Statement of Austin C. Schlick
General Counsel
Federal Communications Commission

Before the Committee on Commerce, Science, & Transportation
United States Senate

"Privacy and Data Security:
Protecting Consumers in the Modern World"

June 29, 2011

Good morning Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee. Thank you for this opportunity to discuss the Federal Communications Commission's programs to protect consumer privacy. I am particularly pleased to be here with representatives of two strong partners in this effort, the Department of Commerce and the Federal Trade Commission.

The FCC has decades of experience implementing privacy protection statutes. These include provisions of the Communications Act that require communications providers to safeguard their customers' personally identifiable information, as well as provisions that protect consumers against unwanted telephone and fax solicitations.

At the same time, increased use of personal data in connection with new online and wireless applications is raising serious privacy and security concerns. As the FCC recognized in the National Broadband Plan, successfully addressing these concerns will be critical to increasing adoption and deployment of technologies that benefit consumers, government, and the economy.

The Commission historically has focused on three privacy-related goals: ensuring that personal information is protected from misuse and mishandling; requiring providers to be transparent about their practices; and enabling consumers to make informed decisions. These goals remain our primary focus as we implement the various sections of the Communications Act that directly impact privacy.

For example, Section 222 of the Communications Act requires telecommunications carriers and interconnected Voice over Internet Protocol providers to secure customer proprietary network information, which is known as CPNI. CPNI includes consumers' call records and call-location information.

Under Section 222, the FCC has adopted rules addressing the handling, use, and sharing of CPNI. We also have adopted rules to prevent pretexting, a practice by which unauthorized third parties attempt to gain access to telephone subscribers' personal information. Through our rulemakings and enforcement, we have resolved difficult issues such as when opt-in and opt-out notifications are appropriate, minimum notice standards, data sharing rules, reasonable data security measures, and notification to law enforcement and consumers in the event of data breaches.

In just the last six months, the Commission issued 28 warnings and Notices of Apparent Liability for various CPNI violations. Because of our active enforcement and education efforts, the Section 222 protections are now well-known and well-understood, and the number of consumer complaints the FCC receives on CPNI issues has declined steadily.

Sections 338 and 631 of the Communications Act also protect personal information. These provisions establish requirements for satellite and cable television providers' treatment of their subscribers' personally identifiable information. The requirements include clear and conspicuous notice about collection and use of subscribers' personal data, limiting disclosure of personal data, and remedies for subscribers who suffer a violation of these provisions.

Working in parallel with the FTC, the FCC adopted "Do-Not-Call" regulations under Section 227 of the Communications Act. Since 2009, we have issued nearly 150 warning citations for Do-Not-Call violations. The FCC and the FTC also collaborate on implementation of the CAN-SPAM Act, with the FCC adopting rules that prohibit sending unwanted commercial e-mail messages to wireless accounts without prior permission.

The FCC and the Department of Justice enforce Section 705 of the Communications Act, which prohibits unauthorized interception of radio communications and unauthorized disclosures of wire or radio communications.

The FCC supports consumer education in the areas of privacy and information security. The FCC is a partner in *OnGuard Online*, an online initiative led by the FTC that helps consumers guard against Internet fraud and identity theft, protect their children's personal information, and avoid e-mail and phishing scams. The FCC also is a member of the National Initiative for Cybersecurity Education partnership led by the Department of Commerce.

Just yesterday, we held a workshop at the Commission on location-based wireless services and the privacy issues they raise. At this webcast event in which the FTC participated, we gathered information from wireless carriers, application developers, and business and academic leaders about trends in the development and use of location-based services, industry best practices for protecting personal information, and what consumers and parents should know about protecting themselves while using these services. We heard about the many potential benefits of location-based technologies, as well as the challenges of educating consumers to protect their privacy while using these new products and services.

The FCC brings to these issues accumulated privacy expertise, as well as expertise about new communications technologies and services. Protecting privacy is a necessary part of providing communications services. So too, it is part of the FCC's mandate to promote a healthy and competitive communications marketplace that meets consumers' needs.

Thank you for the opportunity to testify today, and I look forward to your questions.