Remarks of Matthew S. DelNero

Chief, Wireline Competition Bureau, FCC

FCBA / ABA 11th Annual Privacy and Data Security Symposium

March 3, 2016

Thank you to the FCBA's Privacy and Data Security Committee and the ABA Forum on Communications Law for inviting me to speak with you all today.

The symposium that the ABA and FCBA jointly present each year has become an important forum for discussion on developments in privacy and data security – cutting across policy, legal, technological, and business dimensions. And the fact that this is the *eleventh* annual forum that you've presented on privacy and data security speaks to the fact that these issues are not new to the communications sector.

Indeed, Congress first enacted a privacy law for a segment of the industry – cable providers – in 1984, and that was at a time when less than half of the country was reached by cable. But I'm here today to talk about another part of the Communications Act, Section 222, and in particular staff's work towards developing a notice of proposed rulemaking (NPRM) that, if adopted, would set forth proposals and seek comment on rules to protect the privacy interests of broadband subscribers. With broadband as the defining infrastructure of the 21st Century, it is no surprise that we are discussing the privacy and data security of information that American consumers send over those networks every day.

Before we go further, it's worth taking a step back and looking at Section 222 in the broader context of U.S. privacy law and policy. Before I joined the FCC, among other things I advised online providers and other parties on privacy developments abroad, which, as in the U.S., have been significant – particularly in emerging markets experiencing rapid growth in Internet usage. When speaking with regulators abroad, I often would be asked "why doesn't the U.S. have a privacy law?" The answer of course, is that the U.S. has multiple privacy laws, both at the federal and state level. Which these laws have different functions, individually and collectively they serve to protect consumers. I think FTC Commissioner Brill explained the U.S. approach best when she referred to the multiple strands at the federal and state level that form the "strong fabric" of U.S. privacy law.

First, under its Section 5 authority, the FTC has an important enforcement mandate to address unfair or deceptive acts or practices – a general consumer protection mandate that dates back to the 1930s but which the FTC has successfully used in the 21st Century to take action against companies that don't keep their privacy promises to consumers or that mislead them by not maintaining security for sensitive information. These decisions have set important precedents for the Internet ecosystem and beyond. Second, nearly every state has adopted some form of privacy or data breach law, covering a range of subjects. Third, Congress has enacted sector-specific privacy protections – including with respect to financial institutions, schools and other educational institutions, healthcare providers, and credit reporting agencies.

And communications networks. It is within that construct of sector-specific privacy regulation that we find Section 222 of the Communications Act, captioned "Privacy of Customer Information." In enacting that provision as part of the Telecommunications Act of 1996, Congress found that information collected by communications networks requires particular protections and expert agency oversight. So just as the Department of Health and Human Services regulates the privacy practices of "covered entities" under HIPAA – such as doctors, hospitals, and health insurance plans – the FCC has applied section 222 to protect data that carriers collect by virtue of providing telecommunications services to their customers.

More specifically, the FCC has adopted, and over time amended, implementing rules for section 222. Those rules are focused on ensuring that consumers have the tools they need to make informed choices about customer proprietary network information (CPNI) – in layman's terms, information a provider has about you by virtue of the customer-provider relationship. The existing rules, which apply primarily to voice services, provide consumers decision-making authority over how such information is used and shared, and they seek to protect the confidentiality of CPNI through data security and data breach notification requirements. As you heard earlier today from my colleague, Travis LeBlanc, the FCC's Enforcement Bureau has substantial expertise in these rules and has actively enforced them.

As most of you know, when the FCC reclassified broadband Internet access service as a telecommunications service in the *2015 Open Internet Order*, it forbore from applying many of the Title II requirements to broadband services. But the FCC found that applying and enforcing section 222 for broadband is in the public interest and necessary for the protection of consumers. At the same time, the FCC found that the current section 222 rules are not necessarily well-suited to broadband, and forbore from them – instead suggesting that it would likely move forward with a privacy rulemaking to consider new, modern rules to protect the privacy interests of broadband subscribers.

Since then, staff of the Wireline Competition Bureau has been working closely with experts across the agency to craft a proposal for broadband subscriber privacy that we can recommend to the full Commission. And let me be very clear. Consistent with the Act, what we are focused on are the privacy practices of broadband providers regarding the data they obtain by virtue of providing broadband service. The privacy laws and best practices that govern the rest of the Internet ecosystem are helpful in informing our thinking. But section 222 applies to telecommunications services; that is section 222's "strand" of U.S. privacy law. It does not apply to other activities, including the activities of edge providers.

Last April we kicked off our exploration of broadband providers' privacy practices with a workshop sponsored by the Wireline Bureau and the Consumer and Governmental Affairs Bureau. Since then we have spoken with a wide variety of stakeholders, including industry associations and individual broadband providers, public interest organizations, academic experts, and other state and federal agencies. On that front, I'd like to especially thank Jessica Rich, from whom you heard earlier today, and her staff at the FTC's Bureau of Consumer Protection. Also, a number of parties – including industry representatives and public interest organizations – have released letters or papers with thoughtful ideas for the Commission's consideration, and there is no shortage of good ideas.

There is, in fact, lots of agreement. Everyone we've spoken with seems to agree that the privacy protections for customers of broadband services should include certain basic principles. We at the staff level are keeping these principles front and center as we develop proposals and areas of possible comment for the Commission's consideration.

First is transparency – the notion that customers of broadband access services should receive clear, conspicuous, and understandable information about providers' privacy practices. This bedrock principle animates existing communications laws and regulations like the voice CPNI rules, notice provisions of the Cable Privacy Act, and the open Internet transparency rule, among others. You also see it reflected in best practices regimes like those articulated by the FTC, the Digital Advertising Alliance, Network Advertising Initiative, and the Administration through the work of the NTIA.

Second is choice, recognizing that at the core of section 222(c) is a requirement that customers generally should have the opportunity to "approve" the use, disclosure of, and access to individually identifiable CPNI for purposes other than the provision of the telecommunications service. Here, the goal is to ensure that consumers have the tools they need to make choices about the use and sharing of that information, with a recognition that what those tools should be are dependent in part on context.

Third is data security. In focusing on this principle, we recognize that privacy and security are inexorably linked. Broadband subscribers expect that their broadband providers will protect their data with reasonable measures to safeguard customer information from unauthorized use, disclosure, or access. And when that information is breached, customers have a right to know.

These principles have their origin in the Fair Information Practices Principles. They are reflected in our current section 222 rules, our enforcement work, FTC caselaw and guidance, and in many statutes and in pending legislation, to mention just a few of the myriad places where these principles exist. We also see them in many broadband providers' existing practices and policies, and we are well aware of the value of maintaining flexibility to achieve privacy goals in innovative ways to the benefit of consumers.

Of course, there are many paths to choose from in deciding how best to apply these principles in practice. That is the role of a rulemaking, which allows for robust public debate and discussion. With that in mind, one of our goals at the staff level is to present the Commission, for its consideration, with an item that sets a pathway to final rules – seeking comments and encouraging parties to propose their own ways of achieving an effective privacy framework for broadband providers.

Thank you again for inviting me to speak with you today. I look forward to working with all of you as we continue to think about customer privacy on the nation's communications networks.