ordinary consumers – just ask San Francisco's

---

[7] *See, e.g.*, Staff of the Fed. Trade Comm;n, Possible Anticompetitive Barriers to E-Commerce: Contact Lenses (Mar. 29, 2004), http://www.ftc.gov/os/2004/03/040329clreportfinal.pdf*;* Letter from Susan Creighton, Director of the Bureau of Competition, FTC, et al. to New York Assemblyman William Magee et al. (Mar. 29, 2004), http://www.ftc.gov/be/v040012.pdf;

[8] Andrew McGill, *The Inevitability of Being Hacked*, THE ATLANTIC, (Oct 28, 2016), http://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/

Muni riders. Imagine what a nuisance ransomware will be when it involves paying a toll to turn on your refrigerator or stop your car radio from blaring.

There are a number of issues industry and regulators need to develop best practices around. For instance, can consumers be trusted to update products on their own or should these devices be automatically updated as patches and operating systems improve and new vulnerabilities are discovered?

How long should a company support a product in the field? How do you update devices, inform consumers, and maintain these arrangements throughout the expectant life of the product? What are the responsibilities of a manufacturer if they brick a product early or unexpectedly? These are questions we are grappling with at the FTC, and as the sector grows these will become more important.

All of these issues will need answers in order to establish reasonable consumer expectations, and to ensure continued innovation and development in Internet connected devices.

Importantly, the FTC is not the only agency grappling with these issues – expert regulators are confronting them in cars, drones, critical infrastructure medical devices, financial institutions and communications. That's why the FTC has not only continually engaged in sharing our approach to privacy and security with other agencies, but also recommended – on a bipartisan basis – comprehensive data security legislation, and comprehensive privacy legislation.

Because we're really just at the beginning. Our rapidly scaling connectivity and increasing processing power is creating data feeding algorithms and smarter technology, and those algorithms, in turn, affect consumer choice implicating our laws and our public policy along the way.

Algorithms, machine learning, AI are raising some pretty challenging questions regarding the role of human beings in decision making.

There can be a tendency to overestimate the accuracy or insightfulness of these tools precisely because they are so powerful and they hold so much potential. As has become abundantly clear in the last year, algorithms and artificial intelligence are far from infallible.

Against this backdrop, we have attempted to make informed decisions that will both protect consumers and competition – and promote innovation.

At the FTC we primarily do this through enforcement, at other agencies it takes place through stakeholder engagement and guidance – and even regulation.

While the FTC has broad authority to protect consumers, I happen to believe that the best way to protect the most people is to have more than one cop on the beat.

For instance, the FTC can police edge providers and device manufacturers, but we lack jurisdiction over common carriers.

We can try to weed out the most harmful anticompetitive behavior through ex post antitrust enforcement – but we can't protect Internet openness and all the innovation that will flow from it with strong ex ante rules like the ones the FCC enacted.

Nor can we, through enforcement alone, provide a guarantee to consumers that they will be able to control what personal data about them is used and shared by the providers of their connectivity.

In areas of new technologies, like medical devices or connected cars, the FTC's general privacy expertise might need to be augmented by scientists at the FDA or engineers at NHTSA.

Meanwhile, some of the largest data breaches affecting the most consumers have happened at universities and health systems- entities that are often out of our jurisdiction because they are non-profits.

It is through a robust, shared-enforcement model that these cross-cutting cross-jurisdictional issues can be properly evaluated and, if need be, regulated. This makes sense, not only as a way to ensure consumer trust, but also to maximize government efficiency at a time of resource constraints.

So where are we headed on these issues?

Next year we will have a new Administration. Although personnel and policy will change, the importance and centrality of these issues will not. In fact, they will only grow in significance.

Like most in this room, I have no special insight into where President Trump is on these issues, or his views of technology writ large.

I can only speak from my own perspective. I believe it would be a mistake for the next Administration to back away from progress we are making – like opening data for innovation, bringing technologists into government to inform policy decisions, engaging in smart enforcement, promulgating guidance and – yes – even well designed regulations where there is a sound basis to do so.

There is not an either-or choice that must be made between smart regulation by an expert regulator on the one hand and enforcement by a competition/consumer protection enforcer on the other. Both are different tools with different features that have a role to play in protecting consumers, promoting competitive markets and fostering innovation.

Of course, it is a challenge to keep pace with a dynamic market – but the ample record in the FCC's Open Internet proceeding underscores the enormous benefit to consumers and innovators of preserving network access through clear ex ante rules.

That is overwhelmingly the status quo in the US – and insuring that the Internet remains a fountain of innovation and disruption is at the heart of open Internet policy.

The elimination of it would put us in uncharted territory.

It doesn't take an expert political prognosticator or legal mind to figure out that some of the most contentious FCC decisions of recent years could be reversed by the incoming Administration.

I suspect the FCC's privacy rule will be in the cross hairs. Rolling it back will be an unfortunate result for consumers – not just because it will weaken their privacy but also because, without reform of the FTC's jurisdiction over common carriers, it will leave consumers with very little protection at the federal level and potentially create further skepticism among our European partners of hard fought agreements that facilitate vital cross border data flows like the US-EU Privacy Shield framework.

In the last eight years, the economy has changed dramatically. I believe we have achieved a bipartisan consensus at the FTC on how to approach many of the issues I have outlined today. We are working hard to bring this knowledge to other government agencies that also have a role to play. It is my fervent hope that we maintain this collegiality, bipartisanship, and constructive engagement over the next four years - and that the incoming Administration continues this important work, which has enabled the American economy to produce world-class innovation while also ensuring consumers have trust in their safety and security.