
Federal Trade Commission Signals Intensified Focus on Security-By-Design and the Internet of Things With New *Start with Security* Initiative for Small and Medium-Sized Businesses

MAY 22, 2015

The Federal Trade Commission (FTC) recently launched a new *Start with Security* initiative that aims to provide businesses with resources, education and guidance on best practices for data security. [Announced by FTC Consumer Protection Director Jessica Rich](#) at the International Association of Privacy Professionals' annual Global Privacy Summit in March, the *Start with Security* initiative will initially focus on encouraging small and medium-sized businesses to embrace security-by-design principles. The FTC will hold a series of presentations, seminars and meetings across the country to educate companies and groups about best practices for evolving security needs.

Last week, FTC Chairwoman Edith Ramirez [announced that the initiative's first seminar](#) will take place on September 9, 2015, at the University of California Hastings College of Law in San Francisco. The event will bring together experts from across the country to discuss guidelines for data security, particularly for smaller businesses.

The *Start with Security* initiative seeks to encourage companies to build security into devices from the start, rather than as an afterthought in the design process. With small and medium-sized businesses collecting increasingly large amounts of sensitive customer data, Commissioner Ramirez has expressed concern about the proliferation of new organizations entering the market without the security experience of more mature businesses, noting that smaller businesses often lack the same data security experience as more mature technology companies.

The FTC seems particularly concerned with security issues relating to the Internet of Things-the emerging market of everyday devices that are now Internet-connected and continuously tracking personal data. As the Internet of Things grows to include more and more components of households and vehicles, the FTC is emphasizing the importance of prioritizing security in the initial design process, rather than launching potentially insecure beta versions and increasing security over time.

"The number of Internet-connected devices that may be vulnerable to attackers is increasing exponentially," FTC Commissioner Terrell McSweeney observed in a [January 2015 article](#). "To

mitigate security risks, the FTC recommends that [Internet of Things] device manufacturers incorporate security into the design of connected products. Properly implemented, security-by-design requires manufacturers to consider security throughout the entirety of a product's lifecycle. This means, for example, incorporating security practices into the culture of a corporation, bringing security expertise into the design phase of a product, working with vendors who prioritize it, and establishing breach protocols that can be implemented when flaws are discovered or attacks occur."

Previous FTC guidance on security-by-design focused on [best practices for security in mobile app development](#). The FTC's app guidance, issued in 2013, did not dictate specific technical requirements, but instead embraced a flexible standard for app developers depending on the amount and sensitivity of the information collected. The FTC provided a dozen tips for mobile app developers, such as practicing data minimization and carefully selecting software libraries or third-party services. These tips focused on thinking critically about security needs and making informed decisions on best practices for the individual company.

The launch of the *Start with Security* initiative comes at a time when the FTC is facing criticism from companies that claim they lack sufficient guidance on acceptable security practices. Recently, [the FTC was sued](#) for "the failure . . . to disclose documents . . . describing standards, guidelines, or criteria for what conduct or omission constitutes an unfair act or practice in or affecting commerce authorizing FTC action, and criteria for bringing such an action, under 15 U.S.C. § 45, related to data or cyber security."

While the FTC's initial focus in the *Start with Security* initiative has been on providing guidance to small and medium-sized businesses, it also serves to put companies of all sizes on notice that the FTC will be increasingly targeting security practices relating to emerging technologies, apps and connected household devices. We will monitor the initiative closely as it evolves. The lawyers in WilmerHale's Cybersecurity, Privacy and Communications Practice are available to discuss the implications of this initiative and to help clients develop strategies for avoiding scrutiny by the FTC and other regulators in this area.