Opening Remarks

Understanding the Risk of Identity Theft Workshop
October 18, 2016

Katie Race Brin[1]
Chief Privacy Officer, Federal Trade Commission

Good morning! It's wonderful to see so many of my fellow federal privacy professionals here with us at the Federal Trade Commission today.

My name is Katie Race Brin. I'm the Chief Privacy Officer at the FTC, and I would like to welcome all of you to today's event, "Understanding the Risk of Identity Theft." We have a truly exceptional agenda planned for today, with experts from across the federal government here to talk about everything from understanding how to assess the risk resulting from ID theft to what to do when a breach occurs at your agency.

To open today's workshop, I'd like to take a few minutes to talk about the current state of privacy protections in the federal government, and why a fulsome discussion about identity theft is so important.

There has never been another time when privacy and the protection of information about individuals has been so at the forefront of our national discussion . Every day in the news we hear about how companies in the private sector are using (and sometimes misusing) personal information. From the internet of things, to wearable devices, to the use of big data, to discrimination by algorithm, privacy issues pervade our discussion of new and emerging technologies.

Privacy has become even more important for federal agencies as well, particularly in the wake of last year's OPM breach. There certainly have been no shortage of data breaches suffered by federal agencies, unfortunately, but the very scope, scale and sensitivity of the information involved in the OPM breach was a wake-up call for many in the federal government.

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any Commissioner.

Federal agencies collect, store, use and disseminate some of the most sensitive information about people. What happens when this information falls into the wrong hands? This is not just about financial losses or credit card fraud. As we'll discuss at today's workshop, stolen personal information can result in harms ranging from medical ID theft, unemployment benefit fraud, and tax fraud. It also can result in embarrassment, reputation harm, and in some cases, even physical danger or risk to personal safety.

When assessing the damage resulting from a loss of personal information, it is important that we consider all possible harms. For instance, as you all know, many victims in the OPM breach had their fingerprint information stolen. What does that mean down the line for the use of biometric information for authentication purposes? How can we assess what those potential harms will be?

Concurrent with heightened awareness about privacy risks, the last few years have seen significant developments in the evolution of privacy in the federal government. In February, President Obama issued an Executive Order creating the Federal Privacy Council. This was a watershed moment for federal privacy. The creation of the Council shows a recognition by the White House that protecting the collection and handling of personal information is fundamental to the government accomplishing its mission. As the President stated in the Executive Order, "Privacy has been at the heart of our democracy from its inception, and we need it now more than ever."

In addition, we've seen a bevy of new guidance from OMB, including the groundbreaking updates to Circular A-130, which focus on sound privacy practices as more than just checking a set of compliance boxes, but building in privacy controls from the ground up and ensuring that those controls are operating as intended. We also look forward to the forthcoming updates to OMB Memo 07-16, which outlines for federal agencies how to assess harm resulting from a breach and the steps agencies must take to mitigate that harm. The second half of today's workshop will be spent generally discussing this upcoming guidance and the ways in which agencies should deal with breaches.

As we continue to move the privacy ball forward in the federal government, harms resulting from ID theft play a key part in justifying why privacy is important. Why should agencies spend valuable funds on supporting a robust privacy program instead of on mission-related activities?

Because if government agencies can't be trusted to protect individuals' information, they won't be trusted for much else. This erosion of confidence in federal agencies is something we must combat – in order for government to function for the people, it must be trusted by the people. It is imperative that individuals have faith in federal agencies for government to be effective, and a mistrust of how personal information is used or safeguarded makes that difficult to achieve.

That's one reason why events like today's are so important. We strive for consistent approaches to protecting personal information across the entire federal government. One small piece of that very large pie is understanding the harms that can result when the information we are trusted with falls into the wrong hands.

I'd now like to turn it over to John Krebs, from the FTC's Division of Privacy and Identity Protection. John is an expert on ID theft and is the main architects of today's event. He will discuss in more detail the goals of the workshop and the themes we hope to explore today.

Thank you so much for joining us and for your participation today. We look forward to an interesting discussion. Thanks very much.