BIG DATA: INDIVIDUAL RIGHTS AND SMART ENFORCEMENT
European Data Protection Supervisor-BEUC Joint Conference
Brussels, Belgium
September 29, 2016
Remarks of Commissioner Terrell McSweeny[1]

It is an honor to be here as part of this conference. As many of you know, the U.S. Federal Trade Commission is both a competition and consumer protection enforcer. Today I am going to talk about how the FTC is undertaking its mission to protect consumers in our hyperconnected world and where I think this mission will take us in the future.

Protecting Consumers in a Hyperconnected World

The pace of change of 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 and a half years ago or about 2.5 trillion Google searches ago. At that time, self-driving cars were an experimental oddity confined to the backlots of some tech companies. Two weeks ago, 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, about 25% of adults worldwide had them. Next year, projections are that more than 80% of Americans will have them and nearly half of all adults worldwide will own one. In 1965, Intel Co-Founder, Gordon Moore published his seminal work predicting an ever increasing capacity to, as he wrote; "Cram more and more components onto integrated circuits."[2]

He further quantified this "cramming" into what we now know as Moore's Law, the regular doubling of the components in an integrated circuit every two years. Since that paper was published, we've seen the processing capacity of computers double nearly every two years. This, in turn, is creating more and deeper Internet connectivity than ever before and increasing the volume and variety of data collected about consumers and increasing the velocity with which data be analyzed and used.

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

[2] Gordon E. Moore, "Cramming More Components onto Integrated Circuits," Electronics 114–17, Apr. 19, 1965, https://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf.

It is not just handhelds, tablets, laptops, and desktops that are connecting people and collecting data. There is an entire ecosystem of devices from in-home thermostats, to electric meters, to roadway toll readers, to fitness trackers, appliances, coffee makers, and lightbulbs. In fact, there are now twice as many connected devices as there are people.

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.[3]

The Flow of Data Is Global

And the flow of data is global so one of our principal challenges as enforcers is not just how to keep pace with this rapid technological change but also how to allow for the free flow of data while harmonizing different legal frameworks and different social norms around data sharing. It is generally recognized that the free flow of data is essential in order to realize its potential benefits.

For example, in announcing the drive for the Digital Single Market, the European Commission said that easing the flow of much of this data across borders could add 1.9% to overall European GDP and save European companies more than €400 billion a year.[4] The "full use" of big data by European governments could reduce administrative costs and create the equivalent of €150 - €300 billion in new value, according to a McKinsey study. The study estimates that this would increase annual productivity growth in Europe by half a percentage point.[5]

The Economic Impact of Our Hyperconnectivity Is Significant

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.

---

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

[4] *See* Factsheet, European Commission, "Why we need a Digital Single Market," Feb. 2016, https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/digital_single_market_factsheet_final_20150504.pdf.

[5] James Manyika et al., MCKINSEY GLOBAL INSTITUTE, BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION AND PRODUCTIVITY, May 2011, at 54, http://www.mckinsey.com/business-functions/business-technology/our-insights/big-data-the-next-frontier-for-innovation.

The important component of many of these firms is data. 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.

This data 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.

Our Hyperconnectivity Provides New Benefits and New Challenges

The Obama Administration has been at the forefront of recognizing the positive impact that data handled with appropriate privacy safeguards can have not just in the commercial sector but also in the public sector. In May of 2013, President Obama signed an executive order opening up government-collected data for researchers and developers.

The data released through the Open Data Initiative is being used to improve public health, energy efficiency, traffic flow, and even drought management. It is pioneering precision medicine for individual patients and making hospitals work better. There are apps created from the data that are helping families looking for colleges and consumers who want to avoid unhygienic restaurants.

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, new risks for consumer privacy, and potentially new impediments for innovators to enter the marketplace.

All of this presents new challenges for policy makers and enforcers. How do we maximize the benefits of new technologies and data processing while also minimizing the harms? 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?

First, and importantly, even amidst this sea of data and connectivity, consumers still matter. Every innovation is reliant on consumer trust – as several speakers today have noted. This is true in the digital world as much as in the analog one. Companies that make unsafe cars quickly find their sales drop. As consumers understand risk they turn their backs on risky products. We have started to see this in the Internet of Things space.

Consumer faith in security of their data is already low. In a recent poll, 84% of U.S. households expressed concern about privacy and security.[6] Identity theft is the most common fear of American consumers – crossing all demographics, ages, and education levels.

For instance, nearly 60% of American consumers have expressed hesitancy about buying Internet-connected devices due to security or privacy concerns. Some IoT devices have become vectors for infecting home networks; or have been rendered inoperative by software updates; or have left consumers with unease about their quality and security. This creates a cascading effect with lower sales, leading to decreased adoption, which in turn diminishes investment and ultimately, innovation.

The fact that consumer trust appears to be a growing issue one that may affect adoption suggests to me that we enforcers have an important job to do, and that it is necessary to strengthen privacy and data security laws on the one hand and remain vigilant competition enforcers on the other (more on that in a moment).

Coordination between and Cooperation among Consumer Protection Enforcers Is Critical

Getting the balance right between optimizing for innovation and protecting consumers is challenging in highly dynamic, global digital markets. It will require coordination and cooperation between regulators. Coordination is at the heart of the clearinghouse proposal reflected in the paper released last week by the European Data Protection Supervisor (EDPS). I recognize that this is largely a European initiative but I want to take a moment to applaud the idea of greater engagement among privacy enforcers.

There are some similarities between the digital clearinghouse and an existing project of the Global Privacy Enforcement Network: The GPEN Alert system. At least year's International Conference of Data Protection and Privacy Commissioners, the FTC and seven other privacy agencies from North America, Europe, and Asia-Pacific launched GPEN Alert, a secure information-sharing system for coordinating privacy investigations.

It now has ten participants, and the FTC welcomes the greater engagement from EU Data Protection Authorities. The system allows privacy authorities to share information, preserve confidentiality; and enhance privacy enforcement activities. While we will keep an eye on how the European Clearinghouse proposal develops, I hope more privacy authorities participate in GPEN Alert to improve cooperation.

---

[6] Rafi Goldberg, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, NTIA (May 13, 2016), available at https://www.ntia.doc.gov/print/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

We also need frameworks that allow data to flow across borders. The new E.U.-U.S. Privacy Shield is an example of how we can work together to ensure continued data flow. U.S. companies are quickly adopting the Privacy Shield and in the few weeks since it has "gone live" about one thousand companies are at some stage of the application process.

What Privacy Shield demonstrates is the importance of trans-Atlantic coordination among privacy enforcers. Much of the agreement is predicated on FTC enforcement of promises made by American companies to European citizens. I hope Europeans know they have a vigorous enforcement partner in the FTC.

But Is the U.S. Enforcement-Based Approach Sufficient?

As many of you know, as part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumer data in the U.S. We have brought more than 500 cases involving the collection, use and sharing of data, deceptive tracking of consumers, violations of the Do Not Call provisions of our Telemarketing Sales Rule, Childrens Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act and other deceptive and unfair data security practices.

For example, this year alone, the FTC has brought cases involving health information, router security and a case involving one of the world's largest mobile ad networks, InMobi. In this case, InMobi allegedly defeated consumers' geolocation privacy settings on their phones by collecting information regarding the Wi-Fi networks consumers' devices connected to and triangulating their geolocation from that data.[7]

I think this case is a good example of the core principles that are the basis of the FTC's privacy enforcement program - transparency, choice, and context. Consumers must have meaningful choices before sensitive information is collected, and use and collection of data should be within consumers' expectations.

The FTC's consumer protection mission doesn't simply rest on enforcement. We also study trends in technology – this Fall our tech series is focused on disclosures, ransomware, drones, and smart TVs. We challenge the research community to provide new information about how technology is impacting consumers and to provide new options for consumers we will host our second PrivacyCon showcasing new privacy and security research in January 2017. And we issue guidance to help businesses comply with the law, and reports to help shape policy and new laws we have called for comprehensive privacy legislation, data broker legislation,

[7] *See* Compl., Fed. Trade Comm'n, In the Matter of InMobi Pte Ltd. (Jun. 22, 2016), https://www.ftc.gov/system/files/documents/cases/160622inmobicmpt.pdf

improvements in student data privacy protections, and baseline data security legislation. Finally, we have expanded our in-house technology capabilities last year we established the Office of Technology, Research and Investigations so that we can understand how technology works.

I believe that understanding the technology we're talking about today is absolutely essential for enforcers, regulators, and policy makers.

Data Ethics by Design

For all of the innovation and empowerment that can be unleashed by our data revolution, I think my colleague on the FTC, 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 deceptive and unfair acts related to data security and privacy – but increasingly our hyperconnectivity, and the massive amount of data generated by it, raises new issues in antitrust and consumer protection.

To begin with, data can only positively affect people's lives if the data itself is sound. Too often, the poor, the disabled, the elderly, minorities, 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 reports of hazards and potholes in wealthy neighborhoods than in poorer areas of the city. Clearly, the data collected were 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 my country faces 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 used to determine where, and for whom, mortgage 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 still struggling to correct.

With that tragic history as a backdrop, the Leadership Conference on Civil Rights coalition 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 our equal opportunity and antidiscrimination statutes like FCRA, which have their origin in the brick and mortar world, apply in the digital one.[8]

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 machine learning, 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 too should we have Data Ethics by Design.

For companies, this will mean first, and foremost, understanding what their technology is doing. It will require transparency in the use and methods attached to data. It will mean more rigorous testing and it will mean speaking with stakeholders and communities that are typically not engaged in product development and analyzing the quality of data underlying decisions.

What Are the Implications of Our Hyperconnectivity for Competition Enforcers?

Consumer protection enforcement is only one-half of our work at the FTC. We are also increasingly called upon to understand how big data and algorithms can affect market competition. I am often asked whether "big data" can constitute a relevant market and whether "big data" can 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, a lot of data can be obtained 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

[8] 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

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 facts and circumstances of those cases.[9] But a one-size-fits-all view of data holdings is not the right approach in a world where so much data is available through multiple sources.[10]

The role of big data in determining the competitive significance or strategic value to a firm can be important, and something antitrust enforcers should consider. As such, the EDPS's work is important, as it seeks to address the intersection of competition and privacy in the context of big data. In reviewing the opinion, I see shared values – for example, the importance of dialogue about these issues. We have a mutual interest in closely following developments in this area and examining their effects on competition and data privacy, and we should expand our collaboration.

Another important topic when it comes to big data is the relationship between antitrust law and concerns related to privacy and data protection. While this is still a somewhat new issue, there are differences in the American and European approach to the relationship between

---

[9] 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. 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.

[10] 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.

antitrust, privacy, and data protection – at least with respect to certain investigations ongoing at the Member State level. For example, in the German Facebook investigation, the Bundeskartellamt (BKA) is examining whether Facebook may have exploited its alleged dominant position in the market for social networks by adopting terms of service on the use of user data in violation of data protection provisions.[11] In the United States, we would view the violation of data protection provisions on its own as a consumer protection issue.

Another difference is the European view that dominant firms have "special obligations." The potential competition law violations identified in the recently-issued EDPS opinion are primarily "exploitative abuses," which do not have an analogue under the American antitrust laws.[12] In the U.S. context, extracting more data from customers than would be possible in a competitive market could be viewed as akin to charging monopoly prices. U.S. law is clear that monopoly pricing by itself does not violate the antitrust laws.

Privacy advocates have urged the FTC to challenge mergers on the premise that the combination of personal datasets could be exploited in a way that threatened consumers' privacy. We responded in the same way DG Competition has: by underscoring that our sole objective in merger review is to prevent harm to competition. Now it is important to note, however, that harms to competition can involve non-price dimensions of competition like harms to innovation or harms to quality.

The decisions firms make about consumer privacy can give rise to non-price competition. In this context, we can consider consumer privacy in a merger investigation. Absent a clear nexus to competition, privacy and data protection concerns are considered under applicable consumer protection statutes rather than under our antitrust laws.

There are a number of advantages to the FTC's dual mandate to address both competition and consumer protection issues. Blending privacy and competition law is not one of them, and it is something we are careful to avoid at the FTC. Even if data privacy does play a meaningful role in our antitrust analysis, the focus of a merger investigation is always on the effect of the transaction on competition – and thus privacy protection as a quality dimension of non-price competition. I believe it will continue to be important that competition enforcers not use their power over a transaction to exact privacy or data protection concessions unrelated to the underlying competition analysis.

---

[11] Press Release, Bundeskartellamt, Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules, Mar. 2, 2016, http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html.

[12] European Data Protection Supervisor, EDPS Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data, Aug. 2016, at 15, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Events/16-09-23_BigData_opinion_EN.pdf.

There are good reasons for competition enforcers to focus just on elements of competition. It is not our role to limit the growth of a market based on the notion that the market is not well functioning or problematic from a public policy perspective. In a democracy, the job of making policy choices related to these tradeoffs is best left to legislatures.

Conclusion

In conclusion, I want to underscore that I believe there is a fair amount of consensus among United States and European enforcers that we can, and should, as EDPS has recommended, do better from a public policy perspective on privacy and data protection.

We share many of the same goals. Indeed, as I noted, the FTC has advocated for greater transparency and choice for consumers with respect to privacy and data protection policies, including recommending that Congress consider enacting general privacy legislation, data security and breach notification legislation, and data broker legislation. And if you look at enforcement cases such as *Google/Doubleclick* and *Facebook/Whatsapp*, for example, the FTC and our European counterparts, including the European Commission, reached similar conclusions.

On the whole, I view the relationship between the United States and Europe on these issues as a partnership. We have worked constructively in the past towards collaborative solutions to competition enforcement as well as on privacy and data protection issues and I fully expect that to continue. There will be cases where we come out differently from one another. Sometimes, this stems from different environments and cultural contexts. Sometimes the differences stem from distinctions in the laws we enforce.

One thing we can be sure of moving forward is that we will continue to face new challenges as consumer protection and competition enforcers and that we all have a part to play in protecting consumers in global digital markets. This is an exciting time for everyone involved in these fields and I am optimistic that we will continue to work together to ensure the best possible outcomes for consumers. I look forward to your questions.