Statement of Clete D. Johnson
Chief Counsel for Cybersecurity
Federal Communications Commission

Before the Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives

Hearing on
"Discussion Draft of H.R. __, Data Security and Breach Notification Act of 2015"

March 18, 2015

Chairman Burgess, Ranking Member Schakowsky, distinguished Members, thank you for providing the opportunity to discuss the FCC's current programs and authorities with respect to consumer protections concerning data privacy, security, and breach notification requirements for communications data.

Congress has recognized for decades that information related to consumers' use of communications services is especially sensitive, for reasons that go beyond potential economic harm such as financial fraud or identity theft. If Americans cannot communicate privately, if we are not secure in the privacy of information *about* our communications, then we cannot fully exercise the freedoms and rights of an open and democratic society. As with medical and health care data governed under the Health Insurance Portability and Accountability Act and financial data governed under the Gramm-Leach-Bliley Act and other statutes, Congress has long treated communications-related consumer information as a special category of consumer data that calls for expert oversight, tailored protections and effective enforcement.

The privacy and security of sensitive personal information held by communications networks is a bigger issue than ever given recent developments, such as public concerns about the availability of telephone call records, the widespread use of fixed and mobile broadband communications, the privacy implications of important improvements to Next Generation 9-1-1, and recent cyber attacks, such as the one aimed at suppressing the release and viewing of a motion picture. As the expert agency that regulates communications networks, we continually seek to improve these protections for the good of consumers.

I would like to begin by discussing with specificity the legal framework currently in place to protect consumers and the responsibilities of communications providers to secure their networks in the first instance, and take remedial actions where data breaches occur. The draft bill would alter this legal framework and leave gaps as compared to existing consumer protections.

The Communications Act, through sections 222, 338(i), and 631 among others, establishes important consumer protections with respect to data security and breach notification. Specifically:

- Section 222 of the Act establishes a duty for telecommunications carriers and interconnected VoIP providers to protect the confidentiality of customers' proprietary information, including, but not limited to, call records, location information, and other information related to the service, such as the features of the customer's service, or even the customer's financial status. FCC rules promulgated under section 222 require carriers to notify law enforcement and consumers of breaches. Carriers that fail to meet the requirements of section 222 and its implementing rules are subject to an enforcement action brought by the FCC. Many of these consumer protections, including the protection of several particular types of proprietary information, would no longer exist if the draft bill were enacted.

- Sections 631 and 338(i), which apply to cable and satellite television providers, protect customers' viewing history – that is, the television shows that they watch and the movies that they order — as well as any other personally identifiable information available to the service provider. Consumers' privacy on these matters is also protected by FCC enforcement authority.

The FCC actively enforces the data privacy and security provisions of the Communications Act and related rules.[1] If enacted, Section 6(c) of the draft bill would declare sections of the Communications Act, as they pertain to data security and breach notification, to "have no force or effect" except with regard to 9-1-1 calls. The Federal Trade Commission would be granted some, but not all, elements of the consumer protection authority that the FCC presently exercises. For example, if the draft bill were to become law, the FTC would not have the authority to develop rules to protect the security of consumers' data or update requirements as new security threats emerge and technology evolves.

Finally, while the draft bill attempts to maintain the protections of the Communications Act for purposes other than data security, the FCC's experience implementing privacy and security requirements for consumer data reveals that there is no simple distinction between the two interrelated concepts. In short, whether a company (either by human error or technical glitch) mistakenly fails to secure customer data or deliberately divulges or uses information in ways that violate a customer's privacy rights regarding that data, the transgression is at once a privacy violation and a security breach.

I thank you again for the opportunity to provide a summary of the FCC's programs with respect to data privacy and security and I look forward to answering any questions you

[1] *See, e.g.*, Sprint Corp., *Consent Decree*, 29 FCC Rcd 4759 (2014) (involving alleged violations of do-not-call rules); Verizon, *Consent Decree*, 29 FCC Rcd 10303 (2014) (involving alleged violations of CPNI rules).

may have. The FCC stands ready, willing, and able to provide this Subcommittee any assistance it may request in its important work to protect consumers in the 21st century.