Data Protection and the Internet of Things
U.S. Federal Trade Commissioner Julie Brill
Keynote Address for EuroForum European Data Protection Days
Berlin, Germany
May 4, 2015

Thank you, Bojana, for your kind introduction. It is a pleasure to be here in Berlin with colleagues from Europe, Asia, and Latin America. We are all facing the challenge of how to protect privacy as technology, business models and practices, and consumers' expectations evolve, and this forum provides an excellent opportunity for us to learn from one another. To that end, I am delighted that I will have the opportunity this morning to discuss big data's challenges – and potential benefits – with European Data Protection Supervisor Giovanni Buttarelli.

I would like to focus my talk this morning on the Internet of Things, the term that we use for the phenomenon of connecting nearly anything – from cars to clothing to light bulbs – to the Internet. The Internet of Things will add exponentially to information that we now refer to as big data, making it even bigger. In fact, the Internet of Things is already here and growing. Network equipment manufacturer Cisco reports that there are 25 billion networked devices in the world today and predicts that there will be 50 billion by 2020.[1] These sensors, along with our smartphones, tablets, and computers, generate twice as much data today as they did two years ago, and this trend is expected to continue.

The numbers and the relentless accumulation of data are only part of the story. As data becomes cheaper to collect and keep, our ability to analyze it is also improving. This development holds many promises. Cities can better maintain their infrastructures by getting early warnings about gas and water leaks, for example. Medical researchers can enroll patients in large-scale research projects in which they collect streams of data that, in the past, would have been a trickle coming from surveys and patients' own reports.[2] And the prospects for connected devices to help companies run their operations more efficiently seem nearly endless.

Policy makers in Europe and the United States recognize these promises, and strive to promote them. The European Commission stated in a July 2014 Communication that we are "witness[ing] a new industrial revolution driven by digital data, computation and automation."[3] The Digital Agenda that has been laid out so far includes a "smart living" initiative, with environmental,

---

[1] DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. These estimates include all types of connected devices, not just those aimed at the consumer market.

[2] *See, e.g.*, UCLA Fielding School of Public Health, Apple Launches 'ResearchKit' for Medical Studies (Mar. 10, 2015), *available at* http://hpm.ph.ucla.edu/news/apple-launches-researchkit-medical-studies (describing use of ResearchKit to track "disease variations and the hourly, daily or weekly ebb and flow of symptoms that are not being tracked and completely missed by biannual visits to the doctor").

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, Towards a Thriving Data-Driven Economy, at 5, July 2, 2014, *available at* https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy.

energy, transportation, and city government components.[4] And less than three weeks ago, European Commissioner Günther Oettinger sketched out an ambitious vision for Europe to develop an industrial base that integrates Internet connectivity into every aspect of its operation.[5]

In the United States, the government is also promoting the use of big data through a variety of activities, including providing data for all to use, partnering with the private sector and academia on new projects, and using big data in its own policymaking. In 2012, for example, the White House announced $200 million in research funding for industry and academia to develop new tools and techniques to organize, access, and understand big data.[6] More recently, President Obama announced the Precision Medicine Initiative, which seeks to build a database of medical information from one million or more volunteers in order to develop more personalized treatments for a range of diseases.[7] Individual states are getting into the act, too. The state of Indiana, for example, announced last year an effort to use big data to reduce the infant mortality rate in that state.[8] And cities such as New York and San Francisco are leaders in providing open data from government sources. New York City alone publishes more than 1200 data sets on a seemingly endless variety of topics, from pothole complaints to school-level test results, and makes them freely available to the public.[9]

The Federal Trade Commission (FTC), which is one of the leading competition, consumer protection and privacy regulators in the United States, sees these potential benefits, too, and wants to encourage them to flourish. Our groundbreaking report on the Internet of Things, issued in January, points to driverless cars, disease management tools, and home management systems as IoT uses that can make us healthier, happier, and safer.[10]

Of course, there are many technical and engineering problems that remain to be solved to make these benefits a reality. In addition, the Internet of Things also presents some big privacy and data security concerns. As Nicole Wong, who was one of President Obama's top technology

---

[4] *See* European Commission, Smart Living (last updated Mar. 2, 2015), *available at* http://ec.europa.eu/digital-agenda/en/smart-living.

[5] *See* Günther Oettinger, Speech at Hannover Messe: Europe's Future Is Digital (Apr. 14, 2015), *available at* http://ec.europa.eu/commission/2014-2019/oettinger/announcements/speech-hannover-messe-europes-future-digital_en (proposing "action in four key areas: digital innovation hubs; leadership in platforms for digital industry; closing the digital skills gap; and smart regulation for smart industry").

[6] Tom Kalil, Office of Science and Technology Policy, Big Data Is a Big Deal (Mar. 29, 2012), available at https://www.whitehouse.gov/blog/2012/03/29/big-data-deal.

[7] White House, Fact Sheet: President Obama's Precision Medicine Initiative (Jan. 30, 2015), available at https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative.

[8] Mohana Ravindranath, In Indiana, State Government Tries Using Big Data Project to Reduce Infant Mortality, WASH. POST (Aug. 24, 2014), *available at* http://www.washingtonpost.com/business/on-it/in-indiana-state-government-tries-using-big-data-project-to-reduce-infant-mortality/2014/08/23/66d57bc0-2973-11e4-8593-da634b334390_story.html.

[9] NYC Open Data, *available at* https://data.cityofnewyork.us/data (last visited Mar. 30, 2015).

[10] *See* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 14 (2015) (staff report), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (discussing views of workshop participants) [IOT REPORT].

advisors, recently wrote, "[t]here is no future in which less data is collected and used."[11] This comment states a fact and a challenge. The challenge lies in taking full advantage of the benefits that the Internet of Things promises while appropriately protecting consumers' privacy, and ensuring that consumers are treated fairly.

Let me be more specific about the challenge. More devices in our homes, cars, and even our clothes will mean much more sensitive data will be collected. User interfaces on devices will shrink or disappear, making it more difficult for consumers to know when data is being collected, or to exercise any control. In fact, the Internet will "disappear," as Google's chairman, Eric Schmidt predicts. That is, connectivity will just be part of how things work, as electricity is today. Data from the Internet of Things will feed new kinds of algorithmic decision-making and the burgeoning data analytics industry. And securing many inexpensive connected devices, as well as the data they generate, may present both technological and economic challenges.

Policymakers in the U.S. and Europe recognize these challenges and see similar solutions. On both sides of the Atlantic, policymakers recognize that consumer trust in IoT technologies and the companies that collect and use IoT data is critical to its success. The FTC emphasizes this point in its Internet of Things report, where we noted that a failure to provide appropriate privacy protections in the Internet of Things "may erode consumer trust."[12] The European Commission's July 2014 Communication stated that consumers must "have sufficient trust in the technology, the behaviors of providers, and the rules governing them" in order for the Internet of Things to reach its full potential. Similarly, the Article 29 Working Party noted last September that the Internet of Things "must also respect the many privacy and security challenges."[13]

How to preserve this trust is another question. Law enforcement will certainly be part of the equation. Best practices within businesses and better ways for consumers to exercise control over their information also have vital roles to play. And, because much of big data analytics depends on collecting data from many different sources and using it for purposes that may be different from those for which it was collected, we must ensure that companies are accountable for using all of this data in a way that is consistent with consumers' expectations. With so much happening outside the view of consumers, and such high degrees of sophistication needed to understand how different processing activities relate to one another, it is crucial for companies and regulators to be guided by fundamental privacy values as well as a sense of ethics – and for consumers to have strong, enforceable legal protections. For this reason, both baseline privacy legislation and data broker legislation would also play important roles in building consumer trust in the United States.

I am optimistic that policy makers in Europe and the United States will succeed in addressing these issues, not only because we share an interest in interoperable data protections and

---

[11] Nicole Wong, *Obama's Consumer Bill of Rights Should Spark National Dialogue About Privacy*, CHRISTIAN SCIENCE MONITOR PASSCODE (Mar. 4, 2015), *available at* http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0304/Opinion-Obama-s-consumer-bill-of-rights-should-spark-national-dialogue-about-privacy.

[12] IOT REPORT, *supra* note 10, at 44.

[13] Art. 29 Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 3 (Sept. 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

the free flow of data, but also because we share many of the same beliefs about why privacy matters and its important role in protecting other values.

U.S. Privacy Law: Ready for the IoT's Challenges

The starting point for that conversation in the United States is U.S. privacy law, and that's where I would like to turn next. The fabric of U.S. privacy law is strong, but it takes some effort to see how all the strands fit together. At the federal level, the U.S. has enacted privacy protections that apply to specific activities or economic sectors, such as healthcare,[14] banking,[15] credit reporting,[16] and communications.[17] Other federal laws protect children's privacy[18] and students' privacy.[19] Individual states are also active privacy regulators.[20]

In addition, the FTC has the authority under Section 5 of the FTC Act to take action against companies that engage in unfair or deceptive data practices. When Congress added this authority almost 80 years ago, in 1938, it was not thinking about data privacy or security in the digital age. Rather, Congress was concerned that harmful deception, fraud and unfair treatment can change quickly, as technology and business practices evolve. To ensure that the FTC could keep up with these changes, Congress created Section 5 to give the FTC broad, flexible authority to remedy harms to consumers in the market place.

Privacy and data security became FTC priorities in the late 1990s, when it became clear that the personal data flowing as part of electronic commerce could cause significant harm to consumers if used or disclosed inappropriately. Since then, the FTC has brought more than 40 privacy-related enforcement actions and approximately 55 data security enforcement actions under the general consumer protection authority granted by Section 5 of the FTC Act.[21] The FTC has taken action

---

[14] Health Insurance Portability and Accountability Act, Pub. L. No.104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

[15] 15 U.S.C. §§ 6801-09.

[16] 15 U.S.C. § 1681 *et seq.*

[17] 47 U.S.C. §§ 222, 338, and 631.

[18] *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-06.

[19] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

[20] Last year, approximately 60 new privacy laws were passed at the state level in the U.S. State privacy laws range from limiting employers' ability to view their employees' social network accounts, *see* Nat'l Conf. of State Legislatures, Employer Access to Social Media Usernames and Passwords, available at http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last updated Nov. 18, 2014) (noting that in 2014, at least 28 states had introduced social media and employment legislation or had such legislation pending), and prohibiting employers and insurers from using information about certain medical conditions, *see, e.g.*, Privacy Rights Clearinghouse, *California Medical Privacy Fact Sheet C5: Employment and Your Medical Privacy*, *available at* https://www.privacyrights.org/content/employment-and-your-medical-privacy (last updated July 2012), to requiring companies to notify consumers when they suffer a security breach involving personal information, *see* Nat'l Conf. of State Legislatures, Security Breach Notification Laws (Jan. 12, 2015), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification- laws.aspx (collecting references to more than 45 state laws).

[21] *See* FTC, Privacy & Security Update (2014), *available at* http://www.ftc.gov/reports/privacy-data-security-update-2014.

against some of the biggest Internet companies in the world, including Google, Facebook, Twitter, and Snapchat. We have also brought cases against companies that are not household names but violated the law by deceptively tracking consumers online, putting spyware on their computers, or violating consumers' privacy in other ways.

Today, as more and more information about our online and offline activities, health, finances, friends, and families is readily available, Section 5's prohibition against unfair or deceptive practices is a useful source of protection against inappropriate data collection, use, and disclosure with respect to the Internet of Things. This is evident not only from specific FTC cases and policy initiatives but also from companies' understanding of the *concepts* of deception and unfairness. Chief privacy officers and other privacy officials within companies think a great deal about the contours and prohibitions of Section 5, and their analysis leads companies to examine what the companies tell consumers about their data collection and use practices, and what consumers understands about these practices. This creates a consumer-oriented focus in many companies' thinking about how they handle consumers' data. It also empowers privacy professionals within companies and gives them access to top decision-makers. U.S. privacy scholars Deirdre Mulligan and Ken Bamberger made this point in their well-known paper describing "privacy on the ground"[22] in the United States. In a book that will soon be published, Mulligan and Bamberger examine the role of chief privacy officers and privacy leads in the United States, Britain, France, Spain, and Germany. These scholars will report that the experience of privacy leads in U.S. companies has some strong similarities to privacy leads in some European companies – particularly in Germany.

To see how Section 5 of the FTC Act creates a consumer-oriented focus that applies forcefully to the Internet of Things, let me first discuss deception. When a company tells consumers what personal data it collects, how it uses this data, and to whom it is disclosed, those representations must be truthful. One of many examples: if a company says it does not disclose personal data to third parties but in fact it does, then the company may be inviting a law enforcement action from the FTC.[23]

There is another side to our authority over deceptive practices. What a company *does not* tell consumers may be just as important as what it states expressly. In other words, omissions of material information can also be deceptive. In one recent well-known case, the FTC charged that the producer of a mobile app that turns the phone's camera flash bulb into a flashlight inappropriately neglected to tell consumers that the app collected precise location information, persistent identifiers, and other personal and sensitive information that consumers would not expect to flow from a flashlight app.[24]

---

[22] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

[23] *See, e.g.*, Facebook, Inc., No. C-4365 (F.T.C. July 27, 2012) ¶¶ 34-42 (complaint), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf (alleging that Facebook "provided advertisers with information about its users" in violation of representations to the contrary) ["Facebook Complaint"].

[24] *See* Goldenshores Techs., LLC, C-4466 (F.T.C. Mar. 31, 2014) ¶¶ 11-12 (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf.

The FTC's unfairness authority provides a separate basis for privacy enforcement under the FTC Act. An unfair practice is one that causes substantial injury to consumers, is not reasonably avoidable, and does not have offsetting benefits. We use unfairness in cases that meet this standard, even if a company has said nothing about the practice at issue. The FTC has used its unfairness authority to take action against companies that we believed materially changed how they use personal data they have already collected without getting consumers' permission,[25] or failed to provide reasonable data security.[26]

These two basic principles – don't deceive consumers by express representations *or* omissions, and don't harm them in ways that they cannot avoid – play an important role in addressing some of the biggest data protection challenges arising from the Internet of Things.

Addressing Specific IoT Challenges: Data Security, Sensitive Information, Fair and Ethical Data Uses

Data security is the first – and possibly foremost – challenge we face with respect to the Internet of Things. A recent study by Hewlett-Packard found that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data without encryption.[27] Moreover, traditional consumer goods manufacturers that are now entering the Internet of Things market may not have spent decades thinking about how to secure their products and services from hackers in the way that traditional technology firms have. And many connected devices will be inexpensive and essentially disposable. If a vulnerability is discovered on such a device, will manufacturers notify consumers, let alone patch the vulnerability?[28] And the security of many *devices themselves* will be just as important as security of the data they generate, as we will need to ensure that the functionality of connected cars, pacemakers and other devices are reasonably protected.[29]

The first case that the FTC brought in the Internet of Things area was against TRENDnet, which makes Internet-connected video cameras. Our complaint alleged that TRENDnet's cameras were vulnerable to having their feeds hijacked. And, indeed, around 700 private video feeds, some of which included images of children and families going about their daily activities in their homes, were hacked and publicly posted as a result of the company's security practices, which we believed

[25] *See, e.g.*, Facebook Complaint, *supra* note 23, at ¶ 29.

[26] *See, e.g.*, *See* GMR Transcription Servs., No. C-4482 (F.T.C. Aug.14, 2014) (consent order), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf.

[27] Hewlett-Packard, *Internet of Things Research Study* 2 (July 2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

[28] *See* IOT REPORT, *supra* note 10, at 13-14.

[29] *See id.* at vii. *See also* Tadayoshi Kohno, Comments at Federal Trade Commission Workshop on Internet of Things 245 (Nov. 19, 2013), available at https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

were deficient. This exposure of private activities within consumers' homes was precisely the harm that we believed made TRENDnet's conduct unfair.[30]

A second, distinct challenge stemming from the Internet of Things is the collection and use of health, location, financial, and other sensitive information. Some of the most exciting prospects for society-changing innovations come from the collection and use of such data, but the very same data poses some of the greatest privacy and security risks. In the absence of appropriate controls over user-generated health information, some companies will aggressively collect and use this sensitive data from consumers outside the context in which the consumer provided the information. Last year, FTC staff studied 12 health-related mobile apps to determine whether they were transmitting personal information to third parties, and if so, what kind of information they were transmitting and to whom. FTC staff found that these apps transmitted sensitive health conditions, such as information about "pregnancy" and "ovulation", to seventy-six third parties, including ad networks and analytics firms.[31] In many instances, third parties received this personal information linked to the consumers' real name, email address, or other unique and persistent identifiers.[32] These third parties could combine this information with other data from smart devices – including location, lifestyle, and consumption habits – to generate additional sensitive inferences.

Such surprisingly personal disclosures are at odds with consumer trust. This study of mobile health apps, as well as the TRENDnet and flashlight app cases that I just discussed, should provoke some hard thinking by companies about whether they are handling sensitive data in an appropriate manner.

A third challenge stemming from the Internet of Things is to ensure the fair and ethical use of the big data that will flow from connected devices. We at the FTC are wrestling with questions raised by the ever-improving ability of algorithms to make inferences and predictions about us. These algorithms have been around in one form or another for a long time, but their power could grow dramatically as the profiles that analytics companies generate grow richer with information from connected devices. Data brokers – firms unknown to most consumers – collect and combine tens of thousands of bits of data about each of us and weave them into profiles that contain information about where we live, where we work, and our activities and interests. But they can also contain inferences about more sensitive attributes, such our race, our health conditions, and our financial status, and lead to targeting and disparate treatment on the basis of these traits.

The FTC's data broker report found that segmentation along such sensitive lines is part of current industry practices. Our report notes that some data brokers create lists of "Metro Parents" (single parents who are "primarily high school or vocationally educated" and are handling the

---

[30] *See* TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014), ¶¶ 18-19 (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[31] *See* Jared Ho, Comments at Federal Trade Commission Consumer Generated and Controlled Health Data Seminar 26–27 (May 7, 2014), *available at* http://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf.

[32] *Id.* at 26.

"stresses of urban life on a small budget")[33] and "Financially Challenged" consumers. These profiles could be used as tools for inclusion, as well as tools to harm consumers. For example, banks might target "financially challenged" consumers with offers for safe, low-cost banking products as an alternative to high-cost options like check cashing services and payday loans, thus helping them escape their current status as unbanked or underbanked. But the very same profiles could be used to target the same consumers with high-cost loans, or even scams, thus worsening their financial situation. The Internet of Things will add depth, precision, and accuracy to these profiles, and thus companies must consider carefully how such sensitive information – whether contained in a data broker's profile or collected through the companies own information[34] – is used.

Beyond Enforcement: Legislation, Best Practices and Ethics

Law enforcement is only one part of the FTC's approach to protecting privacy and data security, and thereby strengthening consumer trust, in the Internet of Things. I'd like to draw attention to some recommendations for legislation, as well as development of best practices, that would further advance these goals. These recommendations highlight the FTC's understanding of the importance of consumers' awareness and ability to exercise choices about personal data collection and use, as well as the limitations on what policymakers and companies can reasonably expect of consumers' current ability to navigate this complex ecosystem.

Strong baseline privacy legislation would establish a common set of rules for all players – whether through the Internet of Things or otherwise – that collect or use personal data. And those rules should provide strong, bottom-line protections for consumers. Such protections, unfortunately, were missing from the Consumer Privacy Bill of Rights discussion draft that the Administration released in February, but I am eager to work with the Administration, Congress, and other stakeholders to develop a stronger, more appropriate proposal. In addition, the Internet of Things provides further evidence of the need for data broker legislation and strong data security legislation, both of which I have long supported.

While legislation is the right long-term solution, industry can and should develop best practices right now to address the most urgent consumer protection issues surrounding the Internet of Things. The first recommendation is for companies to get creative about providing transparency and control for connected devices. Some argue that it is too difficult to follow this bedrock principle with connected devices. Wearable fitness devices, for example, might not have a user interface to serve as a means to present consumers with a choice about data collection, the argument goes, and the multiple connected devices will become too numerous for consumers to manage their information. I am encouraging companies to think bigger.[35] Immersive apps and websites could

---

[33] FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 20 n.52 (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal- trade-commission-may-2014/140527databrokerreport.pdf.

[34] Michael Schrage, *Big Data's Dangerous New Era of Discrimination*, HARV. BUS. REV. (Jan. 29, 2014), *available at* https://hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination.

[35] *See* Julie Brill, *Regulators Must Guide the Internet of Things*, N.Y. TIMES ROOM FOR DEBATE (Sept. 8, 2013), *available at* http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things.

describe in simple terms the nature of the information being collected and give consumers choices about whether any of this information can be used by entities or persons who fall outside the context in which the consumer is employing the device, and in which the consumer expects her information to remain private. Another promising tool for providing consumer choice is the "command center" that companies are now developing to run multiple household connected devices.[36] The driving force here is convenience, but these command centers could also provide an opportunity for consumers to understand the information their devices are generating, and to control where that information goes.

My second recommendation concerns what goes on with data behind the scenes, way beyond the view of consumers. Whether fed by connected devices or more traditional sources – such as data from a consumer's history of dealing first-hand with a company or from a data broker's profile – big data analytics is exerting more and more influence over the ads that consumers see, what offers they receive, how they are treated by companies, and whether companies will deal with them at all. Some of these activities may very well fall within existing laws in the U.S., such as the Fair Credit Reporting Act and the Equal Credit Opportunity Act, giving consumers and regulators more authority over the practices. But the boundaries are still a bit murky, and will require further analysis and action to define. And in the meantime, some of these activities will be beyond consumers' control, even if their expectations ought to be the guiding force.

I have been urging companies to take a close look at how they use data to make decisions about consumers, and to see whether these decisions are leading them to treat consumers inappropriately on the basis of racial, ethnic, or other sensitive characteristics. This conversation should not be confined within individual companies. Computer scientists and technologists, ethicists, and advocates all have a role in shaping decision-making practices at this frontier of the Internet of Things and big data.

* * * * * *

Since it is a consumer protection agency, the FTC's privacy and data security work will remain focused on consumers – the devices and services that they use, the harms to which they are exposed in the marketplace, and their interest in trustworthy technologies and services. Our record of enforcement and policy development shows that this consumer-oriented focus is equipped to protect many of the same interests that other countries' privacy laws express in different ways. Yet it is through the Internet of Things that we may also be able to recognize some similarities that inform the ongoing global discussions about the interoperability of privacy frameworks. I look forward to continuing that discussion today.

Thank you.

[36] *See* Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL ST. J. (Jan. 5, 2015), *available at* http://www.wsj.com/articles/the-race-to-build-command-centers-for-smart-homes-1420399511.