

**Statement of Chairman Julius Genachowski
Federal Communications Commission**

Hearing on “Internet Privacy: The Views of the FTC, the FCC and NTIA”

**Before the Subcommittee on Commerce, Manufacturing, and Trade and the
Subcommittee on Communications and Technology**

U.S. House of Representatives

July 14, 2011

Chairman Bono-Mack, Chairman Walden, Ranking Members Eshoo and Butterfield, Members of both subcommittees, thank you for this opportunity to discuss the issue of Internet privacy.

The right to privacy is a core American value, and the Federal Communications Commission, at the direction of Congress, has worked for years to implement laws that protect the privacy of consumers when they use communications networks and services.

The Internet, which has enabled information sharing on an unprecedented scale, raises new privacy challenges. The FCC is committed to working with Congress, the Federal Trade Commission, the Department of Commerce, and our other colleagues across the government to tackle these issues.

To understand the importance of privacy challenges in the digital age, one must appreciate the extraordinary opportunities created by broadband Internet services. High-speed Internet is an indispensable platform for innovation and economic growth, creating 2.6 new jobs for every job lost according to a recent study. The U.S. captures more than 40 percent of global Internet revenues, making broadband essential to American job creation, as well as our global competitiveness. And broadband has unlocked new opportunities to transform health care, education, energy, and public safety.

To fully realize the benefits of broadband people need to trust that the Internet is safe and secure.

Privacy concerns are a barrier to broadband adoption. When people fear that new technology puts their privacy at risk, they’re less likely to use those new technologies. This was one of the important findings of the FCC’s National Broadband Plan, in connection with data showing that one-third of Americans aren’t online.

Consider cloud computing – a \$68 billion global industry that’s growing 17% annually, with enormous opportunities to generate job creation and consumer benefits. Trust is essential to the growth of this promising industry and also the broader economy.

If small businesses don't trust the Internet and consequently don't take advantage of cloud-based opportunities to reach new customers and lower costs, that's a lost opportunity for our economy.

Location-based services similarly offer large economic and consumer benefits. McKinsey estimates that this growing sector will deliver \$700 billion in value to consumers and business users over the next decade, and businesses that use geo-location technologies are already creating hundreds of jobs a month.

The new opportunities presented by location-based technologies also extend to areas like public safety. And indeed, the FCC is working on an initiative to improve the location accuracy of mobile 911 calls.

Two weeks ago, the FCC, with the participation of the FTC, hosted a workshop on helping consumers harness the potential of location-based services while protecting basic ideals of consumer choice. The discussions at the workshop highlighted the fact that consumers and businesses alike are upbeat on the many opportunities created by location-based services. Stakeholders also recognize the importance of addressing privacy questions, both to protect basic privacy values, and so that consumer concerns about the use and security of their location information do not slow the adoption of innovative services or undermine the opportunities.

It is clear we need to strike a balance – ensuring that personal information and consumer choice is protected, and at the same time ensuring a climate that encourages new investment and new innovations that will create jobs and improve our quality of life.

At the FCC, our approach to privacy centers on three overarching goals: 1) Consumer control and choice; 2) Business transparency about privacy practices, and 3) Data security.

Congress has long recognized that protecting privacy is fundamental to a healthy communications landscape. Congress has also long recognized that, as the nation's expert agency on our communications networks and infrastructure, the FCC has an important role to play in protecting the privacy of consumers using our nation's communications networks.

The Communications Act charges the FCC with implementing a number of privacy protection provisions. Section 222, for example, requires telecommunications carriers to safeguard information about whom consumers communicate with, the length of time they spend using the network, and their location when they use wired or wireless services – what we call customer proprietary network information, or CPNI.

The FCC has adopted rules regarding the handling, use, and sharing of CPNI and vigorously enforces those rules. In the last six months, the Commission issued an Enforcement Advisory, reminding companies of their CPNI obligations, and we have issued 28 Notices of Apparent Liability and warnings for CPNI violations under Section 222.

Through our rulemakings and enforcement, the FCC has addressed 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.

Sections 338 and 631 of the Communications Act require satellite and cable providers to give subscribers clear and conspicuous notice and choice about the collection and use of their personally identifiable information such as name plus address, financial account information, and Social Security number. Those sections of the Communications Act also provide consumers with legal remedies if their personal information is improperly collected, used or disclosed.

At the FCC, we recognize that educating consumers and small businesses about privacy and data security can provide substantial benefits. For example, we want to get the message out to consumers that they need to secure their home Wi-Fi networks, so we've developed an online guide on how to activate the encryption features on wireless routers. Two months ago, the FCC released a cybersecurity tip sheet to help small businesses understand and implement basic precautions to secure their networks and data. We have partnered with the U.S. Chamber of Commerce, the National Urban League and others to develop and distribute this tip sheet and other educational resources.

We have also worked collaboratively with other agencies to educate consumers, making sure they are getting the same clear information and guidance from government agencies like the FCC, the FTC, the Small Business Administration, and the Department of Commerce.

The Small Business Administration was a partner in our small business cybersecurity initiative. We've partnered with the FTC on education efforts like Net Cetera and OnGuard Online, which offer consumers advice on how to protect their children's personal information, guard against identity theft, and avoid email and phishing scams. The FCC also is a member of the National Initiative for Cybersecurity Education partnership led by the Department of Commerce.

Our collaborative efforts extend beyond education.

The FCC and FTC jointly implemented and enforce the "Do-Not-Call" rules. Since 2009, the FCC has issued nearly 150 warning citations and other enforcement actions for Do-Not-Call violations. We have also worked with the FTC in implementing the CAN-SPAM Act to prevent unwanted commercial email messages from being sent to consumers' wireless accounts.

As we tackle privacy issues, it's worth keeping in mind three points about technology that are virtually always true. Technological advances bring great benefits for our economy and consumers. The same technological advances can bring new dangers and challenges. And technology can help address those dangers and challenges.

This is all true of the area we discuss today. Technology can and must be part of the solution. I continue to encourage industry to use its expertise to empower consumers, provide transparency, and protect data.

Many companies are already doing so. For example, in connection with mapping and navigation services offered by wireless providers, in most instances, the first time a consumer uses such a service, he or she sees a pop-up notice asking consent to the collection and use of location information. Providing that kind of timely information and choice to consumers creates a climate of informed trust, which encourages consumer adoption of new products and services, and furthers innovation and economic growth.

To conclude, broadband and the new technologies and services it makes possible are creating incredible opportunities that spur our economy and improve our quality of life. Seizing these opportunities will require us to tackle emerging privacy challenges. As the government's expert agency on broadband and communications networks, with a long history of taking common-sense steps to protect consumer privacy, the FCC has an important role going forward. Our network-focused privacy and data security rules are sound, settled, and legally tested. Some updating of the Communications Act's network-oriented privacy regime is appropriate for the digital age. But that can be done harmoniously with other agencies' implementation of any generally applicable consumer privacy or data security legislation.

We look forward to working with Congress, with my colleagues here at the table and elsewhere, and with all stakeholders outside of government to harness technology to promote innovation, job creation and economic growth, while protecting basic principles of privacy.

Thank you again for this opportunity to testify. I look forward to your questions.