Opening Remarks of FTC Chairwoman Edith Ramirez
FTC PrivacyCon 2017
Washington, DC
January 12, 2017

When it comes to privacy, technology has always presented a challenge – how can we make use of the tremendous benefits of technological innovations while ensuring that our privacy is protected. This has been true from the “snap” camera of Warren and Brandeis’ time to the drones of today.

The last several decades have brought change at a breakneck pace – we saw the rise of the personal computer in the 1980s, the internet in the 1990s, the smartphone in the 2000s, and, this decade, the Internet of Things.

The dizzying array of technological advances is only going to continue to grow. Last week, I was in Las Vegas at the Consumer Electronics Show and had a chance to walk the showroom floor. There were smart cars that use new technologies to sense driver emotion and deploy sound, scent, temperature, and light in an effort to promote mental awareness and potentially reduce incidents of road rage. There were also: organic light-emitting diode (OLED) TVs as thin as cell phones that are capable of controlling the light of each individual pixel; passenger-carrying helicopter drones that can be used to transport organs for transplants; drones that can fold up and fit inside your pocket, and others that were outfitted with connected virtual reality goggles that promise a whole new experience.

From the robotic vacuum cleaner that also serves as a mobile home security camera and an air humidifier to the smart trash can that scans bar codes of disposed items in order to build a shopping list of items needing to be replaced, almost all of these technologies will rely to varying degrees on the collection of consumer information.

And data collection is growing exponentially. Experts estimate that, by the year 2020, there will be a 4,300% annual growth in the amount of data that is collected. Just around the corner are huge advances in artificial intelligence, fueled in part by IoT data. A recent White House report notes, for example, that data generated by artificial intelligence technology can enable enormous advances in health outcomes. It can improve traffic management technologies, resulting in efficiency, lower emissions, and energy savings.

But if all of this innovation is going to achieve its potential, consumers need to be assured that the risks do not outweigh the benefits. Today, I'd like to describe briefly some of the risks this new technological landscape poses, and how PrivacyCon is helping the FTC to address those challenges.

I. Privacy and Security Implications of New Technologies

Some of the risks of these new technologies are similar to ones we have encountered before. For example, traffic management technologies might only prove useful if they use data that includes a person's geolocation information. We have long-recognized that geolocation information is sensitive, and should not be collected or used without a consumer's opt-in consent. Risks of unauthorized exposure of geolocation information include stalking, revelation of political, health, and religious affiliations, and even burglary. As this example shows, the possibility of unexpected uses for information must be weighed against the benefits.

But in addition to some of these familiar challenges, there are new ones. One is the ever-growing number of actors that have a role in collecting, compiling, interpreting, and using data in a world that relies and operates on big data, IoT, and AI. There are consumer-facing companies – a device manufacturer, a smart hub platform, or a publisher website or app. There are behindthe-scenes technology companies – software vendors that connect IoT products to the internet. And, of course, the numerous analytics and advertising companies.

This vast array of entities makes it difficult to provide consumers with informed choices, and this challenge is exacerbated when non-consumer-facing entities increasingly handle consumer data. This also raises concerns about whether all of these actors are appropriately protecting the security of consumers' personal information.

Second, with new technologies, privacy and security failures aren't simply about threats to personal information. They can include threats to health and safety, particularly in relation to certain health devices and connected cars. For instance, the failure of security of IoT devices – in particular the ease with which IoT devices can be recruited into vast botnets to be used in distributed denial of service (DDOS) attacks – could pose substantial risks. To meaningfully thwart potential botnet armies, for example, a significant majority of manufacturers would have to act collectively to improve security.

Third, by relying on algorithms based on big data techniques and machine learning, companies may disadvantage certain populations. As we note in our big data report, issued earlier this year, even large data sets may be missing information about certain populations, such as those who have unequal access to technology or are less involved in the formal economy. And, big data analytics can reproduce existing patterns of discrimination or reflect the widespread biases that exist in society. For example, an algorithm that isolates attributes of good employees or good students may simply be replicating biases that existed in previous hiring or admission decisions.

The only way to keep this balancing act in equilibrium is to earn and maintain consumer trust. And this is where the FTC comes in.

II. How the FTC Uses PrivacyCon

So what *do* these emerging technological developments – and the challenges they present – mean for the FTC? It means we have to continue to be nimble and smart to keep pace. And we have to leverage our resources. At the FTC, research and data play a key role in helping to guide our work. This is precisely why PrivacyCon is so important – the research this event generates directly informs three critical areas of our privacy and security agenda.

First, we use research, both that presented at PrivacyCon as well as other research, to identify potential areas for investigation and enforcement. As an example, tech researchers brought to our attention the practices of InMobi and Turn, two companies that were the subject of recent FTC enforcement actions. In our action last year against InMobi, a mobile advertising network, we alleged that the company tracked the locations of hundreds of millions of consumers without their knowledge or consent, even when consumers set their privacy settings to deny access to their location. More recently, in our case against Turn, we alleged the digital advertising company deceived consumers by tracking them online and through their mobile applications, even after consumers took steps to opt out of such tracking. We are grateful to the outside researchers who worked hard to identify and publicize these practices.

Second, PrivacyCon provides data for our policy work and helps identify areas where additional research is needed. For instance, we used OpenWPM, a tool developed by one of last year's presenters that automates evaluation of privacy on websites, in our recently published study about cross-device tracking. In this study, OTech staff looked to assess what information about cross-device tracking is observable from the perspective of the end user, including through data flows and public disclosures. In particular, they looked at 100 popular sites on two different devices connected to the same IP address to see what information was collected that could be used for cross-device tracking.

Overall, staff detected a lot of data collection practices that could be used for cross-device correlation. It was often not clear why the parties were sharing such information – the sharing could be for cross-device tracking, or it could be for other purposes. But clearly a broad range of companies have the capacity to correlate user behavior across different devices that the users own. Staff then reviewed the privacy policies of the 100 sites, which revealed that the privacy policies were vague. In the vast majority of cases, it was unclear whether the site would share data for cross-device tracking. As a result, it would be very challenging for even a very sophisticated user to determine how much cross-device tracking is taking place. We think this type of research is incredibly helpful for informing industry, consumers, and policymakers what is happening in the marketplace, and it was a tool presented at PrivacyCon that let us do it.

Third, PrivacyCon helps us to identify and develop solutions to the privacy and security challenges we are seeing in the marketplace. For example, this past year, we have heard about the harms that can result from IoT vulnerabilities – the hacking of vehicles that could place lives at risk or of an insulin pump that raises significant safety concerns, and the malicious use of the IoT botnet, Mirai, that was used in DDoS attacks around the world. It has never been more clear that we have to secure the software and devices supporting our digital lives.

To further such efforts, last week, we announced an IoT security challenge. We will give prize money to anyone who can create a tool to help consumers quickly identify security vulnerabilities and push out updates to address those vulnerabilities. We will give bonus points to tools that can prompt consumers to change default passwords. We think this important initiative will draw attention to IoT security problems and facilitate solutions that consumers can use.

III. Conclusion

As I think about the not-too-distant future, where robotics, artificial intelligence, and more sophisticated IoT developments reign supreme, PrivacyCon will continue to help bridge the gap between the academic, tech, and policy worlds. We will continue to learn from this event to enhance our understanding of consumer expectations, to inform how practices in this dynamic economy align with those expectations, and how devices and data collected can be secured in this new landscape.

Today's forum – which will feature discussions on IoT and big data; mobile privacy; consumer privacy expectations; online behavioral advertising; and information security – will undoubtedly provide valuable insight on these and other issues, and help the FTC address emerging privacy and security challenges in a complex, dynamic marketplace.

To close, I want to thank our panelists for sharing their expertise and all of you for joining us as we seek to study these important issues. I would also like to thank the FTC staff who organized today's event, and in particular Kristin Cohen, Peder Magee, Justin Brookman, and Mark Eichorn.

Thank you.