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

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 behind-

the-scenes technology companies –

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 [illegible]