Remarks of FCC Commissioner Mignon L. Clyburn
9th Annual FCBA/ABA
Privacy and Data Security Symposium
Washington, DC
March 13, 2014

Good afternoon everyone. I appreciate the opportunity to speak with you today about two of the most pressing and talked about issues of our time—privacy and data security.

For those of you still getting to know me, allow me a few moments to share my philosophy and perspectives on regulation. I am a public servant dedicated to working in the public interest. Before coming to Washington, I served as member of the Public Service Commission in my home state of South Carolina, where I represented both rural and urban constituents as a state regulator of investor owned utilities. At the Federal Communications Commission, I continue to see myself as a champion of the voiceless — those without well-connected lawyers or lobbyists in Washington, who also deserve to be heard. I strive to be a "facilitator of opportunities," and a "connector of the disconnected."

I am also a strong advocate for free enterprise, competition and for allowing those markets the chance to solve problems. Markets should be left alone when they are working well, but I affirm repeatedly that I am not afraid to step in to regulate when the market does not work to promote fair and equitable results.

As an unabashed proponent of diversity, I strive to ensure a level playing field and for the game to be open to every player who wants to step onto the field. I am especially concerned about those disconnects in society — not just when it comes to technology, but in many other life applications where technology can play an important role, such as health care, entrepreneurship, finance, and education.

My work at the FCC has been guided by the four principles of the Communications Act — (1) competition; (2) protecting consumers; (3) universal service; and (4) public safety. So let's speak a bit more about that second pillar—consumer protection, particularly when it comes to privacy.

Privacy is a vexing issue that is neither simple, nor easy. How many of you caught this week's edition of "60 Minutes"? Their lead-in story was titled: "The Data Brokers: Selling Your Information." The story then went on to describe how "thousands of companies you've probably never heard of," called data brokers, have been collecting, analyzing and packaging information, about consumers' activity. They are selling it to each other, advertisers, and more, often without our direct knowledge. Much of this is the kind of harmless consumer marketing that's been going on for decades. What's changed is the volume and nature of the data being mined from the Internet and our mobile devices, and the growth of a now multi-billion dollar industry.

The data broker industry generates over $150 billion in revenues annually. That is twice as large as the entire intelligence budget of the U.S. government. The activities of this industry are subject to little or no oversight or regulation. And most troubling to me is that, according to a report by the Senate Commerce

Committee, data brokers use this data and information to group consumers like you and me into categories according to their incomes and economic capabilities. They sometimes single out the vulnerable groups for marketing purposes by targeting those vulnerabilities and assigning rather offensive names to those groups such as:

- "Rural and Barely Making It"
- "Tough Start: Young Single Parents"
- "Rough Retirement: Small Town and Rural Seniors" and
- "Zero Mobility"

Our digital lives leave us more open and vulnerable, especially online. Our personal information is being collected, analyzed, harvested and sold. Our financial decisions, health and lifestyle choices, and other very personal information is collected aggregated, used, and leveraged by those in search of financial gain.

As for the role of government, we find ourselves clearly at an important stage of the regulatory and enforcement continuum. What is the recourse if our most personal information and habits are exploited without our knowledge or consent? What do we do, when there is a widespread breach that compromises the data collected by companies, retailers, universities, hospitals or financial institutions?

There is obviously a role for government to play and there are two key issues involved in government oversight or regulation of privacy.

- The first is how to protect consumers from abusive and over-reaching data gatherers; and
- The second is how to make sure that companies are protecting the data they lawfully gather.

As we speak, there are over one dozen bills relating to privacy making their way through Congress. I do not know how many, if any, will be enacted, but they cover the waterfront of concerns in the marketplace.

For example:

- The Personal Data Privacy and Security Act would expand civil and criminal penalties for data breaches and abuse of personal information;

- The Do Not Track Online Act would establish a simple "Do Not Track" mechanism for consumers;

- Drone Aircraft Privacy and Transparency Act would limit the use of drones in U.S. airspace;

- The Cyber Intelligence Sharing and Protection Act allows the federal government to conduct cyber security activities to respond to cyber incidents;

- The Mobile Device Tracking Act requires a retailer using mobile tracking technology, to display a notice that the technology is in use.

There are others, but I think you get the point.

When it comes to the protection of consumer privacy, it is fair to say that our sister agency, the Federal Trade Commission, has taken the lead. The FTC has an entire set of privacy initiatives ranging from online privacy protection to identity theft protection and protection of children online.

That agency has recommended a "Do Not Track" option for websites and has kept a vigilant watch over industry self-regulation. At the FCC, our approach to privacy and cyber security is to ensure that we promote both of those important policy goals, while also promoting innovation. In other words, we see this as a virtuous cycle.

In the area of mobile wireless services, we believe that the reason more American consumers are choosing to cut the cord and rely only on these services for their telephone needs, is because they feel their privacy is being protected. The greater demand for these services is encouraging investment and innovation in mobile network deployment, more services in each new edition of smart phones, and cooler mobile apps.

When an issue regarding consumer protection comes to our attention, we try to take an approach that promotes privacy and public safety, without stifling innovation. For example, last summer when I was Acting Chair during the first Open FCC meeting under my watch, we voted to adopt a Declaratory Ruling to protect consumer proprietary network information – or in acronym parlance – CPNI, on mobile devices. CPNI includes the phone numbers dialed and the location from which those numbers are dialed.

For decades, the Communications Act has given the Commission authority to protect that information. A question arose whether wireless providers were responsible for protecting that information when wireless handset makers design phones to capture that information. The declaratory ruling clarified that a carrier has "received or obtained" CPNI when the carrier causes that information to be stored on the device and it or its designee has access to or control over that information.

But to promote innovation, the declaratory ruling also made clear that it did not prohibit carriers from collecting information needed to improve networks. We also did not require carriers to implement any particular type of protection. Instead, we allow them to choose their own method of safeguarding CPNI as long as it provides appropriate protection against unauthorized access.

We took a similar approach a couple of months ago when we adopted a Notice of Proposed Rulemaking to improve location accuracy standards when people use their mobile devices to dial 9-1-1. The Commission's current E-9-1-1 rules were primarily designed to deal with outdoor locations, and this clearly needs to be reevaluated in light of the fact that wireless calls are increasingly placed from indoors.

In November 2013, we held a workshop to examine these issues further. We heard how call centers in certain areas of the country were not receiving the information they needed to dispatch help to those in need because mobile calls pose more challenges to first responders than wireline calls.

Citizens understandably expect and believe that their mobile handsets – especially those smartphones with location based services – provide them with the same capacity to get help as their wireline phones. But all too often, this is not the case and the results can be heartbreaking.

So I was pleased to see that Chairman Wheeler circulated an NPRM to address these issues only three months after that workshop. For the first time, the Commission proposed rules requiring that wireless providers to meet location accuracy standards for wireless 9-1-1 calls, from indoors.

The Commission also, for the first time, proposed testing methods to ensure that the carriers are meeting these proposed rules. But, again, so as not to stifle innovation, we encouraged carriers to propose other testing methods that may better suit their particular business plans or practices.

Here are a couple of questions that you might be thinking about concerning the FCC's approach.

Q: What are the FCC's plans regarding cyber security?

- The FCC has always focused on the security and resiliency of networks.

- As you all know, public safety and national security pertaining to communications is written into Title I of our governing statute.

- As more of our communications – including crucial public services, such as 911 and the Emergency Alert System – move to a heavier reliance on IP-based networks, the question for us now is how do we fulfill our responsibilities to the public to ensure the security and resiliency of today's networks?

- Chairman Wheeler has made it clear, that he wants the FCC, to play the role that our society needs it to play, and I am encouraged by our developing cyber security posture.

- Our approach will build on the mutually reinforcing principles of security, privacy, and innovation – understanding that if we focus exclusively on one of these principles, the others will suffer.

- But if we aim to achieve all three, we can create a virtuous cycle in which security, privacy and innovation, all build on one another.

Q: Is the FCC gearing up for a heavier emphasis on cyber security?

- As you know, Chairman Wheeler brought in Admiral Dave Simpson to lead the Public Safety and Homeland Security Bureau and to ensure that we are doing what is necessary to protect the security and resiliency of our networks – including, against cyber security threats.

- Admiral Simpson brings to the FCC tremendous experience and leadership on these issues – both in cyber security and with regard to communications more broadly. Among other responsibilities such as serving on the U.S. delegation to the World Conference on International Telecommunications with Ambassador Verveer, and running the communications infrastructure in Iraq, Admiral Simpson was most recently the Vice Director of the Defense Information Systems Agency.

- There is also a new position on Admiral Simpson's team – the chief counsel for cyber security—which has been filled by Clete Johnson, Senator Rockefeller's former counsel on intelligence and cyber security.

- In recent weeks, the Bureau has posted new jobs for cyber security engineers in the Cyber Security and Communications Reliability Division, and there may be additional opportunities forthcoming. And, Admiral Simpson has started a cyber-security internship program for engineers and lawyers that will start this summer.

Q: How should members of the FCBA approach these issues?

- Try to move beyond entrenched ways of thinking, about these challenges, and instead, present new solutions, that these revolutionary changes require. Be creative and innovative in your legal thinking and in your advice to clients.

- The internet economy and 21st Century communications are inherently based on innovation. Therefore, the lawyers who work in this sector need to be as in sync with all of the technological innovation through creative, innovative approaches to the law.

Thus, as you can see ladies and gentlemen, privacy is a multifaceted issue that will be with us always. I look forward to lending and receiving all the help I can as we address these critical issues in the future.

Thank you.