**TecNation 2016**

**September 20, 2016**

**United States Chamber of Commerce**

Thank you for that warm introduction. It is an honor to be here as part of TecNation 2016.

I just want to start off by making the usual disclaimer, the opinions in this speech are my own and are not reflective of my fellow Commissioners or the staff of the Federal Trade Commission.

Today I'm going to talk about consumer protection in the age of hyperconnectivity.

The pace of change from technology- both from the products being created to how our governing institutions must respond- is occurring at a velocity that is unparalleled in our experience.

I was sworn in as a Commissioner two years ago.

At that time self-driving cars were an experiment in the back lot of Google. Last week a fleet of semi-autonomous Ford Fusions took to the streets of Pittsburgh to pick up passengers for Uber.

When I was sworn in, about 50% of Americans had smart phones. Next year, projections are that more than 80% will have them – worldwide, nearly half of all adults will own smartphones.

When I was sworn in, the term "selfie" was not yet in the Oxford English Dictionary…well, not all technological change is for the better.

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 and we were given the broad mandate that we should make the marketplace fair for competition and for consumers.

Over our 101 years, the Federal Trade Commission has been where the American marketplace is. On the consumer side, in the 1940s it could mean ensuring that a purported mink coat actually used mink fur, while in the 1990s it could mean claims surrounding a weight loss product.

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. The consumer's marketplace is no longer the corner store of the 1920s, or the mall of the 1980s, it is now likely to be their handheld device.

In 1966, Gordon Moore published his seminal work predicting an ever increasing capacity to, as he wrote; "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 **i**n 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 handhelds each with more power, memory, and capability than the one preceding it.

There has been an explosion of sensors and Internet connected devices at increasingly lower and lower prices. Last year, Cisco released a report that the Internet of Things will generate more than 400 zetabytes of data a year by 2018[1]- or the rough equivalent of all the data created from the dawn of the written word to the dawn of the Internet.

This data is creating new opportunities for better products, lower prices, more personalization, stronger networks, while helping to foster new businesses and even entirely new industries.

On the opposite side of the ledger, the explosion of data collection is creating new risks for consumers, new enterprises for criminals, new opportunities for prejudice and discrimination, and potentially new impediments for innovators to enter the marketplace.

---

[1] Cisco: The Zetabyte Era-Trends and Analysis, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

The FTC plays an important role in guarding against those down side risks and ensuring the digital marketplace offers the same protections and expectations of the analog one.

For all the innovation and empowerment that can be unleashed by our data revolution, I think my colleague Commissioner Ohlhausen put it best by saying, "Big data isn't knowledge or wisdom." It is a tool, and like any other tool, it can be used for good or ill.

That is where policy makers, regulators, and enforcers come in and it is where the FTC will have to take our consumer protection mission. The FTC already focuses on data security and privacy – but increasingly our hyperconnectivity, and the massive amount of data generated by it, is raising new issues in antitrust and consumer protection.

To begin with, data can only positively affect people's lives if the data itself is good. Too often in this country, the poor, the disabled, the elderly, and new immigrants are not adequately counted.

Two years ago, the city of Boston unveiled an app called Street Bump. It allowed drivers to report potholes and other road hazards directly to the public works department from their smartphones.

After a few weeks, the City began noticing that there were far more hazards and potholes in wealthy neighborhoods than in poorer areas of the city. Clearly, the

data collected was skewed. Wealthy people downloaded the app. Wealthy people drove private cars. Poorer people didn't have smartphones. They often took the bus. It became obvious to the City that an innovative and cost-effective way of tackling a nagging problem was exacerbating inequality.

In fact, many of the most intractable problems we face as a nation have their roots in how we gathered and used data as policy makers and businesses.

It might not have been done with computers and algorithms, but for most of the twentieth century banks and government agencies produced data sets on where, and for whom, loans could be made and houses could be sold.

They created maps that redlined communities and enforced a rigid segregation based on race and class. This was big data, albeit collected through analog means, used for discriminatory purposes and it has left a legacy that we are struggling to correct.

With that tragic history as a backdrop, the Leadership Conference on Civil Rights issued a set of principles to ensure that our new data era is one of empowerment and opportunity rather than one of data driven prejudice.

Among their principles is that audit mechanisms should be used to limit risks of profiling and discrimination. They also ask that computerized decision making- especially in the areas of employment, education, and health- be subjected to human oversight to be consistent with good public policy.

I believe these are necessary goals for government and industry.

This year, the FTC released a report entitled "Big Data: A Tool for Inclusion or Exclusion?" that underscores the need for transparency and oversight – and outlines the way in which antidiscrimination statutes like FCRA, that have their origin in the brick and mortar world, apply in the digital one.[2]

For years, the FTC has promoted "Privacy by Design" and "Security by Design"- both concepts seek to protect consumers' privacy and security from the outset of product design.

In an era when algorithms and big data sets can hire and fire, inform health care decisions, and extend financial opportunities it is vital that these technologies do not run counter to established legal protections or public policy goals. In the same way companies incorporate privacy and security, so to should we have Data Ethics by Design.

For companies, part of this will mean a modicum of transparency in the use and methods we attach to data. Part of it will mean more rigorous testing and part of it will mean speaking with stakeholders and communities that are typically not engaged in product development.

---

[2] *See* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION 1-2 (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

Ensuring there is trust in the algorithms and machine learning goes hand in hand with ensuring consumers trust the security of their data and devices. This trust is essential to adoption -- to making sure that there is actually demand for all the data driven innovation and new IoT products.

We know consumer trust in connectivity is at a relatively low point. Recent survey data shows that 84 percent of US households expressed concern about privacy and data security. Identity theft continues to be the top complaint in our consumer complaint database – with hundreds of thousands of incidents reported to us each year.

So as an enforcer, the FTC will continue to operate a vigorous privacy and data security program. This year alone we have announced several privacy and data security cases involving health information, children's information, and security of IoT devices.

For example, we recently brought a case against a router manufacturer ASUS. Home routers are the central nervous system for our networks and personal devices. Poorly secured routers could result in infected appliances and computers, stolen data, and identity theft.

In ASUS, we alleged that the company's failure to test its routers prior to launch contributed to several breaches and was an unfair and deceptive trade practice under Section 5 of the FTC Act.

This year we also brought our first case against a mobile ad network – InMobi. InMobi offers an ad platform for app developers and advertisers. By using InMobi's software development kit, developers could sell ad space in their apps. Geolocation is a valuable data point in these markets. So InMobi offered products that could target consumers' location. HOWEVER, InMobi also sidestepped consumers geolocation settings on their phones by collecting information regarding the wifi networks their devices connected to and triangulating their location.

This case underscores the core principles that the FTC's privacy program is founded on: transparency, choice (including affirmative express consent before retroactive changes are made, meaningful choices around collection of sensitive information) and context (collection and use consistent with consumer expectation).

Enforcement on the consumer protection side is only one area of our work. We are also increasingly called upon to understand the technology to maintain a competitive marketplace. Some times that means weighing in on behalf of new entrants. While others times it is trying to understand how Big Data can affect markets.

First, let me stress that data – even massive amounts of it – are nothing new in antitrust. What *is* changing in the digital economy is the volume, velocity, variety and value of data – or the four Vs. Each of these categories is growing briskly – there is more data than ever before, companies can accumulate and analyze data faster than ever before, and increasingly sophisticated data analytics permit

companies to combine and jointly analyze more previously disparate sources of data than ever before.[3]

For competition enforcers, the four Vs of data raise some questions such as: does "big data" constitute a relevant market and can "big data" be a barrier to entry? The short answer to both these questions is: yes. The longer answer is that it depends on the facts.

In the big data world, there are a lot of data that anyone can obtain for a fairly nominal cost. But there are also a lot of valuable data that *are* proprietary and can operate as a barrier to entry.

An incumbent may have a significant advantage over entrants if it possesses a valuable database that would be difficult, costly, or time consuming for a new firm to match or replicate. In those situations, competition enforcers can and should assess the competitive implications of data.

The FTC has treated data as a relevant market in one recent case and found it to be a barrier to entry in others based on the specific facts and circumstances of those cases.[4] But a one-size-fits-all view of data holdings is not the right approach in a world where so much data is available and so easily gathered. [5]

---

[3] *Ibid*

[4] In *Dun & Bradstreet-Quality Education Data* (2010), the FTC determined that data, itself, was the relevant product. The FTC found that the parties "were the only significant U.S. suppliers of [K-12] educational marketing data." Analysis of Agreement Containing Consent Order to Aid Public Comment, In the Matter of The Dun & Bradstreet Corporation, Dkt. No. 9342, at 1 (Sept. 10, 2010), https://www.ftc.gov/sites/default/files/documents/cases/2010/09/100910dunbradstreetanal.pdf.

In *Nielsen-Arbitron* (2013), the FTC determined that the proprietary data of Nielsen and Arbitron was a key input to offering downstream cross-platform audience measurement services. The FTC found access to television audience data with individual-level demographic information to be a significant barrier to entry in that matter.

Another important topic when it comes to big data is the relationship between antitrust law and concerns related to privacy and data protection – some of the complex consumer protection areas that I have been discussing.

In general, I see antitrust enforcement and the broader policy concerns regarding privacy and data protections as two separate, but important areas. As I've noted, our hyperconnectivity poses consumer protection policy issues that are multi-dimentional – involving equal opportunity, non-discrimination, data security.

Of course, competition enforcement and privacy can intersect. The FTC has yet to challenge a merger specifically over whether it would lead to less privacy protections, but we have recognized the possibility that consumer privacy can be part of the competition between firms.

But, absent a clear link to competition, I believe that privacy and data protection concerns are best handled as consumer protection issues. I believe that it is

---

Analysis of Agreement Containing Consent Order to Aid Public Comment, In the Matter of Nielsen Holdings N.V. and Arbitron Inc., File No. 131-0058 (Sept. 20, 2013) at 3, https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130920nielsenarbitronanalysis.pdf.

And in in *Reed Elsevier-ChoicePoint* (2008), the FTC treated data as an input in the market for electronic public records services for law enforcement customers. Reed Elsevier's Lexis-Nexis and ChoicePoint were the largest suppliers of public records services, with a combined 80% market share. The FTC found that the parties' combination of data and analytics were unique among electronic public records services and that other firms lacked the data an analytics to compete effectively for law enforcement customers. Analysis of Agreement Containing Consent Order to Aid Public Comment, In the Matter of Reed Elsevier and ChoicePoint, File No. 081-0133 (Sept. 16, 2008) at 2, https://www.ftc.gov/sites/default/files/documents/cases/2008/09/080916reedelseviercpanal.pdf.

[5] For example, the FTC decided to close its *Google-DoubleClick* investigation in 2007. Staff examined whether the combination would enhance Google's power in the ad intermediation market and concluded that it would not. The FTC found that "neither the data available to Google, nor the data available to DoubleClick, constitutes an essential input to a successful online advertising product." Statement of the Fed. Trade Comm'n Concerning Google/DoubleClick (Dec. 20, 2007), File No. 071-0170 at 12, https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

dangerous to engage in competition analysis based on what we think consumers *should* want or value, independent of market realities. Doing this would cross the line from antitrust enforcement to market regulation.

The FTC has advocated for greater transparency and choice in privacy and data protection policies. We also would Congress to pass general privacy legislation, data security and breach notification legislation, and data broker legislation.[6] We can and should do better in these areas. But we shouldn't use antitrust laws to solve policy issues they are ill-suited to address.

The rise of high-velocity computerized markets also present a new frontier for antitrust enforcers. Last year, DOJ brought a case for price fixing against two e-commerce sellers who agreed to align their algorithms to increase prices for online poster sales.[7] In that case, humans reached the agreement to fix prices. But as algorithms become more sophisticated, there is the possibility that they may engage in consciously parallel pricing behavior on their own initiative. The competitive harm associated with price-fixing is the same whether initiated by humans or algorithms. For that reason, some have suggested that the latter may require revisions to antitrust's historic focus on "agreement" and "intent."[8]

---

[6] *See, e.g.,*FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[7] *See* Press Release, U.S. Dep't of Justice, Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution (Apr. 6, 2015), http://www.justice.gov/opa/pr/former-ecommerce-executive-charged-price-fixing-antitrust-divisions-first-online-marketplace.

[8] *Id*. at 37-38.

An increase in the sophistication of pricing algorithms could also lead to narrower product market definitions in the future. Under the 2010 Horizontal Merger Guidelines, we specifically evaluate the possibility of price discrimination against targeted customers.[9] Moreover, the *Guidelines* explain that "[w]hen discrimination is reasonably likely, the Agencies may evaluate competitive effects separately by type of customer."[10] By using big data and algorithms to engage in in increasingly targeted price discrimination, companies may create more and narrower relevant product markets.

## CONCLUSION

As we advance further into the 21st century – complete with its brave new world of innovation, big data, and novel technology – we will face new challenges as competition and consumer protection enforcers. We must be mindful of these challenges, yet we must also continue to be aggressive in advancing our mission to protect consumers and to promote competition.

[9] U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, 2010 HORIZONTAL MERGER GUIDELINES § 3.

[10] *Id*.