Bitkom Privacy Conference
Keynote Address
Commissioner Julie Brill
September 24, 2015

Good morning. Thank you to Bitkom for inviting me to speak with you this morning. It is a pleasure to be among so many leaders in industry, and in the fields of privacy and data protection.

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. 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 number of connected devices and the relentless accumulation of data are only part of the story. Data is becoming cheaper to collect and keep, and our ability to analyze it is also improving. This development holds many promises. Cities can better maintain their infrastructures by developing sophisticated early warning systems for gas and water leaks. Medical researchers can enroll patients in large-scale research projects and collect streams of useful data that, in the past, would have been a mere trickle coming from surveys and patients' own reports.[1] 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."[2] The Commission's Digital Agenda thus far includes a "smart living" initiative, with environmental, energy, transportation, and city government components.[3] And last spring, 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.[4]

---

[1] *See, e.g.*, Elizabeth Whitman, *Apple ResearchKit: Is New Open-Source Software for Sales or the Greater Good of Health Care*, INTL. BUS. TIMES (Mar. 16, 2015 3:51 PM), *available at* http://www.ibtimes.com/apple-researchkit-new-open-source-software-sales-or-greater-good-health-care-1848612.

[2] 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.

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

[4] *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").

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.[5] 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.[6]

Individual states in the U.S. 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.[7] 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.[8]

My agency, the U.S. 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.[9]

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 serious privacy and data security concerns. As Nicole Wong, who was one of President Obama's top technology advisors, recently wrote, "[t]here is no future in which less data is collected and used."[10] 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.

---

[5] 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.

[6] 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.

[7] Mohana Ravindranath, In Indiana, State Government Tries Using Big Data Project to Reduce Infant Mortality, Wash, Post (Aug. 24, 2014).

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

[9] FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 1-4 (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].

[10] 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.

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.[11] That is, connectivity will just be part of how things work, as electricity is today.

And the data that will be available as a result of these connected devices will be deeply personal. Some of these devices will handle deeply sensitive information about our health, our homes, and our families. Some will be linked to our financial accounts, some to our email accounts. And all of this sensitive data will feed the burgeoning data analytics industry and new kinds of algorithmic decision-making.

Policymakers in the U.S. and Europe recognize these challenges. They recognize that consumer trust in IoT technologies and the companies that collect and use IoT data is critical to the success of the data driven economy. The FTC emphasizes this point in our 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. And the Article 29 Working Party noted last September that the Internet of Things "must also respect the many privacy and security challenges" that surround it.[13]

How to preserve this trust is another question. Appropriate enforcement of data protection and privacy laws, by my agency and data protection agencies around the globe 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. I know these issues are under discussion as the Trilogue in Brussels moves forward to finalize the General Data Protection

[11] Chris Matyszczyck, *The Internet Will Vanish, Says Google's Eric Schmidt*, CNET (Jan. 22, 2015, 6:00 PM), *available at* http://www.cnet.com/news/the-internet-will-vanish-says-googles-schmidt/.

[12] IoT REPORT, *supra* note 9, 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.

Regulation.[14] In the United States, I believe enactment of both baseline privacy legislation and data broker legislation would play important roles in building consumer trust.

But one of the biggest challenges to maintaining consumer trust will stem from the security issues presented by the Internet of Things. My agency, the Federal Trade Commission, has been engaged in data security issues for well over a decade. In terms of data security enforcement, the FTC began to use its general consumer protection authority in the early days of the commercial Internet, as it became clear that consumers suffer real harm when companies handle their personal information carelessly. Since around 2002, the FTC has brought more than 50 law enforcement actions against companies that, in our view, misrepresented how good their security was or failed to take reasonable measures to secure consumer data.[15]

The FTC is ready to use its enforcement authority to protect the personal data that will flow through the Internet of Things. In fact, we have already brought a case involving data security and the Internet of Things. The case focused on a company that makes Internet-connected video cameras. Our complaint alleged that the company'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 were deficient. This exposure of private activities within consumers' homes was precisely the harm that we believed made the company's conduct unfair.[16]

That was just one case, but there is some evidence that security vulnerabilities are rampant in 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.[17] Part of the reason may be economic. 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. For these companies, adding security expertise may be particularly costly. But many connected devices will be inexpensive and essentially disposable. If a vulnerability is discovered on such a device, will such manufacturers have the appropriate economic incentive notify consumers, let alone patch the vulnerability?[18]

---

[14] *See, e.g.*, Remarks by Commissioner Jourová After the Launch of the Data Protection Regulation Trilogue (June 24, 2015), *available at* http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm (announcing beginning of Trilogue and outlining main issues under discussion).

[15] *See* FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

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

[17] 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.

[18] *See* IOT REPORT, *supra* note 9, at 13-14.

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.[19]

The technical challenges of security in the Internet of Things are also significant. The complexity of device connections and data flows is its own challenge. We are moving irreversibly toward devices and systems that are more complex and powerful, and they will be constantly communicating with one another. This means that companies will not only have to get their devices and data systems ready to handle appropriately sensitive personal information or maintain their ability to keep us safe in the contexts in which their designers expect them to be used. Companies also have to make their devices and services robust enough to handle the unexpected events that will come from so many devices being connected and passing information back and forth. As software and connections between devices become more complex, it not only becomes more difficult for developers to avoid introducing vulnerabilities that become exploited, but it also becomes more difficult to find the vulnerabilities through testing.

A couple of examples will help to illustrate the stakes involved. Earlier this summer, two researchers demonstrated that they could take control of a car from a laptop connected to the car's data port. These researchers were able to operate the accelerator and brakes while someone else was driving. And this was a Ford Escape, not some magical self-driving car of the future. Previous research showed that it was possible to exploit a car's wireless data connection. This demonstrates the possibility that attackers may be able to take over devices from a distance, but also that they could do so on a large scale, because they wouldn't have to visit each and every targeted device in person. I understand that auto manufacturers and regulators are taking these issues seriously: they are focusing on setting privacy and security guidelines for connected cars, and regulators have recalled the vehicles that contain the systems led to vulnerabilities.[20] Ensuring the security of cars and other devices – such as medical devices – that can put consumers' physical safety at risk should be a top priority for the companies that make them, and the regulators that oversee them.

Another example shows how the connections among many different devices can lead to new and unexpected security risks. Researchers at one of the world's largest computer security conferences recently demonstrated that they could hack the network traffic of a smart refrigerator. This particular appliance was transmitting much more than information about the refrigerator's temperature and contents. It also sent credentials for consumers' email accounts, so that the refrigerator could display the owners' calendars on the fridge. According to one

---

[19] *See id.* at vii. *See also* Remarks of Tadayoshi Kohno, FTC Workshop on the Internet of Things (discussing experiment in which an attacker could gain "access to the car's internal computer network without ever physically touching the car").

[20] *See* Nora Macaluso, Connected-Car Security Has International Attention, Bloomberg BNA Privacy & Data Security Law Center (Aug. 20, 2015), *available at* http://www.bna.com/connectedcar-security-international-n17179935125/; Bernie Woodall and Joseph Menn, *Fiat Chrysler Recall Highlights Cyber Risks of Connected Cars, Telematics*, INSURANCE JOURNAL (July 27, 2015), *available at* http://www.insurancejournal.com/news/national/2015/07/27/376356.htm (noting that the U.S. National Highway Traffic Safety Administration is investigating whether the recall is sufficient to address reported cybersecurity risks).

report, the refrigerator was employing a faulty implementation of the protocol that is used to keep the passwords to such important accounts secret.[21] This apparently left the credentials vulnerable to anyone who happened to be on the same WiFi network as the fridge. It may be convenient to be reminded that you need to drop off your dry cleaning as you reach for the orange juice, but perhaps not so convenient that it is worth the exposure of important personal information that could give others access to your sensitive online accounts.

One lesson to draw from these examples, and many others like them, is that the unexpected connections among many different devices and services generate many potential benefits but also some significant risks. The other important lesson is that it will be a tremendous challenge for consumers to spot these risks and manage security on their own. This insight – that consumers' attention is a precious and limited resource – is key to many of the FTC's privacy and data security recommendations. It's the reason that the FTC recommends privacy by design, so that privacy protections are built into products and services from the beginning and persist through their lifecycle. It is also why we encourage companies to think carefully about the critical decisions consumers need to make, and providing the information they need to make them.

The FTC also promotes *security* by design. This means building security into the design of products and services, rather than trying to deal with security issues after products are launched and flaws are discovered. Indeed, the FTC is encouraging companies to go further in helping consumers, their devices, and their data stay secure. Our advice includes setting secure defaults, limiting permissions to data and device interfaces to what is necessary to carry out the device's functions, and educating consumers about the safest uses of their devices.

Finally, the FTC is calling on companies to take a long view of how their devices will be used in practice. Companies understandably focus on developing the next generation of their products and services, yet they should also recognize that many consumers will keep older versions of their devices for a long time, even when something newer and better is available. It will be important for companies to find workable ways to prevent older devices from becoming security risks.

One of the pioneers of computer science, Sir Charles Hoare, has provide this insight about the role of complexity and security: "There are two methods in software design. One is to make the program so simple, there are obviously no errors. The other is to make it so complicated, there are no obvious errors." The first of Hoare's possibilities – the world of simplicity – is not our world. The time and care that it takes to create simple software and devices that can be exhaustively tested are no longer consistent with the commercial pressures that companies face. The results for consumers can be exciting, but complexity is often a result of rapid, decentralized development. Errors hidden by complexity don't stay hidden forever. Companies owe their customers a reasonable effort to keep their devices and data secure. As an enforcement official, it's my job to help take action against companies that fail to do so. But there is a larger role for all of us – regulators, companies, researchers and other stakeholders – to

[21] *See* Cory Doctorow, *Samsung Fridges Can Leak Your Gmail Logins*, BOINGBOING (Aug. 25, 2015), http://boingboing.net/2015/08/25/samsung-fridges-can-leak-your.html.

work together to find better ways to make connected devices more secure from the beginning. I hope you will consider joining me and the FTC in this effort.

Thank you.