Internet of Things Issues Guide

Internet of things issues guide

Devices that formerly existed in only the physical world are now entering the digital world, and as a result, the Internet of Things (IOT) is here. Both familiar and unfamiliar objects are part of the IOT: toothbrushes that track one's brushing pattern,[1] wireless blood pressure monitors that connect seamlessly with one's phone,[2] power outlets that test air quality,[3] and oil hydraulics systems that optimize energy use.[4] From improving industrial efficiency to driving medical insights, these technologies and devices, which are capable of sensing information and communicating it to the Internet or other networks, present a tremendous opportunity for citizens, companies, and governments alike.[5] To seize this opportunity, companies traditionally operating in the physical world are entering into one that they might find unfamiliar—the digital world.

Connecting devices to the Internet requires companies account for new considerations: primarily those related to communications, privacy, and cybersecurity. This guide is meant to address these concerns, and is aimed at helping IOT device manufacturers, or original equipment manufacturers (OEMs) understand the regulatory landscape in which they will operate as they enter the digital world.

Equipment authorization and radiofrequency selection

To be a part of the Internet of Things, IOT devices must be able to connect to the Internet or to other devices. Devices may do so either through a wired or through a wireless connection, though most IoT devices will communicate through wireless connections. These devices will thus need to use electromagnetic spectrum, which the Federal Communications Commission (FCC) regulates. Spectrum regulations were designed, in part, to minimize "harmful interference," where a signal originating from one device disrupts the signal of other devices using the same or neighboring frequencies.[6] At the same time, these regulations seek to encourage competition and innovation.[7]

To achieve its spectrum management goals, the FCC offers two types of spectrum: licensed and unlicensed. People interact with both types of spectrum on a daily basis. Connecting to a wireless network with Wi-Fi requires using unlicensed spectrum; connecting to a mobile carrier requires using licensed spectrum. Both types have benefits and drawbacks, which are mentioned below. OEMs must decide whether to use unlicensed or licensed spectrum. Additionally, they must determine whether their device requires Equipment Authorization from the FCC.

Unlicensed or licensed spectrum

Devices that use unlicensed spectrum can do so without express FCC authorization to access the frequencies they occupy. Consumers use unlicensed spectrum on a daily basis. Laptops, for example, connect to the internet through Wi-Fi, which communicates in the unlicensed bands of either 2.4 GHz or 5 GHz.

While the FCC's rules and policies for unlicensed devices do not require authorization to occupy radio spectrum, the FCC requires operating conditions and various forms of prior approval for the devices themselves. To market equipment that uses unlicensed spectrum, OEMs must accept any interference their devices receive and must avoid causing harmful interference. OEMs must also ensure their devices comply with Part 15 of the FCC's regulations.

The two predominant unlicensed frequencies that OEMs might design their devices to use are the 2.4 and 5 GHz bands. Devices communicating in the 5 GHz band can send greater amounts of information over shorter distances with less building penetration, and the devices require smaller antennae.[8] Devices using 5 GHz frequencies risk incompatibility with Wi-Fi routers because older routers remain unequipped to receive this frequency. Devices using 2.4 GHz communicate less information over somewhat longer distances with greater building penetration, though these devices demand longer antennae.[9] The reach of 2.4 GHz signals means that the band can become congested more quickly than the 5 GHz band.

OEMs might wish to equip their devices to be compatible with multiple frequencies and add additional capabilities. While doing so increases interoperability, it also imposes additional hardware requirements on the device. OEMs should account for any constraints on the device size when they decide which frequencies the device will use.

OEMs using licensed spectrum receive a more reliable signal, though they will need to pay for it. To use licensed

spectrum, OEMs generally will partner with a company holding a license and owning the requisite infrastructure, such as Verizon or T-Mobile. However, OEMs will need to pay as the license holder needed to purchase the spectrum and build, maintain, and operate the necessary infrastructure. Licensed spectrum is more reliable than the unlicensed variety because it receives legal protection from harmful interference.[10] Large OEMs might also decide to purchase licensed spectrum from a government auction or the secondary market.[11]

Part 15 of the FCC regulations set out the conditions and requirements for devices using unlicensed frequencies. It has eight subparts:

- Subpart A sets out general regulations regarding devices using unlicensed spectrum. This part includes provisions that restrict the devices from sending harmful interference, that prohibit OEMs from using devices to eavesdrop, and that spell out general technical requirements.[12]
- Subpart B governs unintentional radiators, such as Wi-Fi-disabled computers, televisions, and digital clocks. Unintentional radiators intentionally generate radio frequency energy, but that do not intend to emit the signals via radiation or induction.[13]
- Subpart C sets out requirements for intentional radiators, such as cell phones, walkie-talkies, and anything using Bluetooth connectivity. These devices intentionally generate and emit radio frequency energy by radiation or induction.[14]
- Subpart D regulates unlicensed personal communication service devices, which are intentional radiators operating on the 1.9 GHz frequency band that provide a "wide array of mobile and ancillary fixed communication services to individuals and businesses."[15]
- Subpart E regulates unlicensed national information infrastructure devices, such as wireless ISPs. These devices are intentional radiators operating on the 5.15–5.35 GHz and 5.470–5.85 GHz bands that "use wideband digital modulation techniques and provide a wide array of high data rate mobile and fixed communications for individuals, businesses, and institutions."[16]
- Subpart F states the technical requirements for devices using ultra-wideband operations, such as PC peripherals, wireless monitors, and device-to-printer communications. These devices transmit high volumes of data over short distances without substantial interference or energy demands.[17]
- Subpart G includes regulations for access broadband over power lines.[18]
- Subpart H relates to white space devices, which operate on unused broadcast spectrums.[19] Any device can be equipped to use white space spectrum like devices can be equipped to use Wi-Fi.

Companies traditionally operating in the physical world are entering into one that they might find unfamiliar—the digital world.

Equipment authorization

The FCC requires that all radio frequency devices (RF devices) be authorized under Part II of its regulations prior to their marketing in and importation to the United States.[20] OEMs must first determine whether their devices are RF devices, and if so, must then complete the necessary approval procedure.

RF devices are "capable of emitting radio frequency energy by radiation, conduction, or other means."[21] Almost all electronic devices are capable of emitting RF energy, and thus must demonstrate compliance with the FCC's rules.[22] Products might contain more than one RF device, and as a result, might require completing all three approvals listed below.[23] RF devices are grouped into the following four categories: incidental radiators, unintentional radiators, intentional radiators, and industrial, scientific, and medical equipment.[24]

- **Incidental radiators** are devices such well pumps, motion detection light fixtures, and photocopy machines, which are not designed to use, generate or emit radio frequency energy over 9 kHz intentionally.[25] Incidental radiators do not require equipment authorization, though they must still comply with 47 C.F.R. § 15.5.[26]
- **Unintentional radiators** are devices like Wi-Fi-disabled computers, televisions, and digital clocks. These radiators use "digital logic, electrical signals operating at radio frequencies for use within the product, or send radio frequency signals by conduction to associated equipment via connecting wiring, but [are] not intended to emit RF energy wirelessly by radiation or induction."[27] Products that contain only digital logic may be exempted from an equipment authorization.[28]
- **Intentional radiators** are devices such as cell phones, wireless microphones, and garage door openers. They "intentionally generate and emit radio frequency energy by radiation or induction that may be operated without an individual license."[29]
- **Industrial, scientific, and medical equipment** are devices like magnetic resonance equipment, medical diathermy equipment, and industrial heating equipment. They use RF energy for uses other than telecommunications. OEMs can receive equipment authorization for their device through one of three approval procedure: certification, declarations of conformity, and verification.[30]
- **Certification** is the most rigorous approval process, reserved for devices with the highest chance of harmful interference such as mobile phones, walkie-talkies, and remote control transmitters.[31] Certification requires applicants submit a written application and test data, collected by an FCC-accredited testing laboratory, to a Telecommunications Certification Body.[32]
- **Declaration of Conformity** is the procedure that requires the use of an FCC-accredited testing laboratory to ensure the device complies with appropriate technical standards. Devices subject to a declaration of conformity include personal computers, TV interface devices, and microwave ovens.[33] Companies do not need to file for approval with the FCC, but must demonstrate compliance if the FCC inquires.[34]
- **Verification** requires operators to rely on measurements that they, or another party, take on their behalf to ensure the device complies with the technical standards. Devices subject to verification include non-consumer ISM equipment, TV and FM receivers, and business computer equipment.[35] OEMs do not need to use an FCC-accredited testing laboratory, nor must they submit data to the FCC. The company must demonstrate compliance if the FCC inquires.[36]

Privacy

The promise of the Internet of Things goes beyond devices that can communicate: it also is about the volume of data that can be collected, used, and analyzed to generate new insights about the world.[37] Because Internet of Things devices might collect and transmit information about individuals, these devices may implicate privacy concerns. OEMs should understand the legal landscape in the United States regarding privacy.

The primary privacy regulator in the United States is the Federal Trade Commission (FTC). The FTC administers several statutes that have specific requirements, but more generally, the FTC regulates privacy practices through its Section 5 authority. The Federal Trade Commission Act prohibits "unfair or deceptive acts or practices."[38] Unfair is defined as practices that either "cause or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[39] Deceptive is undefined statutorily, though the FTC states that it considers deception as a material representation, omission, or practice that is likely to mislead reasonable consumers.[40]

The FTC's Section 5 authority is not the only law that protects privacy in the United States: Congress has also passed several pieces of privacy legislation that apply to specific industries, certain commercial practices, and vulnerable groups. Additionally, state law might impose additional requirements.

Unfair or deceptive acts or practices

OEMs must look to the FTC's enforcement proceedings to better understand what it expects from companies, as the Commission lacks proactive rulemaking authority. The FTC's enforcement decisions are a form of precedent for understanding privacy enforcement.[41]

To avoid allegations of deceptive acts, OEMs must disclose their privacy practices and avoid making any misrepresentations. The FTC has initiated proceedings based on deceptive privacy practices many cases, including the following: (1) a company failed to provide consumers with adequate notice about the feature;[42] (2) a company falsely claimed consumers could opt-out of tracking by using an in-browser setting;[43] (3) a company made many misrepresentations about privacy, including that it complied with the U.S.-E.U. Safe Harbor Framework;[44] and (4) a company acted against its privacy policy when it shared information with advertisers.[45]

To avoid allegations of unfair acts, OEMs should consult counsel regarding whether consumer consent is required to collect and share information. The FTC has only begun to prosecute companies for unfair privacy acts, so the standard is relatively nascent. An example of the FTC initiating proceedings against a company for unfair privacy practices is when the FTC prosecuted a company for tracking consumers without receiving informed consent.[46]

Protected information

In addition to the FTC's general proscription on unfair or deceptive practices, U.S. law also sets out privacy requirements for certain industries and types of information. OEMs should take note if they handle any of the following information.

- **Personal information about children under the age of 13:** OEMs manufacturing devices directed at children under the age of 13 or that knowingly collect personal information on children under the age of 13 must comply with the Children's Online Privacy Protection Act (COPPA).[47] COPPA applies to "any service available over the Internet, or that connects to the Internet or a wide-area network."[48] The FTC administers the statute.
- **Consumer personal finance information:** Companies "significantly engaged in providing financial products or services," as well as their affiliates and service providers, must protect consumer personal finance information pursuant to the Gramm-Leach-Bliley Act (GLBA).[49] OEMs must comply with the GLBA if they do, are affiliated with anyone who does, or provide service to anyone who does any of the following activities: (1) lending, exchanging, transferring, investing for others, or safeguarding money or securities, (2) providing financial, investment or economic advisory services, (3) brokering or servicing loans, (4) debt collecting, (5) providing real estate settlement services, and (6) career counseling of individuals seeking employment in financial services. The FTC administers the Gramm-Leach-Bliley Act.

- **Personal health information:** Two agencies impose privacy protections for personal health information: the U.S. Department of Health & Human Services (HHS) and the FTC.
    - Companies such as health plans, health care clearinghouses, health care providers who transmit health information in electronic form in connection with enumerated transactions, and the business associates of all the above must comply with the Health Insurance Portability and Accountability Act (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health (HITECH).[50] HIPAA protects all individually identifiable health information, also known as protected health information or PHI.[51] HHS administers HIPAA.
    - All vendors of personal health records, PHR-related entities, and third-party service providers that HIPAA does not cover must comply with HITECH's breach notification requirements.[52] The requirement, which the FTC administers, demands that covered entities disclose when there's been an "unauthorized acquisition of PHR-identifiable health information that is unsecure and in a personal health record."[53]
- **Consumer reporting information:** OEMs might be considered furnishers under the Fair Credit and Reporting Act (FCRA), and thus, they might face legal obligations under the Furnisher Rule.[54] FCRA protects consumer credit reports and regulates companies who regularly provide consumer information to credit reporting agencies.[55] The FTC administers FCRA.

Additional concerns: emails and text messages

OEMs might consider communicating with consumers by using text messages or email messages for a variety of reasons, such as notifying consumers about privacy practices. In doing so, they should be aware of two laws that regulate these actions: CAN-SPAM and the Telephone Consumer Protection Act (TCPA).

- **Commercial email communications:** CAN-SPAM regulates emails sent for marketing purposes. The statute applies to commercial messages, which are defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."[56] The FTC administers CAN-SPAM.
- **Auto-dialed text messages:** The TCPA prohibits auto-dialed text messages unless (1) the consumer gave consent, or (2) the message is sent for an emergency purpose. Commercial texts require consumer consent in writing, whereas oral consent is sufficient for other purposes.[57] The FCC administers the TCPA.

Cybersecurity

In 2016, hundreds of thousands of unsecured IOT devices infected with malware were coordinated to take down major websites.[58] This incident, also known as the Dyn incident, brought IOT device security into the spotlight. OEMs should understand the evolving legal landscape regarding IOT device security.

Like privacy, the FTC is the primary security regulator for IOT devices. The FTC regulates these practices primarily through its Section 5 authority, though Congress has also empowered the Commission, and other agencies, to enforce security requirements for entities handling certain types of information.

Unfair or deceptive

FTC enforcement proceedings also shed light on the expectations for IOT device security. However, this area is evolving, so FTC Staff Reports and other forms of guidance are also insightful.

To avoid allegations of deceptive practices, OEMs should ensure they have reasonable practices in place to fulfill its representations about device security. Representations can derive from overt promises to the symbols on the packaging. Examples of FTC proceedings alleging deceptive cybersecurity practices include: (1) a company providing internet-enabled baby monitors described its cameras as "secure,' but had faulty software that allowed anyone to view the feeds online;[59] (2) a company misrepresented both that its devices are secure and that it had a procedure to secure devices from unauthorized access;[60] and (3) a company misrepresented that its "cloud" environment was secure, and failed to adopt reasonable security measures to keep its environment secure.[61] Many other security-related enforcement proceedings exist.[62]

To avoid allegations of unfair practices, OEMs should also adopt reasonable security practices commensurate with "the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities."[63] The FTC has initiated unfairness proceedings against companies in the following examples: (1) a clinical laboratory that failed to adopt reasonable security measures to protect sensitive personal information;[64] and (2) a company selling devices to secure networks failed to take reasonable steps to secure its devices.[65] In LabMD, the company was handling sensitive health information. The FTC's complaint identified several security-related activities the FTC expected, such as implementing "intrusion detection system[s] or file integrity monitoring, monitoring traffic coming across its firewalls, offering data security training to its employees, and deleting any of the consumer data" the company collects.[66]

The FTC seems to be attending to the gap between the lifetime of a device and the lifetime of its software. Thus, the FTC has recommended that companies "be forthright in their representations about providing ongoing security updates and software patches. Disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the safe 'expiration dates' for their commodity Internet-connected devices."[67]

Protected Information

Like it does for privacy, U.S. law sets out security requirements for certain industries and types of information. OEMs should take note if they handle any of the following information.

- **Personal information about children under the age of 13:** COPPA requires covered entities "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[68] FTC guidance recommends OEMs minimize the data collected, share data with only providers and third parties "capable of maintaining its confidentiality, security, and integrity," hold onto information for only as long as "reasonably necessary for the purpose it was collected," and dispose of information securely once no longer a legitimate reason for retaining it.[69]
- **Consumer personal finance information:** The FTC's Safeguard Rule requires covered entities "ensure the security and confidentiality" of consumer personal finance information by taking actions such as developing "a written information security plan that describes their program to protect customer information and that is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles."[70]
- **Personal health information:** HIPAA's Security Rule requires covered entities to adopt "appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[71]

Other sector-specific concerns

Devices in regulated industries might face heightened regulatory burdens. For example, aerial devices might implicate Federal Aviation Administration regulations,[72] medical devices may fall under the U.S. Food and Drug Administration's purview,[73] motor vehicles might trigger National Highway Traffic Safety Administration regulations,[74] and devices connected to the electric grid may fall under the Federal Energy Regulatory Commission's jurisdiction.[75] OEMs should consult with their counsel to ensure they comply with the regulatory schemes relevant to their product.

Contact us

Our experienced attorneys and consultants understand the legal, technical, and business challenges to be addressed when an OEM begins to manufacture Internet of Things devices. For more information contact:

Trey Hanbury
Partner, Washington, D.C.
T +1 202 637 5534
trey.hanbury@hoganlovells.com

Trey Hanbury has a wealth of experience working for the private and public sectors on a variety of communications policy issues, including wireless, spectrum, satellite, and international telecom matters. Companies operating in the telecommunications sector face increasing competition and an ever-changing regulatory environment. Trey brings both legal expertise and an in-depth understanding of the sector.

Trey advises clients on a broad range of matters, including spectrum auctions, licensing, and allocation; mergers and acquisitions; regulatory compliance and harmful interference; procurement; and competition policy. He assists clients with obtaining regulatory authorizations and addressing regulatory issues in relation to the introduction of new products and services. He also advises on licensing issues arising from commercial transactions, rule changes, and regulatory investigations.

Alexander Maltas
Partner, Washington, D.C.
T +1 202 637 5651
alexander.maltas@hoganlovells.com

Alexander (Alexi) Maltas helps communications and media clients navigate the evolving legal and regulatory landscape to maximize flexibility and advance business interests. He also negotiates content licensing agreements for distribution of content across multiple platforms, including broadcast television, cable, satellite, and Internet distribution.

Alexi has particular experience in the legal and regulatory treatment of cable, media, and broadband Internet services. He also advises clients on the regulation of current and emerging wireless technologies, as well as telephone companies and other common carriers. He regularly represents clients in regulatory and enforcement proceedings before the Federal Communications Commission (FCC), other federal agencies, federal and state courts, and state public utility commissions. In addition, he has represented clients in significant transactions before the FCC and Department of Justice, including CenturyLink in its acquisition of Qwest Communications, Time Warner Cable in its assignment of spectrum licenses to Verizon, and Leap Wireless in its acquisition by AT&T.

Endnotes

[1] *KOLIBREE*, https://www.kolibree.com/en/ (last accessed June 27, 2017).
[2] *KBPM+*, NOKIA, https://health.nokia.com/us/en/blood-pressure-monitor?btmsg (last accessed June 27, 2017).
[3] *AWAIR*, https://getawair.com/pages/awair-glow (last accessed June 27, 2017).
[4] *Oil Hydraulics*, DAIKIN, http://www.daikin.com/products/pmc/index.html (last accessed June 27, 2017).
[5] *Technology Assessment: Internet of Things*, U.S. GOV. ACC. OFFICE (May, 2017), https://www.gao.gov/assets/690/684590.pdf.
[6] *Report of the Interference Protection Working Group*, FED. COMM. COMM'N. SPECTRUM POLICY TASK FORCE 1 (Nov. 15, 2002), https://transition.fcc.gov/sptf/files/IPWGFinalReport.pdf.
[7] *Cf. Final Rule in the Matter of Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, No. 12-268, 79 FR 48441, 48444 (Aug. 15, 2014).
[8] J. Armand Musey, *The Spectrum Handbook 2013*, Summit Ridge Group 11 (Aug. 2013).
[9] *Id.*
[10] *See generally, In the Matter of Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, FED. COMM. COMM'N., (Mar. 21, 2013)*, https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-34A1.pdf.
[11] *Accessing Spectrum*, FED. COMM. COMM'N., https://www.fcc.gov/general/accessing-spectrum (last accessed July 3, 2017).
[12] 47 C.F.R. §§ 15.1–15.38.
[13] 47 C.F.R. §§ 15.101–123.
[14] 47 C.F.R. §§ 15.201–257.
[15] 47 C.F.R. §§ 15.301–323.
[16] 47 C.F.R. §§ 15.401–407.
[17] 47 C.F.R. §§ 15.501–525.
[18] 47 C.F.R. §§ 15.601–615.
[19] 47 C.F.R. §§ 15.701–717.
[20] K 47 C.F.R. §§ 2.1–1400. *Equipment Authorization*, FED. COMM. COMM'N. (Oct. 21, 2015), https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.
[21] *Equipment Authorization* – RF Device, FED. COMM. COMM'N., https://www.fcc.gov/oet/ea/rfdevice (last accessed June 20, 2017).
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] 47 C.F.R. § 15.3(n).
[26] *Equipment Authorization* – RF Device, FED. COMM. COMM'N.
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Equipment Authorization*, FED. COMM. COMM'N.
[31] *Equipment Authorization Procedures*, FED. COMM. COMM'N., https://www.fcc.gov/general/equipment-authorization-procedures#sec1 (last accessed June 20, 2017).
[32] *Id.*; see also 47 C.F.R. §§ 2.1031–1060.
[33] *Equipment Authorization Procedures*, FED. COMM. COMM'N.
[34] *Id.*; see also 47 C.F.R. §§ 2.1071–1077.
[35] *Equipment Authorization Procedures*, FED. COMM. COMM'N.
[36] *Id.*; see also 47 C.F.R. §§ 2.951–955.
[37] *Technology Assessment: Internet of Things*, U.S. GOV. ACC. OFFICE at 4–5.
[38] *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (July, 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
[39] *Id.*
[40] James C. Miller III, *FTC Policy Statement on Deception*, FED. TRADE COMM'N. (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
[41] *See generally*, Daniel Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 COLUMBIA L. REV. 583 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.
[42] *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network*, FED. TRADE COMM'N (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.
[43] *Online Advertiser Settles FTC Charges ScanScout Deceptively Used Flash Cookies to Track Consumers Online*, FED. TRADE COMM'N (Nov. 8, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/online-advertiser-settles-ftc-charges-scanscout-deceptively-used.
[44] The US-EU Safe Harbor Framework was a legal mechanism that provided a simple process for US companies to satisfy the EU's data protection requirements so as to be eligible to receive personal information about EU data subjects. The Framework required companies to self-certify that they fulfilled 7 principles: notice, choice, onward transfer, security, data integrity, access, and enforcement. The FTC policed companies who claimed they complied with US-EU Safe Harbor through its Section 5 authority. On October 6, 2015, the European Court of Justice invalidated the Safe Harbor framework. The Safe Harbor framework has since been replaced with the Privacy Shield framework. See also, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, FED. TRADE COMM'N* (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep
[45] *Myspace Settles FTC Charges That It Misled Millions of Users About Sharing Personal Information with Advertisers*, FED. TRADE COMM'N (May 8, 2012), https://www.ftc.gov/news-events/press-releases/2012/05/myspace-settles-ftc-charges-it-misled-millions-users-about.
[46] *E.g., VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, FED. TRADE COMM'N (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.
[47] *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.
[48] *Id.*
[49] *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N. (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (quotation marks omitted).
[50] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERV. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
[51] *Id.*
[52] *Complying with the FTC's Health Breach Notification Rule*, FED.

TRADE COMM'N (Apr. 2010), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.
[53] *Id*.
[54] 16 C.F.R. §§ 660.1–4.
[55] § 15 U.S.C. 1681s-2.
[56] *CAN-SPAM Act: A Compliance Guide for Business*, FED. TRADE COMM'N (Sep. 2009), https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.
[57] *Avoiding Spam: Unwanted Email and Text Messages*, FED. COMM. COMM'N. (Feb. 22, 2016), https://transition.fcc.gov/cgb/consumerfacts/canspam.pdf.
[58] *See generally, Scott Hilton, Dyn Analysis Summary of Friday October 21 Attack*, DYN (Oct. 26, 2016), https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.
[59] *FTC Approves Final Order Settling Charges Against TRENDnet, Inc*., FED. TRADE COMM'N (Feb. 7, 2014), https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.
[60] *D-Link case alleges inadequate Internet of Things security practices*, FED. TRADE COMM'N (Jan. 5, 2017), https://www.ftc.gov/news-events/blogs/
business-blog/2017/01/d-link-case-alleges-inadequate-internet-things-security.
[61] *ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk*, FED. TRADE COMM'N (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.
[62] See, e.g., Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information, FED. TRADE COMM'N (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting; Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data, FED. TRADE COMM'N (Jan. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled; Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates, FED. TRADE COMM'N (Dec. 21, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java.
[63] *Internet of Things: Privacy & Security in a Connected World,* FED. TRADE COMM'N 31–32 (Jan. 27, 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[64] *Commission Finds LabMD Liable for Unfair Data Security Practices*, FED. TRADE COMM'N (July 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices;
[65] *D-Link case alleges inadequate Internet of Things security practices*, FED. TRADE COMM'N (Jan. 5, 2017), https://www.ftc.gov/news-events/blogs/
business-blog/2017/01/d-link-case-alleges-inadequate-internet-things-security.
[66] *LabMD Liable for Unfair Data Security*, FED. TRADE COMM'N.
[67] *Internet of Things: Privacy & Security in a Connected World*, FED. TRADE COMM'N.
[68] *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FED. TRADE COMM'N (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step6.
[69] *Id*.
[70] *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying#how.
[71] *The Security Rule*, U.S. DEP'T OF HEALTH & HUMAN SERV. (May 12, 2017), https://www.hhs.gov/hipaa/for-professionals/security/index.html.
[72] *Unmanned Aircraft Systems*, FED. AVIATION ADMIN. (May 25, 2017), https://www.faa.gov/uas/.
[73] *Medical Devices*, U.S. FOOD AND DRUG ADMIN. (May 22, 2017), https://www.fda.gov/MedicalDevices/default.htm; see also Cybersecurity, U.S. FOOD AND DRUG ADMIN. (Mar. 03, 2017), https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm.
[74] *Technology & Innovation*, NAT. HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/technology-innovation (last accessed June 5, 2017); see also Cybersecurity Best Practices for Modern Vehicles, NAT. HIGHWAY TRAFFIC SAFETY ADMIN. (Oct. 2016), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf; Vehicle Cybersecurity, NAT. HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity (last accessed June 26, 2017).
[75] *Smart Grid*, FED. ENERGY REGULATORY COMM'N (Oct. 18, 2017), https://www.ferc.gov/industries/electric/indus-act/smart-grid.asp/

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jeddah
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, DC
Zagreb

Our offices
Associated offices

www.hoganlovells.com