Commissioner Julie Brill
Promoting Innovation Through Consumer Protections and Competition Enforcement
Remarks at the Computer & Communications Industry Association (CCIA)
Washington Caucus
Washington, DC
April 9, 2014

Thank you, Ed, for that kind introduction. And thank you to CCIA for inviting me to address the Caucus. It is a pleasure to be able to be able to discuss with you three issues that are central to continuing innovation in the information economy: consumer privacy, data security, and patents.

Protecting consumer privacy is one of the FTC's top priorities. Before I go into some detail about how we protect consumer privacy, I'd like to spend a moment explaining why privacy is an important area of our focus.

The amount of data that companies collect, retain, use, combine, and disclose has grown exponentially over the past few decades. Data about each of us – and our activities – our personal information – is an increasingly important part of the U.S. economy. The flow of personal information goes hand-in-hand with many of the innovations that allow us to connect with friends, find our way around cities that we've never visited before, and collaborate with colleagues around the world.

personal information.[2] But in many cases, consumers do not really know what these non-consumer facing companies do with their data, what choices consumers may have about this data use, and what protections are in place for consumers' privacy interests.

In our policy work, the FTC has developed best practices and recommendations regarding how companies can be transparent about their practices and help consumers make meaningful choices about the use of their personal information. Working toward these goals helps to ensure that consumers have confidence in the dynamic and changing marketplace for personal information.[3] In addition, we hope to issue our report about the collection and use practices of nine data brokers – companies that collect online and offline information and create rich profiles about consumers – to help provide a deeper understanding about the practices of some of these companies.

In our enforcement work, we pay particularly close attention to children's online privacy, as mandated by Congress in the Children's Online Privacy Protection Act.[4] We also enforce the Fair Credit Reporting Act.[5] Enacted in 1970, the FCRA has proven to be a durable source of consumer protections where traditional credit reports are concerned. Moreover, FCRA protections apply to uses of information, rather than specific technologies. As a result, the FCRA is a valuable source of consumer protections as consumer reporting activities draw information from more diverse sources[6] and become available through mobile devices.[7]

The bulk of our enforcement cases – brought over the past decade, under both Republican and Democratic leadership – have challenged deceptive and unfair data security and privacy practices under Section 5 of the FTC Act. In that time period, we have brought more than 50 cases against companies that we believe failed to reasonably secure consumers' information, and more than 40 cases relating to the privacy of consumer data. Some of these cases involve household names, [illegible]

against less well-known companies, alleging that they spammed consumers,[9] violated commitments in their privacy policies,[10] installed spyware on consumers' computers,[11] or otherwise crossed the lines of deception or unfairness in their data collection and use practices.

With respect to data security, the FTC uses its Section 5 unfairness and deception authority to ensure that companies provide reasonable security for personal information. We are all too familiar with the potential for harm from financial information falling into the wrong hands. The FTC has alleged in numerous actions that companies violated Section 5 by failing to reasonably protect consumers' financial information.[12] We received a vivid reminder about the importance of data security during the height of the holiday shopping season, when Target acknowledged that 40 million consumers' credit card and debit card information, as well as contact information about some 70 million consumers, had been stolen.[13] The movement toward innovative other forms of payment from mobile devices may create new challenges to securing financial information, and the FTC is watching these developments closely.[14]

From my perspective, there is no data privacy without data security. Inadequate data security can expose information that consumers never meant to put on public display.[15] Security lapses can leave our children exposed in alarming ways.[16] And inadequate security in one link can weaken the security in the whole chain of software and hardware in our devices and apps[17]

to protect consumer information through reasonable policies and procedures that span the entire product lifecycle, rather than waiting until after a breach. As more and more devices become networked, with a greater volume and variety of personal information flows, the costs of security failures only stand to increase. I support legislation that would require companies to adopt and implement reasonable data security practices. I believe it would be very useful for this Working Group to consider proposals that would lead to adoption of data security legislation.

Let me turn very briefly to some emerging privacy issues that the FTC is currently addressing. In November, we held a workshop on the Internet of Things, to explore data security and privacy issues related to connected devices.[18] Both Commissioner Ohlhausen and I attended the Consumer Electronic Show in January, where we saw first-hand the incredible growth in the connected devices sector, including smart cars, smart clothing and wearable accessories, smart appliances, and more. I expect that in the coming months we will issue a report on some of the privacy and security issues that arise with respect to connected devices. In the past two months, the FTC held seminars on two cutting-edge issues:

- mobile device tracking in retail and other business, and
- alternative scoring products that use predictive scoring to determine consumers' access to products and offers.

And on May 9, we will hold a third seminar on consumer-generated health information provided to entities that are not covered by HIPAA, including health information from wearable devices.[19]

Finally, let me shift gears and spend a few minutes discussing the need for patent reform. Focusing on these issues – the intersection of patents, antitrust, and innovation – is built into the FTC's DNA. The person most directly responsible for conceiving of the FTC – Louis Brandeis – was deeply concerned about the role of technology in society. So it is only fitting that various aspects of the patTd arable

Over the past decade, the FTC has closely examined the intersection of patent and antitrust laws. Our extensive work has included numerous workshops and hearings, with input from a wide spectrum of stakeholders – business representatives from large and small firms, the independent inventor community, leading patent and antitrust organizations and practitioners, consumer groups, and scholars. The resulting reports and guidelines, spanning across various administrations, have represented the views of Commissioners of all political stripes.

We hope the eventual report that we issue based on our 6(b) study will provide a fuller and more accurate picture of PAE activity, which we can then share with Congress, other government agencies, academics, and industry. We anticipate that, as in the past, our study, once it is done, will be put to good use by Congress and others who examine closely the activities of PAEs.[31] Notably, 42 State Attorneys General and the Department of Justice Antitrust Division have expressed strong support for our study.