# Internet of Things by Michael Whitener

This year at the Consumer Electronics Show (CES), the top trend was the Internet of Things - the concept that all of our digital devices can be connected and controlled through one source such as a smartphone app. There is a great deal of buzz over a wide variety of new products in this area, and it has been predicted that the global market for Internet of Things devices and services will exceed $7 trillion by 2020, encouraging companies of all types to try to grab a piece of the market. However, this opportunity comes saddled with serious concerns over privacy.

In fact, the FTC Chairwoman, Edith Ramirez, kicked off CES with an opening statement in which she gave a stern warning regarding the threats to privacy presented by the Internet of Things. She estimated that 25 billion connected devices will be in the market this year, meaning that consumers will need to be on high alert for privacy invasions such as “smart home hacking.”

Ramirez identified three key challenges to personal privacy as the Internet of Things expands: 1) ubiquitous data collection, or a digital trail of personal information; 2) unexpected use of consumer data, meaning that information could be shared in a way that would adversely impact individuals; and 3) heightened security risks, such as the breach of multiple devices at once.

According to Ramirez, the solution to the privacy issues that surround these connected devices starts in development. She urged that companies developing these devices keep security top of mind in their design and that they fully understand the possible privacy consequences of their design choices. The more security is built in up front, the more consumers will trust that these devices are safe, allowing the Internet of Things to continue to grow.

Michael Whitener is a VLP Partner. Michael conducts privacy audits and risk assessments, drafts privacy policies and data transfer agreements, and advises on compliance with U.S. and foreign data privacy laws and regulations, including COPPA, HIPAA, the Gramm-Leach-Bliley Act and the EU Data Protection Directive (e.g., Safe Harbor certification).