

Statement of Commissioner Edith Ramirez
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
and
Subcommittee on Communications and Technology
U.S. House of Representatives
Washington, DC
July 14, 2011

Chairman Bono-Mack, Chairman Walden, Ranking Members Butterfield and Eshoo, and Members of the Subcommittees, I am Edith Ramirez, a Commissioner of the Federal Trade Commission. I appreciate the opportunity to present the Commission's testimony on Internet privacy.

Today, personal information about consumers may be collected, sold, and used in almost every conceivable interaction a consumer has, both online and offline. For instance, a college freshman sits in her dorm room using the Internet to research depression for a paper she is writing for a psychology class. When her research is done, she applies online for student loans to help her pay her tuition. Later, heading out of her dorm room, she grabs her smartphone, which she uses to find the closest drugstore. At the drugstore, she uses a loyalty card to get discounts. Afterwards, when the student is back online surfing the web and keeping up with friends on a social network, she sees advertisements for medication for depression and anxiety as well as ads for high-interest credit cards and payday loans.

These activities – made possible by technology unimaginable years ago – offer clear benefits to the student: she enjoyed easy access to information, received discounts at the drugstore, and connected with friends, all in the course of a few hours. But the student is likely unaware that data about her drugstore purchases, web activities, and location may have been sold to data brokers she has never heard of and added to a growing digital profile about her. She may

not know that this information may be used for marketing purposes or to make decisions about her eligibility for credit. And she might be especially surprised to learn that her research into depression may be included in her digital profile, and could be used when she applies for life insurance or might be sold to prospective employers when she graduates a few years later.

The student is not alone in her lack of awareness that vast quantities of information about her are mined and sold every day. Most consumers have no idea that so much information about them can be accumulated and shared among so many companies – including, employers, retailers, advertisers, data brokers, lenders, and insurance companies.

The FTC wants consumers to have effective notice and meaningful choices about what data is collected about them and how it is used. That, in turn, will engender the consumer confidence and trust that are essential for industry to continue to innovate and flourish.

For decades, the FTC has been the nation's lead law enforcer on consumer privacy and data security. During this time, we have also engaged in substantial policy initiatives and educated consumers and businesses on privacy and data security. In recent months, we have brought a number of significant enforcement actions in this area, as described in our written testimony. Just two weeks ago, we announced an action against Teletrack, Inc., a company that sold lists identifying cash-strapped consumers to marketers in violation of the Fair Credit Reporting Act. To resolve our allegations, the company has agreed to pay a \$1.8 million civil penalty and to submit to a court order that ensures that consumers' sensitive credit report information is not sold for marketing purposes.

Privacy and data security also continue to be at the forefront of the FTC's policy agenda. In December 2010, Commission staff issued a preliminary privacy report that recommended three bedrock principles. The first is "privacy by design" – the idea that companies should

embed privacy protections into their products and services from the start. Second, companies should present choices about the privacy of personal data in a simple way and at the time they are making decisions about that data. Third, companies should improve the transparency of their privacy practices, thereby promoting competition on privacy.

Finally, the staff report called for the adoption of Do Not Track – a one-stop tool for consumers to control online behavioral tracking. The Commission has not taken a position on whether Do Not Track legislation is needed, but a majority of Commissioners, myself included, supports widespread implementation of Do Not Track.

In closing, I want to note that the Commission appreciates the Committee's focus on consumer privacy and data security, and we are prepared to provide any assistance you may need on these critical issues. Thank you.