LOEB & LOEB LLP

Privacy

JANUARY 2015

FTC Recommends Privacy and Security Best Practices for the "Internet of Things"

by Ieuan Jolly, Partner

The Federal Trade Commission released a staff report on the Internet of Things, recommending ways companies can minimize the data they collect, suggesting specific steps to increase security of connected devices, and providing examples of how companies can provide notice on devices that might not have a consumer interface.

The recommendations in the report address two key concerns: that data stored on and flowing between connected devices can be hacked and that consumers might not know how their data is being used.

Although the recommendations in the report are voluntary, the FTC reminds businesses that it has "a range of tools currently available to protect American consumers' privacy related to the Internet of Things, including enforcement actions under laws such as the FTC Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act." While the technology enabling connected devices is still developing, the FTC's new IoT privacy report is a wake-up call to companies in this growing industry to take seriously privacy and security concerns raised by connected devices.

Scope of Report

The Internet of Things refers to devices and sensors that are connected to the Internet and send and receive data. The FTC's report is limited to devices that are sold to or used by consumers; it does not address devices sold in a business-to-business context or devices that enable machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Consumer-facing connected devices include:

- Internet-connected cameras that allow you to post pictures online with a single click;
- Home security and automation networks that can be controlled remotely, typically through an app on a smartphone or tablet;
- Smart meters that measure home energy use and can suggest ways to improve energy conservation;
- Internet-connected cars with sensors that offer real-time vehicle diagnostics to drivers and service facilities and automatic alerts to first responders when airbags are deployed;

- Health monitoring devices that can transmit data directly to the doctor's office; and
- Fitness trackers that enable sharing data with friends.

The report is not intended to apply to computers, smartphones, and tablets. Its recommendations can be broken down into three areas: data minimization, providing notice to consumers, and incorporating security into devices and company operations.

Data Minimization

The FTC suggests companies limit the collection of consumer data, and retain that information only for a set period of time. Companies can collect no data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect.

- *Example*. Suppose a wearable device can assess a consumer's skin condition. The device does not need to collect precise geolocation information in order to work; however, the device manufacturer believes that such information might be useful for a future product feature that would enable users to find treatment options in their area. Rather than collecting precise geolocation information now, the company could wait until the new feature is activated to collect such information (after obtaining consent because the FTC considers precise geolocation to be sensitive information). Another approach would be collecting less information, such as collecting zip code rather than precise geolocation information.

Notice and Choice

The FTC reiterates that not every collection of data requires providing privacy choices to consumers. In its 2012 privacy report, the FTC stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits. The FTC's concern is when a company uses data in ways a consumer might not expect.

- *Example*. Consider when the manufacturer of an internet-connected oven should provide notice and choice. If the company decides to use the consumer's oven-usage information to improve the sensitivity of its temperature sensor or to recommend another of its products to the consumer, it need not offer the consumer a choice for these uses, which are consistent with its relationship with the consumer. On the other hand, if the oven manufacturer shares a consumer's personal data with, for example, a data broker or an ad network, such sharing would be inconsistent with the context of the consumer's relationship with the manufacturer, and the company should give the consumer a choice.

The FTC also provides examples of how companies can provide notice about privacy choices on connected devices, especially when there is no consumer interface.

- Providing choice at the time of purchase;
- Providing video tutorials that explain how to manage privacy settings;

- Affixing a QR code or similar barcode, that, when scanned, would take the consumer to a website with information about the applicable data practices and enable consumers to make choices through the website interface;
- Providing choices during set-up, for example as part of a set-up wizard;
- Using command centers or dashboards to provide notice and choice;
- Using icons on the device to convey when a device is connected to the internet and providing a switch for turning the connection on or off;
- "Out of Band" communications requested by consumers, such as allowing users to receive information through emails or texts;
- Providing general privacy settings, such as low privacy, medium or high;
- Applying a user's privacy preferences from one device to all devices in a network or family of devices.

Security

The FTC reiterated best practices for security from previous reports such as:

- Build security into devices at the outset, rather than as an afterthought in the design process;
- Train employees about the importance of security
- Ensure that outside service providers are capable of maintaining reasonable security, and provide reasonable oversight of the providers;
- Consider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;
- Monitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks.

For more information about the FTC's new IoT Report, or advice on implementing privacy and data security protocols into your devices and applications, please contact Ieuan Jolly.

Advanced Media and Technology Practice

KENNETH A. ADLER	KADLER@LOEB.COM	212.407.4284
AMIR AZARAN	AAZARAN@LOEB.COM	312.464.3330
IVY KAGAN BIERMAN	IBIERMAN@LOEB.COM	310.282.2327
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
TAMARA CARMICHAEL	TCARMICHAEL@LOEB.COM	212.407.4225
MARC CHAMLIN	MCHAMLIN@LOEB.COM	212.407.4855
MARGARET CHARENDOFF	MCHARENDOFF@LOEB.COM	212.407.4069
PATRICK N. DOWNES	PDOWNES@LOEB.COM	310.282.2352
CRAIG A. EMANUEL	CEMANUEL@LOEB.COM	310.282.2262
KENNETH R. FLORIN	KFLORIN@LOEB.COM	212.407.4966
DANIEL D. FROHLING	DFROHLING@LOEB.COM	312.464.3122
NOREEN P. GOSSELIN	NGOSSELIN@LOEB.COM	312.464.3179
DAVID W. GRACE	DGRACE@LOEB.COM	310.282.2108
NATHAN J. HOLE	NHOLE@LOEB.COM	312.464.3110
MELANIE J. HOWARD	MHOWARD@LOEB.COM	310.282.2143
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
ELIZABETH H. KIM	EKIM@LOEB.COM	212.407.4928
JANICE D. KUBOW	JKUBOW@LOEB.COM	212.407.4191
JULIE E. LAND	JLAND@LOEB.COM	312.464.3161
JESSICA B. LEE	JBLEE@LOEB.COM	212.407.4073
SCOTT S. LIEBMAN	SLIEBMAN@LOEB.COM	212.407.4838
DAVID G. MALLEN	DMALLEN@LOEB.COM	212.407.4286
DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
NERISSA COYLE MCGINN	NMCGINN@LOEB.COM	312.464.3130
ANNE KENNEDY MCGUIRE	AMCGUIRE@LOEB.COM	212.407.4143
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
BRIAN NIXON	BNIXON@LOEB.COM	202.618.5013
SUE PAIK	SPAIK@LOEB.COM	312.464.3119
ANGELA PROVENCIO	APROVENCIO@LOEB.COM	312.464.3123
KELI M. ROGERS-LOPEZ	KROGERS-LOPEZ@LOEB.COM	310.282.2306
SETH A. ROSE	SROSE@LOEB.COM	312.464.3177
ROBERT MICHAEL SANCHEZ	RSANCHEZ@LOEB.COM	212.407.4173
ALISON SCHWARTZ	ASCHWARTZ@LOEB.COM	312.464.3169
BARRY I. SLOTNICK	BSLOTNICK@LOEB.COM	212.407.4162
BRIAN R. SOCOLOW	BSOCOLOW@LOEB.COM	212.407.4872
WALTER STEIMEL, JR.	WSTEIMEL@LOEB.COM	202.618.5015
AKIBA STERN	ASTERN@LOEB.COM	212.407.4235
JAMES D. TAYLOR	JTAYLOR@LOEB.COM	212.407.4895
JILL WESTMORELAND	JWESTMORELAND@LOEB.COM	212.407.4019
DEBRA A. WHITE	DWHITE@LOEB.COM	212.407.4216
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960