Opening Remarks of FTC Chairwoman Edith Ramirez[1]
PrivacyCon: An FTC Workshop
Washington, DC
January 14, 2016

Good morning and welcome to PrivacyCon—a first-of its-kind conference at the Federal Trade Commission bringing together leading experts to present original research on privacy and data security.

Today, companies in almost every sector are eager to scoop up the digital footprints we leave behind when we post, shop, and browse online. The new generation of products we see in the marketplace – from smart appliances to connected medical devices to semi-autonomous cars – mean that consumers must navigate an increasingly complex and dynamic digital ecosystem. In short, the interplay between technology and data is dramatically transforming how we interact with everything around us. These trends will not only continue, they will multiply.

At the FTC, we are constantly seeking to expand our understanding of emerging technologies and their impact on consumers as we work to ensure that consumers enjoy the benefits of innovation confident that their personal information is being handled responsibly. We know that our enforcement and policy work needs to be guided by research and data. We do a great deal of research and analysis internally. But, with the increasingly rapid pace of technological change and complexity of the privacy challenges consumers face, more than ever, we need to tap into the expertise and insights of the research community to help us fulfill our consumer protection mandate. Today's conference provides a unique opportunity for us to do just that.

[1] As prepared for delivery.

With PrivacyCon, our aim is to bridge the gap between the academic, tech, and policy worlds. Our ambitious agenda is filled with cutting-edge and provocative research. Some of the presentations will lend support for current privacy and data security policies. Others may lead us to rethink our assumptions. Either way, we hope to spur a richer dialogue about privacy and data security. And we hope that this dialogue will be a two-way street. As we seek valuable input from the academic and tech communities, we also aim to provide useful feedback to researchers about the type of work that would be most beneficial in helping us and other policymakers make informed policy decisions.

To set the stage for our program and highlight the importance of research at the FTC, I would like to speak briefly about the way we have incorporated privacy and data security research into our enforcement and policy work.

I. The Role of Research at the FTC

The FTC was founded on the principle that strong research informs strong policy. Today, the agency serves as a research and policy hub on a wide array of front line consumer protection and competition issues, among them privacy and data security.

We have hosted workshops and issued reports on significant and cutting-edge issues such as facial recognition, the Internet of Things, data brokers, mobile device tracking, mobile security, and mobile privacy disclosures. Our workshops have brought together academics, consumer advocates, industry, technologists, and other key stakeholders to help inform policy discussions, and our reports on emerging technologies provide concrete guidance to businesses on how to protect consumers in today's digital world.

Most recently, we held a workshop on cross device tracking. To evaluate the benefits and risks of cross-device tracking, we need to know what it is and how it works. Our workshop

included a session where experts explained how tracking techniques function and discussed whether technical measures such as identifier hashing can be used to protect consumers' privacy.

And just last week, we issued our Big Data report, which outlines a number of suggestions for businesses to help ensure that their use of big data analytics produces benefits for consumers, while avoiding outcomes that may be exclusionary or discriminatory. In the report, we highlight possible risks that could result from inaccuracies or biases about certain groups in data sets, including the risk that certain consumers, particularly low-income or under-served consumers, might be denied opportunities or that big data analytics might reinforce existing socio-economic disparities.

On the enforcement front, the work of tech researchers has helped us identify deceptive or unfair practices of companies such as HTC, Snapchat, and Fandango. Last month, we announced an action against Oracle, in which we alleged that the company's failure to disclose that older, insecure versions of Java would not be removed as part of the software update process was a deceptive practice. Various researchers had pointed out problems with malware exploits for older versions of Java software, which led to our investigation of the issue. The consent order we entered into requires Oracle to make an effective tool for uninstalling older versions of Java available to consumers. In short, our enforcement actions have provided important protections for consumers, and researchers have often played a critical role in helping us achieve that goal.

In certain areas, we have also asked technologists and researchers to help us come up with technological countermeasures to address vexing problems. Illegal robocalls is a key example. VoIP technology allows callers to "spoof" identifying information such as the calling party's phone number. Fraudsters can place millions of cheap automated calls with a click of a

mouse, and they can do so from anywhere in the world that has an Internet connection while hiding their identities in the process. These developments have reduced the effectiveness of the FTC's traditional law enforcement tools.

Recognizing the need to develop new solutions to protect American consumers from illegal robocalls, the FTC has held four public contests to spur the creation of technological solutions to the robocall problem. As part of these robocall challenges, we solicited technical experts to help select the most innovative submissions. One of the winning solutions in our first challenge, Nomorobo, is in the marketplace and available to consumers. Nomorobo reports that it has more than 363,000 subscribers and has blocked more than 60 million robocalls.

Given the importance of research and technical expertise in so much of the FTC's work, we are also continuing to build our internal capacity. Last year, we created the Office of Technology Research and Investigation, or "OTech," as we call it. OTech, which builds on the work of our former Mobile Technology Unit, identifies and conducts research that can guide the development of enforcement and policy priorities, among other important work. The office's interdisciplinary team includes lawyers and technologists who work hand-in-hand to help us study new technologies and developments in the marketplace. With OTech, we are embarking on an even broader array of investigative research on technology-related issues that will aid us in all facets of the FTC's dual consumer protection and competition mission.

II. Today's Agenda

PrivacyCon builds on all of these efforts. Our aim is to deepen our ties to the academic and tech communities and ensure that the FTC and other policymakers have the benefit of the work of leading thinkers in the privacy and data security arenas.

Our program today will feature five main topics. As to each, we will have three or four short research presentations followed by a discussion period featuring top experts.

We will start with sessions addressing the current state of online privacy and consumer expectations about privacy. There is no question that, among other things, we need to better understand consumer expectations and the degree to which consumer perceptions of companies' data practices align with what is actually happening in the marketplace.

Just this morning, the Pew Research Center released a study finding that Americans "see privacy issues in commercial settings as contingent and context-dependent." In certain circumstances, a majority of Americans are willing to share their information, if they perceive they get value in return. For instance, nearly half of those surveyed (47%) said that "the basic bargain" offered by retail loyalty cards is acceptable to them, while a third (32%) viewed it as unacceptable.

But while many consumers may be willing to share personal information in exchange for tangible benefits, the study also found that consumers "are often cautious about disclosing their information and frequently unhappy about what happens to that information once companies have collected it."

We will see what our speakers have to say about this and other topics.

Our other sessions will address big data and algorithms, the economics of privacy and data security, and security and usability. Among the issues that will be addressed will be big data and bias, the economic incentives underlying company data practices, the costs of cyberincidents, and available options for consumers to avoid unwanted tracking.

This is just to give you a flavor of what you will hear about today.

III. Conclusion

We are now just scratching the surface of what is to come by way of technological advancement, increasing uses of big data, and the implications for consumers. If we want to ensure continued progress, we must develop privacy-protective approaches that are built on innovative thinking and breakthroughs we make through research. And at the same time, we want to encourage research that will aid in addressing the complex questions that policymakers are eagerly seeking to answer. Thank you for being here today. Your presence moves us one step closer to that goal.