



Hogan
Lovells

GMCQ

Global Media Technology and
Communications Quarterly

Autumn 17

Editorial

In this issue we explore the inexorable rise of the Internet of Things (IoT). Consumers are increasingly using more and more connected devices, from smart watches to smart healthcare devices. The IoT is transforming our lives but also industry, from manufacturing and energy to transport. IoT innovations present opportunities for companies, to increase efficiency and develop leading-edge products but it also raises issues, in particular the privacy and security concerns that come with connecting devices to the internet.

At the start of the issue Trey Hanbury and Alexander Maltas from our Washington D.C. office offer a guide to IoT device manufacturers on how to navigate the US regulatory landscape, including the US FTC's rules on privacy and cyber-security. Towards the end, Yarmela Pavlovic from our San Francisco office looks at the US authorities' pilot programme to streamline premarket reviews for medical software devices.

Focusing on Europe, we have an interview with Winston Maxwell and Gianni De Stefano from our Paris and Brussels offices on the EU data protection and competition issues arising from smart transport systems (where road systems and cars communicate to share data and reduce traffic jams). Winston Maxwell also explains how Hogan Lovells helps auto manufacturers understand and plan for the huge amount of data they will be collecting, including how we use our Hogan Lovells product "getting to data nirvana". Mark Marfé from our London office looks at the IP issues for start-up technology companies collaborating with luxury brands in the wearable tech market and how best to protect the IP in the new technology.

We also have a key thought leadership piece from Michele Farquhar and Alexander Maltas in our Washington D.C. office and Winston Maxwell in our Paris office on the future of net neutrality in the US and Europe, following the US FCC's recommendation that ISPs should be subject to a lighter touch regulation in the US.

In our fifth article on p.28, experts from our global privacy team in China, Russia and Indonesia look at the trend in national governments introducing data localization rules and outline the challenges for multi-nationals operating or looking to operate in those jurisdictions.

In our final article on p.40 we wrap up with some thoughts from our Head of Strategic Communications in Washington D.C., applicable to all businesses, on how to manage a crisis and avoid the errors made by United Airlines after the widely publicized episode where a passenger was dragged off one of their planes by staff.

We hope you enjoy the issue. We think we are seeing a quiet revolution in the IoT. Whilst a lot of the focus has been on consumer products, such as wearables, we think we are going to see a big increase in spending by companies in all industries; a growth in "enterprise" IoT. Our experts can help companies navigate the issues. Visit our Global Media and Communications Watch blog for more insights over the coming months.



Winston Maxwell
Partner
Paris



Trey Hanbury
Partner
Washington, D.C.



Penelope Thornton
Senior Associate
London

Contents

03 IoT from A-Z: a roadmap to US regulations

15 Does net neutrality have a future?
A closer look at the US FCC's proposed ruling

19 'Fashiontech' hits the catwalk

22 The connected car: getting to data nirvana

28 Controlling the data flow:
China and Indonesia follow Russia's suit

37 US agency pilots streamlined process
for innovative medical devices

40 Managing your message in a crisis: strategic
communications within the bounds of the law

48 References



IoT from A-Z: a roadmap to US regulations

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

“

IoT devices will need to use electromagnetic spectrum, which the (FCC) regulates.

”

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 must decide whether to use unlicensed or licensed spectrum.

”

“

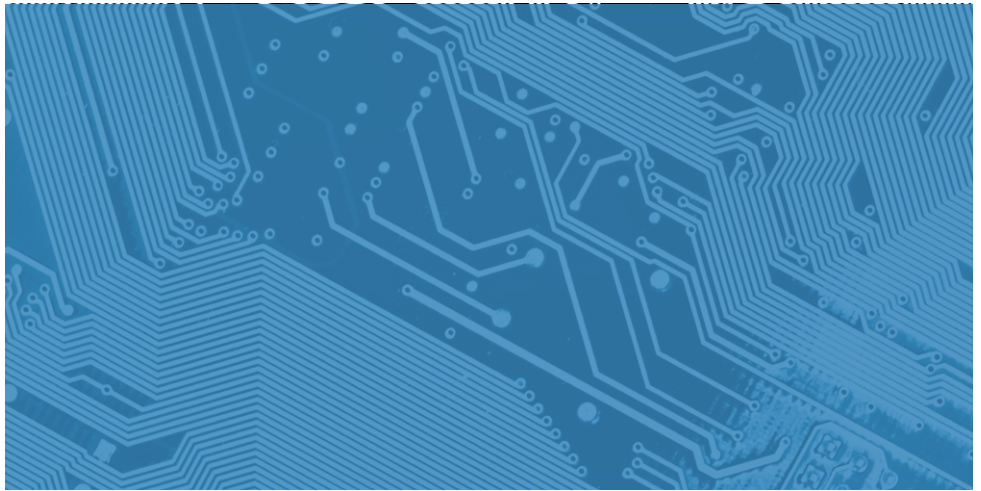
OEMs generally will partner with a company holding a license and owning the requisite infrastructure.

”

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.

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 photocopier 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 procedures: 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

“

Almost all electronic devices are capable of emitting RF energy, and thus must demonstrate compliance with the FCC’s rules. Products might contain more than one RF device, and as a result, might require completing all three approvals.

”

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



“

The FTC has only begun to prosecute companies for unfair privacy acts, so the standard is relatively nascent.

”


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 insecure 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.

”

”

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.

“

Devices in regulated industries might face heightened regulatory burdens.

”

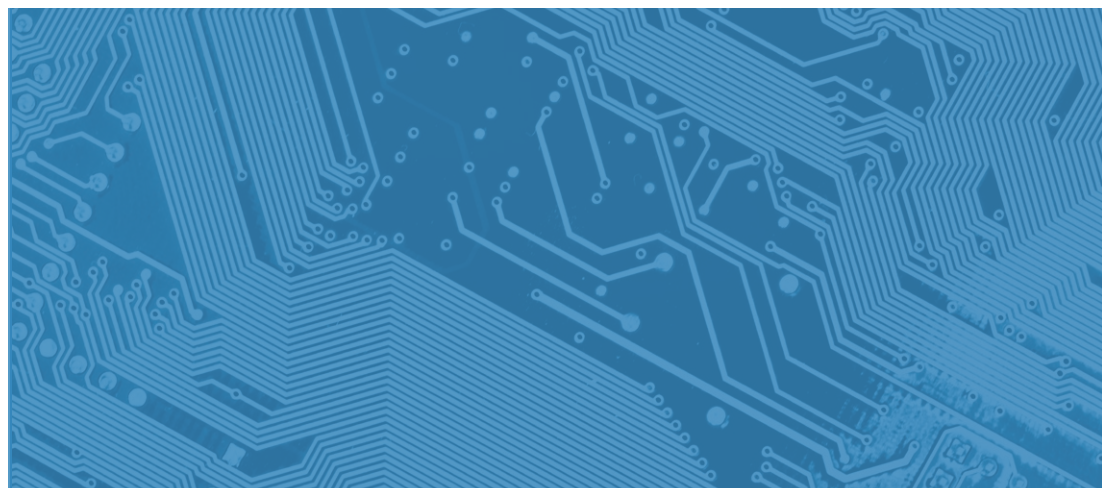
Trey Hanbury

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



Alexander Maltas

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



Does net neutrality have a future? A closer look at the US FCC's proposed ruling

The Federal Communications Commission's (FCC) notice of proposed rulemaking on the open internet⁷⁶ recommends that the FCC's 2015 Open Internet Order be rolled back, and that internet access services no longer be considered as telecommunications services regulated under Title II of the US Communications Act. This comes as no surprise because the FCC is now chaired by an appointee of the Republican party, Ajit Pai, who publicly opposed the FCC's Open Internet Order when it was adopted in 2015.

The issues concerning internet neutrality are highly politicized in the United States. Generally speaking, the Republican party defends a light-touch approach to regulation and the Democratic party supports a more proactive approach. Much of the US debate revolves around the FCC's statutory powers to regulate internet service providers. The US Communications Act, last updated in 1996, does not say a word about net neutrality. The FCC therefore had to search for a statutory basis to regulate. In 2005, under the Bush administration, the FCC restricted itself to a non-binding statement of open internet principles. Under

the Obama administration, the FCC attempted to adopt a binding regulation based on Title I of the Communications Act, but its first attempt was struck down by the federal courts.

On its second attempt in 2015, the FCC changed its legal approach by declaring that the internet access services were common carrier services subject to regulation under Title II of the Communications Act. By declaring internet access services to be telecommunications services regulated under Title II, the FCC could easily impose non-discrimination obligations on internet service providers. However, the FCC had

previously said that internet service providers should not be considered as regulated telecommunications operators but instead as providers of information services subject to lighter-touch regulation under Title I of the Act. The FCC's 2015 decision to reclassify internet access services as regulated telecommunications services constituted a break with the position historically taken by the FCC. For Ajit Pai and most members of the Republican party, this change in position constitutes a threat to internet innovation, opening the door to over-regulation. In addition, most members of the Republican party believe that binding net neutrality regulation should

have a clear statutory basis, via a law adopted by Congress. The FCC should not create regulatory powers that were not expressly given to it by the legislator.

These domestic law issues play an important role in the net neutrality debate in the US. Outside the United States, the more interesting question arising from the FCC's notice of proposed rulemaking is whether binding net neutrality regulations are necessary and useful. The utility of a regulation is generally assessed by comparing the direct and indirect social costs of the regulation with the regulation's direct and indirect benefits. The FCC's new chairman believes that the 2015 Open Internet Order does not bring a net positive benefit to society, and for this reason, should be repealed. To support his argument, Chairman Pai suggests conducting a cost-benefit analysis.

To support its theory that the 2015 order does not create net benefits, the FCC points out that there have been few disputes concerning internet neutrality. According to the FCC, this is a sign that market forces are functioning properly, and that there is no market failure requiring regulatory intervention. ISP behavior would have been the same with or without a binding regulation. Consequently, according to the FCC, the regulation created no social benefit compared to a situation with no binding regulation. In addition to not creating benefits, the FCC believes that the regulation

creates costs for society, notably a decrease in investments made by the operators. The FCC cites an annual decrease of approximately 5.6%, but produces no evidence in its NPRM to show a causal link between this decrease in investment and the FCC's 2015 regulation. In any event, it is probably too soon to draw reliable conclusions on investment levels resulting from the 2015 regulation. The FCC also states that the 2015 regulation limits the development of innovative commercial offers, including those based on commercial partnerships between content distributors and internet service providers. According to the FCC, the public could benefit from innovative internet offers based on the characteristics of two-sided markets. Even though some commercial partnerships could lead to anticompetitive practices, the FCC considers that competition and consumer protection law would be sufficient to address these abuses. To conclude, the FCC considers that the 2015 Open Internet Order creates no benefit to society and generates significant costs.

One might legitimately ask why there have not been more disputes related to internet neutrality, both in the United States and in Europe. Is it because the 2015 European Regulation and the FCC's 2015 Open Internet Order have dissuaded operators from discriminating, or is it because market forces, combined with competition law, would have achieved the same result?



“

In Europe at least, net neutrality has taken on a symbolic value, tied to fundamental rights.

”

In other words, have the FCC's and Europe's net neutrality regulations changed anything?

If we look at net neutrality from a purely economic standpoint, one can reasonably conclude that many kinds of discrimination targeted by the European and US net neutrality rules would be covered by existing competition law. A commercial arrangement pursuant to which an internet service provider favors its own content would in some cases constitute an illegal vertical restriction on competition. Competition law analysis may depend on the level of competition on the retail market, as well as how the relevant markets are defined. A report dated February 2017 prepared for the European Commission⁷⁷ confirms that many kinds of abuses relating to "zero rating" would be covered by existing competition law.

But net neutrality is not just about competition law. In a speech dated July 17, 2017⁷⁸, BEREC and ARCEP Chairman Sébastien Soriano presented the internet's open architecture as an "infrastructure of freedom". Soriano framed net neutrality as a guarantor of fundamental rights, including protection of personal data, freedom of expression and information, freedom to engage in business and innovate. In Europe at least, net neutrality has taken on a symbolic value, tied to fundamental rights. Soriano quoted Lawrence Lessig, who said that net neutrality "codes a First Amendment into the architecture of cyberspace, because it makes it relatively hard for governments, or powerful institutions, to control who says what when". Connecting net neutrality with fundamental rights raises other thorny issues that European regulators have not yet considered: When an ISP takes voluntary action to block content it considers harmful, does that constitute a net neutrality violation, a potential violation of the user's fundamental rights, or both? Violations of fundamental rights generally require a form of action by the state, which would be absent in the case of voluntary ISP filtering. And who is to judge questions that lie at the interface of net neutrality and fundamental rights? Telecom regulators are not generally empowered to judge fundamental rights.

The FCC's emphasis on the costs and benefits of regulation may lead the FCC to remove some of the more prescriptive aspects of the Open Internet Order, but keep transparency obligations so that ISPs are required to disclose their traffic management practices to the public. Transparency facilitates choice and the proper functioning of the market, and does not carry the same costs as more prescriptive regulatory measures.

Cost-benefit analysis is an essential tool for a good regulation. In the United States and in Europe, several texts require a cost-benefit analysis before any new regulation is adopted, in order to predict as far as possible the positive and negative effects of the regulation, and give preference to regulatory options that maximize social welfare. A cost-benefit analysis will give policymakers a clearer vision of the hidden costs of regulation, in particular potential negative effects on innovation and on the open character of the internet. Winston Maxwell recently published a roadmap⁷⁹ to help policymakers identify and measure the positive and negative impacts of regulations affecting the internet intermediaries. *Smart(er) Internet Regulation Through Cost-Benefit Analysis – Measuring harms to privacy, freedom of expression, and the internet ecosystem*, (Presses des Mines, 2017).



Michele Farquhar
Partner, Washington, D.C.
T +1 202 637 5663
michele.farquhar@hoganlovells.com



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



Winston Maxwell
Partner, Paris
T +33 1 53 67 48 47
winston.maxwell@hoganlovells.com

'Fashiontech' hits the catwalk



The popularity of wearable technology has seen a number of collaborations between technology companies and designer brands looking to launch the next big thing in the 'Fashion Tech' space. This summer Levi's Commuter Trucker jacket came on the market, which has Google Advanced Technology woven into the jacket, allowing the wearer to wirelessly access their phone to use apps, end a call or listen to music simply by touching their sleeve. This article looks at some of the issues and opportunities from the perspective of a new technology company (the "TechCo").

Fashion Tech collaborations are clearly advantageous for new technology companies seeking to commercialise their first wearable product. Such technology companies can benefit enormously by being linked to a big name brand with an established reputation and loyal following. The designer and luxury brands also benefit from avoiding the time and cost of the several years of research & development required to bring a new wearable to market.

Initial discussions with a potential business partner may require that TechCo discloses important details regarding its product. The TechCo will want to demonstrate its product has a unique selling point that distinguishes it from its competitors. This will require going into some detail about its technology. The fashion brand may already have some design ideas in mind and will want to understand if TechCo's technology is compatible with its vision.

Trade secrets protect information that is confidential in nature (e.g., product features and design elements if not generally known) and communicated in circumstances of confidence. The length of protection of confidential information can be (potentially) unlimited, but only if proper procedures are in place to maintain confidentiality. This should be a serious consideration for a company with limited resources as trade secrets can be difficult to enforce as it is often hard to identify the confidential information that has been misused. Non-disclosure agreements ("NDAs") can therefore be important to protect against disclosure of protected information.

“

Technology companies can benefit enormously by being linked to a big name brand with an established reputation and loyal following.

”

TechCo will need to demonstrate that its technology cannot be easily replicated by third parties. TechCo will therefore need to consider what IP rights it can obtain. Certain technological areas have been excluded from patentability. In Europe there are exclusions for computer programs and presentations of information. Recent US court decisions have established a similar position in the US where the ability to patent computerizing “abstract” ideas, such as common or fundamental business processes has been restricted. Even if an invention seems at first to fall entirely within an excluded area, it is sometimes possible to emphasize the technical aspects of the invention. It is also worth noting that a novel combination of existing technologies can also be patentable.

Even if patent protection is possible, to have value, a patent must be enforceable. Consumer-facing "front-end" features may be policed more easily. When protecting innovations through patents, TechCo faces a trade-off between disclosing information and obtaining a temporary exclusive right for commercialising their inventions. If the valuable invention is in the "back end", enforcement becomes more challenging. It is more difficult to tell if someone has copied it. If disclosing information in patent applications could help competitors to develop competing innovations based on a similar technological approach, TechCo may opt to keep its inventions secret.

Another reason patents may not be appropriate is the length of the application process. Obtaining a granted patent can take several years. Fashion evolves and changes quickly and a patent may not proceed to grant until after a trend has passed. The US Patent and Trademark Office offer inventors the option of filing a provisional application for a patent. Its purpose is to provide a lower cost first patent filing (covering the US only) and allows filing without a formal patent claim and other details. Other jurisdictions offer similar regimes. However, even a provisional application takes time to draft correctly and it will be several years after filing a patent application before the patent is granted. The process is also costly and TechCo may only have budget to patent core technologies rather than specific applications of its technology.

Design rights are an alternative form of protection where the product may not have qualified for patent protection or where cost is an issue. For example, a Registered Community Design ("**RCD**") offers EU-wide protection of the appearance of the whole or a part of a product, provided it is new with individual character. It is relatively inexpensive to file an RCD and the application process usually takes 48 hours. The relative cheapness of registering further RCDs is also an advantage, as wearable design will change as fashion trends come and go. In the US, a design patent may be a way to protect the look of a wearable product, such as its graphic user interface or its shape. Unregistered design rights automatically arise in some jurisdictions, including the EU, and can protect shape and configuration of a design.

“

Certain technological areas have been excluded from patentability.

”

“

Collaboration potentially gives TechCo's brand a big boost.

”

TechCo will not have the negotiating power of a large, established technology company so cannot steer the direction of any collaboration in the same way. Therefore, another consideration is to think early on about its future plans and direction. TechCo may need to accept that its prototype will need to change to fit the brand ethos and customers' wants. Going into the collaboration the TechCo will need to be aware its product development will be heavily influenced by its partner. This will impact any future designs especially where this is a one-off collaboration. The fashion brand's input will mean new IP rights may be created. This raises the question of who owns the newly created IP. There are a number of ways to deal with jointly created IP but it is important that the parties are aware this may arise and agree on how to proceed at the early stages of any discussions.

TechCo should also raise exclusivity early on. Will TechCo be permitted to work with third parties outside this collaboration? If the final agreement is too restrictive TechCo may be prevented from developing products in other sectors. It may be that this is acceptable and the key is using early product commercialisation as a spring board for its business but TechCo should look at whether any products it is working on in parallel may need to be shelved.

TechCo is advised to take time and think about how its brand is used in conjunction with the product. Collaboration potentially gives TechCo's brand a big boost. Co-branding will ensure the technology is associated with TechCo by the public. This is an important consideration if TechCo plans to launch products in its own name in the future although this may be met with some resistance from the collaboration partner. The fashion brand is likely to have extensive branding and trade mark guidelines and will be wary of its image being tarnished.

This Fashion Tech trend looks set to continue. There will be many opportunities available but TechCo should not rush into partnerships which although they may launch its technology onto the market quickly, in the long run may limit TechCo's future prospects.

A version of this article first appeared in Intellectual Property Magazine (September 2017).



Mark Marfe

Senior Associate, IPMT, London
T +44 20 7296 5824
mark.marfe@hoganlovells.com

The connected car: getting to data nirvana



In this hoganlovells.com interview, partner Winston Maxwell and counsel Gianni De Stefano discuss how European data protection, smart transport systems, and competition law intersect and the impact they will have on the connected car. Maxwell also discusses how Hogan Lovells helps connected car manufacturers to develop simplified frameworks that internal stakeholders can use to understand business and operational needs balanced against data protection legal requirements.

What are some of the European policy issues affecting the connected car?

Maxwell: What's interesting are all the security, environment, and other policy rules beyond privacy that affect data sharing. The European Commission is trying to develop what they call Intelligent Transport Systems (ITS). In that context, the Commission wants cars and road systems to be able to communicate effectively to reduce traffic and therefore reduce CO₂ emissions. The idea is to have smart transport systems so that you avoid traffic jams and fluidify traffic and thereby reduce greenhouse gas (GHG) emissions. The Commission wants auto manufacturers to build intelligent cars that share data.

The European Commission's European Strategy on Cooperative Intelligent Transport Systems (C-ITS) emphasizes the role that data can play in enhancing road safety, road conditions, environment, accident notifications, and so forth. Connected car makers need to have systems in place to actually share data in real time with other actors in the eco system.

“

The Commission wants auto manufacturers to build intelligent cars that share data.

”

“

What a car manufacturer views as a valid safety-related limitation to data access may be perceived as impeding their business chances by independent service providers.

”

”

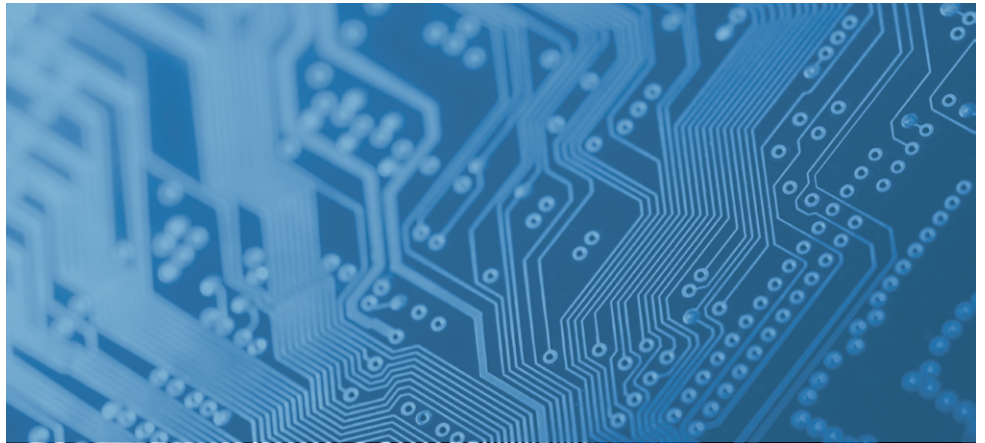
How do European data protection, smart transport systems, and competition law intersect?

Maxwell: You basically have three different policy environments that all come into play here. You have protection of personal data, you have intelligent transport systems, and then you have competition law. These three environments intersect and affect how you think about developing data governance policies for connected cars.

For example, in Europe car manufacturers need to share data with independent repair shops. If you buy a certain vehicle, the manufacturer can't lock out independent garages and force people to only go to an approved garage. An independent garage has to be able to access the data in the onboard diagnostics module, so that car manufacturers don't monopolize the repair market.

That's also going to be very important in the connected car area because there will be service providers who want to access the data in the car to provide value-added services to the user. Some players in this space want to provide the digital interface in the connected car – so it is just an extension of your smart phone. The question is, will car manufacturers embrace the entry of independent service providers or will they try to keep control over the user interface? There may be valid cybersecurity concerns relating to opening up the user interface to independent service providers. Competition law may also come into play.

De Stefano: Antitrust-savvy advice in a connected car business and/or partnership is crucial to avoid any liability down the road. What a car manufacturer views as a valid safety-related limitation to data access may be perceived as impeding their business chances by independent service providers. This could end-up in complaints or litigation.



How will competition law come into play when setting standards for the connected car?

De Stefano: The automotive industry is currently developing a set of standards that apply to the connected car (as envisaged by the EU Intelligent Transport Systems legislation). From a competition law perspective the questions that are relevant relate to the potential restriction of access of independent operators from this new business model, and/or the monitoring of their activities by OEMs which are competing with them. European competition law requires a constant balance under the legitimate concerns of OEMs to protect their intellectual property and the need to permit new market entry.

The other issue relates to sharing of information between existing stakeholders. To create standards stakeholders will need to work together. In some instances stakeholders will be (actual or potential) competitors. There is a concrete risk of "spill-over" discussions among stakeholders. There is a fine line between legitimate discussions about standards and talking about commercially sensitive information, which is forbidden.

How does Hogan Lovells help auto manufacturers map data usage scenarios to their business and operational needs?

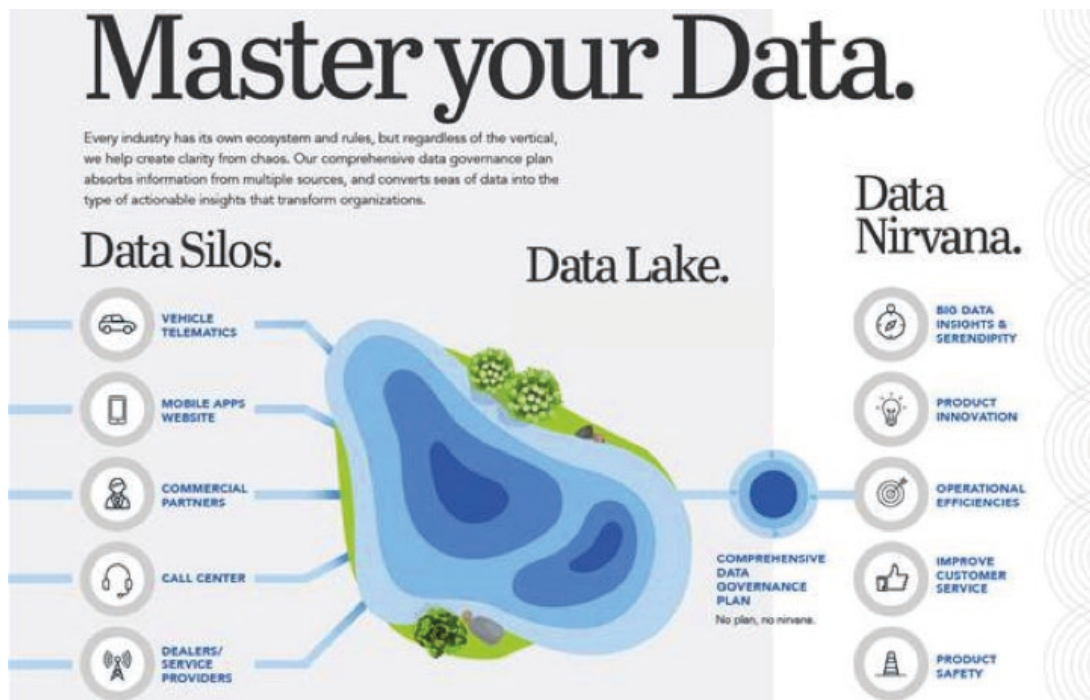
Maxwell: At Hogan Lovells, we advise auto manufacturers on how to think about embedding data protection and other data governance rules into their platforms for vehicle-related data. The manufacturers know that they are going to be collecting massive amounts of data from different sources. And they are all acutely aware that in the future the name of the game will be selling recurring, value-added services to customers. They need to be able to take advantage of the privileged

relationship that they have with the car owner to propose additional services to the full extent permitted by the data protection legislation.

I think one of the most valuable services we offer right now is to help general counsel develop internal business-friendly communication tools for the various project teams within an automotive company. These tools help identify the regulatory constraints that affect how a company thinks about data. We also help them develop a conceptual picture that includes where the data comes from – for example, website visits from the customer or a customer hotline. Then you have to think about what you are going to use the data for.

If the data is needed to save the car occupant's life, of course you are not going to ask for their consent. Saving a life comes first (and the European legislator has introduced an e-Call requirement for new cars for this purpose). If the data is necessary in connection with deciding whether you have to notify the occupant about critical maintenance – then the use of the data may be linked to the maintenance contract. But as you go along the spectrum to more value-added services like – can I use the data to propose a hotel? – you'll have stricter policies that require consent. A recent report by a German Ethics Commission says that user consent is required to use car data for anything beyond safety. But where does safety stop? OEMs focus on safety in all aspects of the car, and are likely to see data as an important tool to improve safety, including through analyzing driver habits. Data protection officials might have a more restricted view on what is necessary for safety.

We've developed a product called "getting to data nirvana", which helps automobile manufacturers create holistic data governance plans for connected car data.



De Stefano: When it comes to competition law compliance, Hogan Lovells offers to all stakeholders involved (i.e., OEMs; suppliers of car components, smart components, chips or software; and insurance companies) business-friendly compliance programs to make sure competition and other rules are not breached while they work together within their partnerships or trade associations for purposes of standards setting or data pooling.

How do you break down data usage scenarios so that each component can be tied to an actionable data protection rule?

Maxwell: We help clients make a map of the different variables so that the business people can understand. Once the business people understand, then you've won half the battle. The idea is to build the privacy rules and the other data sharing requirements into the system – engineers know how to work with that. What's difficult is when privacy lawyers or the general counsel come with big principles like – "we must respect our customers' privacy." It's too general and disconnected from the engineers' design responsibilities. What we are trying to help clients do is transform the principles into actionable rules that can be understood by the business and the engineering community at the auto company.

What I sense we do better than some of our peers is translating those principles into actionable design rules. A car manufacturer could be collecting data about falling asleep at the wheel – there are systems that watch your eyes and can tell if you are blinking too much. If those systems detect that you are falling asleep at the wheel, an alarm will be activated. Those systems could reveal drug abuse issues or other sorts of health data – it's okay to use that data to save an occupant's life but it would be hard to argue that sort of data should be used for anything else.

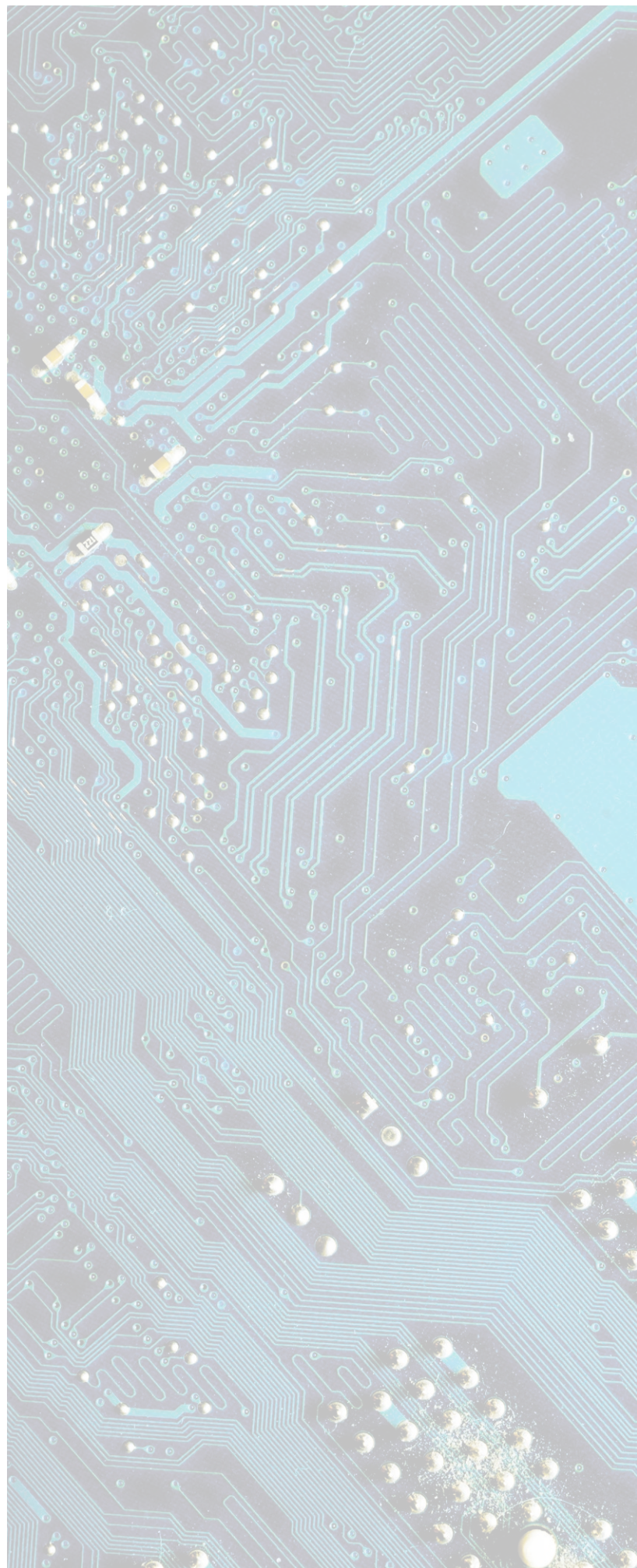
How many data usage scenarios should automakers be planning for?

Maxwell: At this point, there are so many different scenarios and data use cases, it's almost limitless. The data about my eye movement, can it be shared with an insurance company if there is an accident? The data about my GPS location, can law enforcement access it to see whether I was involved in a crime? You can go down the list and create use cases that are almost endless.

We are not trying to solve all of those usage cases now. What we are trying to do is put together clear principles about how to think about these usage cases. The principles are drafted in a way that are understandable by the business and engineering community so that they get it and understand what level of user consent is required depending on where the use case falls on the spectrum.

What are the antitrust and competition risks associated with the connected car's data?

De Stefano: The future of the automotive industry is digital. Vehicles are soon to become like our smartphones, and one of the main applications of the upcoming 5G infrastructure and services will be connected cars. One of the EU's priorities is to boost innovation and support the growth of Europe's data economy. However, from a competition law perspective, certain data is considered an asset that can potentially confer market power, especially in connected industries. There haven't been any cases yet, but the competition authorities in Europe are really focusing on this issue, with Germany and France at the forefront. First, European competition rules warrant independent operators' access to technical information in the connected automotive industry. The notion of independent operators is broad (independent repairers, spare parts manufacturers and distributors, publishers of technical information, automobile clubs, roadside assistance operators, operators offering inspection and testing services and operators offering training for repairers), and the notion of technical information is fluid and includes all possible data application in the connected cars world.



“

Competition authorities have recently begun to take into account privacy and data protection concerns to some extent.

”

Second, other practices may be subject to scrutiny (for example, discounts in return for the customer agreeing that the data belong to the OEM or another stakeholder). There are many factors that can be taken into account. For example, will the data that each OEM obtains as a result of developing connected car standards represent one single market? Would the OEM be considered the owner of those data? Or will the car user? It's something you have to focus on because competition law is about creating a level playing field, and companies considered as being dominant have a special responsibility to compete on the merits and not exclude other stakeholders.

Will the increased levels of consolidation and/or partnerships related to the connected car trigger more antitrust review in Europe?

De Stefano: In Europe, the current consolidation and/or partnerships between or among OEMs, suppliers of components, hardware or software, technology companies, and/or insurance company may need to be notified to the various merger control authorities worldwide – even when the target has limited revenues. Competition authorities have recently begun to take into account privacy and data protection concerns to some extent. When we work with clients on global merger control filings, we are also able to help them address the privacy and data protection aspects of the deal. That's thanks to Hogan Lovells' cross-practice approach to the connected cars and the needs of the players participating in the race.



Winston Maxwell
Partner, Paris
T +33 1 53 67 48 47
winston.maxwell@hoganlovells.com



Gianni De Stefano
Counsel, Brussels
T +32 2 505 09 67
gianni.destefano@hoganlovells.com

Controlling the data flow: China and Indonesia follow Russia's suit

As globalization and growth in the digital economy continues a trend has emerged worldwide of some national governments seeking to assert control and stop the flow of data across borders. China and Indonesia have recently followed Russia's suit by introducing data localization laws – laws intended to keep personal data in-country and subject to local regulation. Such laws create a significant challenge for multi-national businesses operating or seeking to operate in these countries. Below, our global privacy team outlines the legal frameworks in key jurisdictions and how to meet the challenges of operating in these jurisdictions.

China

China has introduced data localization requirements as part of the *People's Republic of China Cyber Security Law*, which was passed in November 2016. Since then, on 11 April 2017, the Cyberspace Administration of China (the "CAC") has released a draft *Security Assessment for Personal Information and Important Data Transmitted Outside of the People's Republic of China Measures* (the "**First Draft Export Review Measures**") and, on 19 May, a revised draft (the "**Second Draft Export Review Measures**").

The Second Draft Export Review Measures do, to an extent, relax some of the more stringent requirements stated in the First Draft Export Review Measures. However, the revised draft measures as set out in the Second Draft Export Review Measures still leave a significant compliance challenge for multi-national businesses operating in China ("MNCs"). While the Cyber Security Law took effect from 1 June, 2017, the data localization measures, once passed, will take effect from 31 December, 2018, introducing a grace period that will be important for MNCs to evaluate their data processing and storage arrangements under the new law.

“

The revised draft measures still leave a significant compliance challenge for multi-national businesses operating in China.

”

The Cyber Security Law regulates two key types of organisations:

- Key/critical information infrastructure ("CII") operators; and
- Network operators ("**Network Operators**")

While the scope of what constitutes CII is vague and ultimately discretionary, it is possible to discern an intent on the part of the drafters of the Cyber Security Law to regulate critical, large scale systems that would have a significant impact on the national interest (as determined by a Chinese government) if disrupted by a cyber attack. Network operators are defined to be the owners or managers of cyber networks and 'network service providers'. As 'network service providers' is not defined the potential scope is extremely broad.

The Cyber Security Law regulates CII Operators and Network Operators in different ways. Based on the text of the Cyber Security

Law, we had expected that the First and Second Draft Export Review Measures would only apply to cross-border transfers of personal data and "important data" by CII Operators, with no data localisation requirement attaching to Network Operators, unless the particular Network Operator is also a CII Operator. This, however, is not the case. Under both the First and Second Draft Export Review Measures, all Network Operators will be subject to data localization requirements.

Network Operators are expected to conduct self-assessments prior to undertaking any export of personal information or important data, and in any of the circumstances below, apply to their industry sector regulators for review prior to undertaking any export that:

- contains personal data of more than 500,000 data subjects
- involves nuclear facilities, bio-chemistry, national

defence and military sectors, public health and other such fields, as well as data on large-scale engineering projects, marine environments and sensitive geographical information;

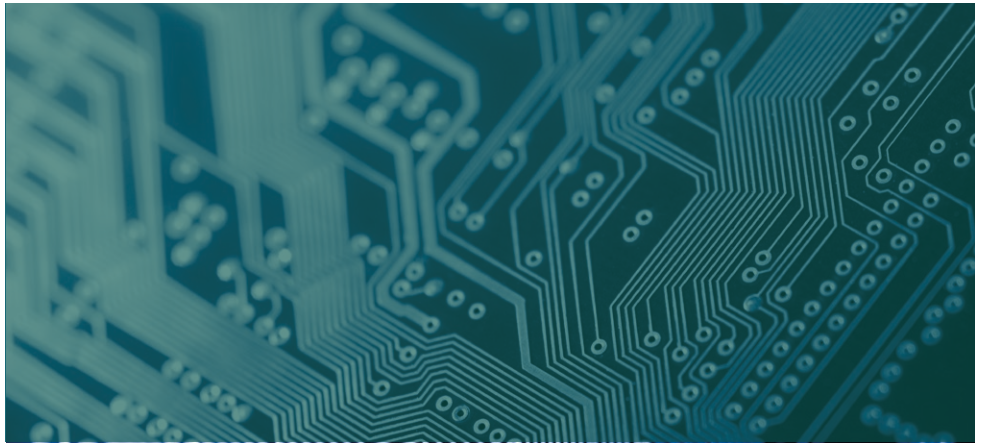
- involves system vulnerabilities and security safeguards for key information infrastructure or other such-like cyber security information; or
- any other data which may adversely impact national security and the public interest.

Article 10 of the First Draft Export Review Measures had proposed a 60 working day timeframe for regulatory authorities to provide network operators with feedback on export review assessments. This long-stop period has been replaced with a more general requirement for the authorities to provide feedback in a timely manner. This is not very helpful, as it means MNCs are not able to plan around a defined timeline framework. The

“

Network Operators are expected to conduct self-assessments prior to undertaking any export of personal information or important data.

”



version of Article 10 in the Second Draft Export Review Measures includes a materially revised stipulation that reviewing authorities shall direct that an export be stopped if any of the matters listed in Article 9 are identified in relation to an export, namely:

- the export would violate laws, regulations or departmental rules
- data subjects have not consented to the export of personal data
- the export is likely to prejudice the public or national interest
- the overseas transmission of data would jeopardize the security of national politics, military affairs, society, scientific and technological matters, information, ecology, resources, nuclear facilities and so forth; and
- any other situations where the CAC, the Ministry of Public Security or the Ministry of State Security and so forth determine that the export cannot take place in accordance with law.

Standard of Data Subject Consent

A key question arising under the First Draft Export Review Measures was the standard of data subject consent required in order to allow exports of personal data from mainland China to take place. Would an express form of opt-in consent be required, or would a more relaxed standard of implied consent be acceptable? The Second Draft Export Review Measures confirm the latter, providing that acts initiated by data subjects, such as making international telephone calls, sending emails or instant messages to overseas recipients and making cross-border transactions online would be sufficient to imply consent to export. Understanding the precise scope for implied consent to export personal data from China will be one of the key areas of interest for MNCs evaluating the impact of the Cyber Security Law.

Whilst there are some useful clarifications on China's data localization requirements in the First and Second Draft Export Measures, there are some significant points left unanswered including:

- what will the standard of review be and the relationship with existing similar provisions? Some industry sector regulators, such as the China Banking Regulatory Commission, already have data export review processes in place, so it will be important to understand how these new provisions will impact existing standards of review that have come to be understood in these industries;
- "important data" is defined as data that is closely related to national security, economic development, and the social and public interest, with reference to relevant national standards and important data classification guidelines which are still in their draft forms.
- How will existing data exports be addressed, given that many MNCs with a presence in China have operating models that involve the leveraging of offshore regional and global operating platforms? There may well be business models that are altogether not viable without offshoring data processing operations to other jurisdictions.

“

The data localization requirement will potentially apply to any party that provides information technology to the public and stores (personal) data of Indonesian citizens.

”

Indonesia

Indonesia has also introduced broad requirements for data localization. Electronic System Providers ("ESPs") that provide public services are required to store data in local data centers and arrange for disaster recovery centers by 1 December 2018 for law enforcement and data protection purposes. Specific data localization requirements for certain industries also apply, primarily in the financial sector.

The regulations relevant for ESPs are Government Regulation Number 82 of 2012 concerning System Operations and Electronic Transactions ("Reg. 82/2012") and, more recently, a Ministry of Communication and Informatics ("MOCI") Regulation Number 20 of 2016 concerning Personal Data Protection in Electronic Systems ("Reg. 20/2016"). Compliance with Reg. 20/2016 is required by 1 December 2018, allowing the market time to implement the provisions of Reg. 20/2016.

Qualifying services and data

For the purpose of determining which services and types of data are subject to data localization, the definitions of the various regulations are relevant.

An ESP is defined as any party that provides, manages, and/or operates a series of devices and electronic procedures that serve to prepare, collect, process, analyse, store, display, publish, transmit, and/or distribute electronic data (Reg. 82/2012).

The regulations only require ESPs that provide public services to store data locally. The relevant regulation does not clearly define public services. If the definition would be applied broadly, this could include any party (including privately held entities) that makes a service available to the public. Implementing regulations may provide further guidance in this respect.

The regulations seem to be intended to cover the protection of personal data. However, there are indications that the data localization requirement may not be limited to personal data alone and may in fact be applied to all data (Reg. 82/2012 and Reg. 20/2016).

Taking the various definitions as whole, the data localization requirement will potentially apply to any party that provides information technology to the public and stores (personal) data of Indonesian citizens. As is common, the various regulations refer to implementing regulation(s) that will contain further provisions. To date, no implementing regulations have been issued that provide further clarification in this respect. It does seem reasonable to conversely conclude that the data localization requirements do not apply to parties that store data that is not obtained as a result of providing a public service as an ESP (e.g. employee data of an entity's own employees).



Operation of data centers and data export

An ESP is not required to own its own data centers (Reg. 20/2016). It is allowed to lease a data center from a third party or to store data with a third party service provider. Commercial offerings have been announced for cloud services that use data centers in Indonesia, seemingly anticipating a need for such services in order to comply with Reg. 20/2016 by 1 December 2018.

Data can be mirrored/exported to data centers outside Indonesia as long as proper customer consent has been obtained, the ESP has coordinated with MOCI and has submitted the required plans and reports (Reg. 20/2016). The regulation also provides that the transfer must comply with cross-border personal data exchange legislation, however no such legislation is in effect to date.

Applicability to foreign businesses

The various regulations do not clearly determine to what extent foreign businesses that store data of Indonesian citizens are subject to the requirement of data localization. It seems to be the objective to capture all data of Indonesian citizens that is processed by ESPs providing a public service. However, some

government officials have taken the view that as a matter of general principle, there is insufficient basis to enforce the data localization requirements against foreign businesses. At the same time and for various purposes, the government is encouraging foreign businesses to establish a presence (be it as a permanent establishment for tax purposes or by incorporating an Indonesian legal entity). An argument could be made that if such presence is established, the data localization requirements would apply. Also in this respect, further implementing regulations are not yet issued and the precise obligations for foreign businesses are not clear cut.

The desire for the government to oblige the establishment of a presence for certain activities can be derived from various sources. In respect of e-commerce, the government has issued a roadmap, which refers to the mandatory registration of e-commerce service providers (Presidential Regulation 74/2017). MOCI has also announced a registration requirement for providers of Over-The-Top services (MOCI Circular Letter No. 3/2016). In both respects, implementing regulations are either in draft form and/or still need to be implemented.

Financial sector

Data localization requirements apply to certain sectors that pre-date Reg. 82/2012. Most notably, several regulations issued by the Indonesian Financial Services Authority ("OJK") require conventional banks, insurance companies and electronic lending service providers. Conventional banks can apply for an approval from OJK to use a data and disaster recovery center outside Indonesia. Certain requirements apply. Reportedly, OJK is taking a more strict approach in respect of insurers and electronic lending service providers.

Russia

Since 1 September 2015, data operators, when collecting personal data of Russian citizens, whether online or offline, are obliged to ensure a record of systematization, accumulation, storage, clarifying (updating, changing) and retrieval of such data in the databases located within the territory of Russia, except in certain limited cases (the "**Data Localization Requirement**")⁸⁰

“

When being collected, personal data of Russian citizens must be processed within the territory of Russia.

”

This means that, when being collected, personal data of Russian citizens must be processed within the territory of Russia, within a "primary" local database. The Data Localization Requirement does not directly prohibit storage of a copy of such a "primary" database abroad (i.e. use of a "secondary" database abroad), and does not restrict, in particular, cross-border transfer of personal data.

In the Russian DPA's view expressed in the meetings with the industry groups, the "primary" database where all personal data processing, including clarifying (updating, changing), is done, should be located in Russia. After the primary processing in Russia, the data may further be transferred abroad under the Russian cross-border transfer rules, where it may further be processed under the applicable regulation of the destination country.

There is no statutory definition of the term "database". However, the Russian DPA expressed its opinion in one of the industry meetings that a database is an ordered set of information in any medium (i.e. paper files, excel charts, etc.).

Exemptions

There are a few exemptions from the Data Localization Requirement. In particular, there is an exemption for *"personal data processed for the purpose of attaining objectives envisaged by an international agreement of the Russian Federation or a law, for the realisation and execution of the functions, powers and duties vested in the operator by the legislation of the Russian Federation"*.

The framework of this exemption is unclear, and many have asked the Ministry of Communications (to which the Russian DPA reports to) to clarify whether it exempts organizations from applying the localization requirements to the personal data of their employees, the processing of which is usually done in accordance with labour laws. The Ministry's guidance was vague and stated that each data operator should assess whether its actions are subject to the exemption (i.e., whether the processing is indeed done in accordance with the obligations imposed on the data operator by law). This assessment should be done on a case-by-case basis, carefully considering whether the employer is indeed processing personal data of the employees only as required by Russian law, in which case an exemption may apply, or is processing the personal data in addition in accordance with its internal/global policies/standards, in which case the exemption likely will not apply. For example, Russian labour law does not require employers to transfer personal data of employees abroad to their headquarters.

Extraterritorial Application

The Data Localization Requirement does not specify whether it applies to foreign persons or not. Under the Ministry of Communications clarifications ("**Ministry's Clarifications**") published on its website⁸¹, following the standard Russian jurisdictional rules Russian laws apply only within the territory of Russia and, therefore, the Data Localization Requirement should not apply to non-residents of Russia, including foreign businesses.

The Ministry's Clarifications, however, further stipulate that because of the Internet's cross-border nature, certain Internet activity may be considered to be conducted within the territory of Russia, and, therefore, is subject to the localization requirements. For example, a website may be deemed subject to the localization requirement if it includes a Russian language option (except where the website is translated with help of an automatic online translator) or uses a Russian top-level domain such as .ru, .su, .moscow, or the like, and at the same time there is other additional evidence confirming that the data operator is interested to include the territory of the Russian Federation into the scope of its business area (e.g. performance of the services agreements concluded online within the territory of Russia, distribution of advertisements in Russian, etc.).

The Ministry's Clarifications, therefore, establish two types of organizations that are likely targets of enforcement, reflecting the practical realities of jurisdiction: (1) organizations with a physical presence in Russia (which e.g. can be subject to on-site inspections), and (2) organizations with direct Internet activity to Russian users (whose websites can be blocked). Foreign businesses with less of a physical connection to Russia, or without a website specifically targeted to Russian users, appear to be less likely enforcement targets under the Ministry's Clarifications. That said, Russian courts have the final say on this and while the Ministry's Clarifications are helpful in determining likely enforcement targets, they do not exempt anyone from the localization requirements.

Potential Liability

A new tool against the violators of data processing rules in Russia has been in force since 1 September 2015: blocking access to the Internet websites from the Russian territory containing data processed in violation of Russian data protection laws, including the Data Localization Requirement. Such blocking can be done only upon a court's ruling.



“

The Russian DPA is currently fairly active in enforcing personal data protection regulations, in particular, on the Internet.

”

”

For this purpose the Russian DPA organized a registry of violators of data processing rules in Russia, including those who violate the Data Localization Requirement. There is a detailed procedure for adding a data operator that violates the data protection laws into such registry, and restricting access to that operator's website from the territory of Russia containing data processed in violation of Russian data protection laws.

The Russian DPA may exclude the website from the registry of violators upon receipt of application from the website owner or hosting provider, provided that measures to eliminate the violation have been duly undertaken, or a court's decision overruling the previous court's decision has been provided.

Enforcement

The Russian DPA is currently fairly active in enforcing personal data protection regulations, in particular, on the Internet and within its inspections.

Enforcement examples include, in particular, blocking of professional social network LinkedIn, administered by a non-Russian entity (LinkedIn Corporation), for failure to, *inter alia*, comply with the Data Localization Requirement⁸².

At the end of each year the Russian DPA issues its inspection plan for next year. For example, Microsoft's Russian affiliate was checked in the Spring of 2016. The Russian DPA issued an inspection report requiring that Microsoft eliminate violations revealed by the inspection by October 2016. After Microsoft submitted its compliance report, the Russian DPA in November 2016 issued a press release⁸³ stating that it considered Microsoft as compliant with Russian privacy laws, including the data localization requirement, and closing the matter.

We also note that the Russian DPA's inspections may be conducted on an ad hoc basis. Usually such inspections are initiated as a reaction to complaints filed by third parties, spotted press news, etc.

Conclusion

Whilst the Russian data localization requirements have been in force since the end of 2015, the laws in China and Indonesia have been introduced more recently. The data localization requirements in Indonesia will come into force at the end of 2018 and according to certain draft implementation rules, the data localization requirements in China will come into force at the end of 2018 as well. In China the implementation rules remain in draft form and in Indonesia no implementing regulations have yet been issued. Consequently, while we have some guidance from the regulators on how to interpret the laws in Russia, MNC's would be well advised to wait before carrying out any full assessments on data localization rules in China or Indonesia until further guidance has been published by the regulators. MNC's operating or planning to operate in China or Indonesia should however bear in mind that compliance is required by the end of 2018 and an evaluation of data processing and storage arrangements under these new laws will be required.



Maggie Shen
Senior Associate, Shanghai
T +86 185 1603 5924
maggie.shen@hoganlovells.com



Natalia Gulyaeva
Partner, Moscow
T +7 495 933 3025
natalia.gulyaeva@hoganlovells.com




Aston Goad
Counsel, Jakarta
T +62 8118818801
aston.goad@hoganlovells.com



Maria Sedykh
Associate, Moscow
T +7 495 933 3000
maria.sedykh@hoganlovells.com



US agency pilots streamlined process for innovative medical devices



In late July the US Food and Drug Administration (the "FDA" or "Agency") FDA announced a new pilot program designed to explore ways in which the Agency could streamline premarket reviews for standalone medical software products.⁸⁴ The pilot digital health software Pre-Certification (PreCert) program is designed to assist FDA in better understanding software design and development practices used by industry. The pilot will lay the groundwork for a future program in which companies would be certified by the Agency or potentially a third party. Certification would allow companies either to bypass completely or use a more streamlined FDA premarket review process. Although the pilot program may not be a good fit for many companies, anyone considering applying may wish to do so in short order.

FDA Regulation of Software

Standalone software products (i.e., products consisting exclusively of software) that are used in the individual patient care may meet the definition of a medical device and be subject to regulation by the FDA. While there have been recent changes to the Food, Drug and Cosmetic Act to exempt certain kinds of software⁸⁵ and FDA policy further exempts other types of low risk medical software,⁸⁶ many software products used by patients and physicians in the U.S. are actively regulated by the FDA. When a product is actively regulated, FDA uses a risk-based classification scheme to determine the applicable regulatory requirements. Three device classes (class I, II, and III) have been established under the current framework,

where class I devices present the least risk and class III devices generally present the most significant risk to patients. Most class I devices are exempt from any type of premarket review by FDA and may be placed on the market so long as they comply with basic FDA controls. Other class I devices and almost all class II devices go through a 510(k) clearance process where manufacturers must demonstrate substantial equivalence to existing, legally marketed class I or class II device(s), referred to as a "predicate device(s)." If products do not qualify for 510(k) clearance, they are automatically placed in class III, requiring companies to use the premarket approval, or PMA, process.⁸⁷ The PMA pathway requires demonstration of safety and effectiveness for a product.

The PreCert Pilot

The PreCert pilot program is intended to be an information gathering exercise for the Agency that would inform a future program designed to reduce the burden of software premarket review on both the Agency and industry. With that goal in mind, the future program would shift some of the Agency's focus to certification of the developers in place of a focus on clearance or approval of the individual products.

FDA indicates that in the future program, the Agency would "pre-certify" software companies who are able to demonstrate a culture of quality and organizational excellence. Once pre-certified, developers could market low-risk devices and software without FDA review, or through a more streamlined premarket review with reduced submission content and faster review. In addition, pre-certified firms could collect postmarket data to affirm the regulatory status of the product, as well as to support new product functions. Companies could potentially take advantage of the National Evaluation System for Health Technology (NEST)⁸⁸ to generate better evidence for medical device evaluation throughout the device innovation cycle. FDA is also considering third party certification.

During the pilot program, FDA is hoping to develop the elements that will be used to judge whether a company has a Culture of Quality and Organizational Excellence ("CQOE"). Elements the Agency is currently considering include (a) providing safe patient experience, (b) being clinically responsible, (c) delivering highest product quality, (d) being cybersecurity responsible, and (e) being proactive versus reactive. The Agency's goal is to identify key performance indicators ("KPI") that can be used to evaluate a company's operations. In comments made during an August 1, 2017, webinar, FDA noted that the PreCert program will likely feature multiple levels of pre-certification.⁸⁹

The pilot program that will help to inform the future PreCert program aims to enroll nine companies of various sizes and types that develop both high and low risk products. Companies will be enrolled on a phased basis, with the first 3 companies participating beginning in September 2017 and the final participants completing the program by September 2018. During webinar comments, FDA noted that the first participants should expect 3 to 4 onsite FDA visits during their participation. In response to questions, FDA also notably did not rule out the possibility of enforcement action (i.e., for identified noncompliance with current regulatory requirements) as a result of those visits, though commented that the focus is more on premarket activities that they would not expect to lead to enforcement.

“

The Agency's goal is to identify key performance indicators ("KPI") that can be used to evaluate a company's operations.

”

“

Having a variety of viewpoints included in the pilot will be key to the success of the future program.

”

FDA began accepting Statements of Interest for the program on 1 August 2017 taking into account the following criteria:

- The company must be in the process of developing or planning to develop a software product that meets the definition of a medical device;
- The company must have an existing track record in developing, testing, and maintaining software products and demonstrating a culture of quality and organizational excellence measures that are tracked by Key Performance Indicators (KPI) or other similar measures; and
- During participation of the pilot, companies must agree to:
 - Provide access to measures for developing, testing and maintaining software products and demonstrating a culture of quality and organizational excellence measures by KPI;
 - Collect real-world post-market data and provide it to FDA;
 - Meet with FDA for real-time consultation;
 - Be available for site visits from FDA officials; and,
 - Provide information about the firm’s quality management system.

The FDA has commented that a successful Statement of Interest would highlight the ways in which a candidate company is “excellent” and that information about product types in development would be helpful.

While the program is hopefully a very helpful step in the right direction, the benefits of the full program have not yet been defined. In addition, the benefits for companies participating in the pilot program are unclear at this time, beyond the ability to include their experience and perspective in FDA’s information gathering activities. Given that the program would impact many different types of programs (e.g., traditional medtech, small software developers, etc.), having a variety of viewpoints included in the pilot will be key to the success of the future program. Non-participating companies are also invited to provide comments to the Agency.




Yarmela Pavlovic

Partner, FDA/Medical Devices San Francisco

T +1 415 374 2336

yarmela.pavlovic@hoganlovells.com

Managing your message in a crisis: strategic communications within the bounds of the law



In 1961 President Kennedy faced his first major crisis, which was a disastrous botched invasion of Cuba that came to be known as the Bay of Pigs fiasco. This led the young President to establish the now famous White House “Situation Room,” as methodology for better coordination and response to unplanned significant events. More than just a physical location with secure communications from which to command a crisis situation, it is fully staffed by watch teams that monitor events; each of these teams have specified duty officers, intelligence analysts, and communications professionals.

Corporations and other large organizations are smart to establish their own virtual “Situation Room” response teams, who swing into action instantly upon the occurrence of a significant unwelcome event. United Airlines’ crisis response to the public horror show of their bloodied passenger, Dr. David Dao, being dragged off its April 9, 2017 Flight 3411 offers the perfect example of why a “Situation Room” approach is necessary.

It is easy to Monday-morning quarterback the many failures of United’s response. Those faults have not only been well-covered, but also offer little insight into exactly how and why things went so unexpectedly poorly for a company that would seem to be well equipped to manage the situation with more alacrity and aplomb. The truth is United did a great deal right several days into the crisis, but as the first 90 minutes of treatment for stroke symptoms usually determines if the victim survives or succumbs, the first 24 hours of decisions and communication of decisions determine how successfully an organization weathers a crisis. Only a pre-

established and organized “Situation Room” approach prepares an organization to immediately begin to manage adverse events.

So how would an excellent and talented CEO, such as United Airlines’ Oscar Munoz, have benefited from a different approach? What could have been done to steer towards a quicker and more successful resolution of the reputational catastrophe?

“

Only a pre-established and organized “Situation Room” approach prepares an organization to immediately begin to manage adverse events.

”

To help answer these questions, it is helpful to look at all the things United did and said in reverse chronological order. That way we can more easily observe how even when a company makes the right statements, offers generous gestures to customers, and communicates transparently and sincerely, it is often discounted as “too little-too late” if its immediate communications set into motion a public narrative that becomes nearly impossible to transform.

On March 17, 2017 Oscar Munoz would have been voted least likely of Fortune 100 CEO to stumble into the worst PR debacle of the year. On that day, Munoz received *PRWeek*’s coveted Communicator of the Year award for his efforts to reconnect his employees to the customers they serve. In accepting the award he said, “communication and communications strategy is not just part of the game, it is the game.”⁹⁰ Those insights on how important a good communications program is to a business could not be further

at odds with United’s reaction to crisis just days later.

On April 9, 2017, multiple video sites – from YouTube to the Chinese platform Weibo – recorded *billions* of views of an elderly United passenger, Dr. Dao, being bloodied and forcibly removed from the plane by Chicago Department of Aviation officers for refusing to surrender his seat, as horrified passengers looked on in dismay.

It would be hard to imagine a CEO who would be more prepared to handle a crisis of this magnitude than the man who not only was just distinguished as Communicator of the Year, but also whose vision for his company’s future is founded upon communicating and connecting his 89,000 employees with the 1.6 million customers they serve.

Reverse Chronology of Events

This is a brief analysis of United’s communications response over the three weeks following the incident. I believe it shows the leadership of CEO Oscar Munoz, and his considerable PR credentials that earned him Communicator of Year just prior to this PR catastrophe. But as praiseworthy as I believe his actions to be from the 72-hour mark to three weeks post-incident, he and those who served him dug an unnecessarily deep hole from which to climb out in just the first 48 hours. As we walk through United’s crisis response in reverse order, it allows us to see what they did well, with detectable input from the different internal stakeholders. It also will help us detect which internal stakeholders were either not in the “Situation Room,” or whose opinions were perhaps not given equal weight.

April 27, 2017. In just two and a half weeks from the date of the incident, United posted a thorough and honest review and action report, highlighting its own failures, and announcing thoughtful policy changes to assure something like this would be unlikely to ever occur again.⁹¹ Importantly, United’s review reserved all responsibility for the “terrible event” for itself and only discussed its own failures—shifting no blame to the passenger or Airport Police.

Analysis: This corrective-action plan was a considerable accomplishment in a few short days and offers evidence of a good deal of advance planning. United:

1. conducted a review and objectively explained everything that occurred;
2. described its pre-existing Involuntary Denial of Boarding process to the public, which explains why the United employees did what they did;
3. enumerated its own failures – not failures to follow its own policies but the inherent failure of the policies themselves which takes introspection and leadership;
4. announced customer-centered policy goals;

5. announced 10 immediately effective and soon to be implemented policy changes to assure achievement of those goals; and

6. spoke honestly to customers to explain the maddeningly complex practices of aircraft downsizing, moving crew, denial of boarding, overbooking, and other annoyances that can appear capricious.

No enterprise could have produced a great review and action plan in the initial 48-hour maelstrom of public criticism. A quality response such as this takes time. Unfortunately, United did not receive its due credit for it once it was produced because the public was already so turned off by United’s initial response that no one was in the frame of mind to praise

United. The proverbial well was poisoned.

What United needed to do is to purchase breathing room in the first moments after the incident came to public light to have the public grant it some grace time to fix whatever had led to this unacceptable outcome. If the strategic communications team, HR, legal, investor relations had all been summoned to the “Situation Room” and prepared to work together, it is easy to imagine that Munoz’s initial comments would not have set public sentiment so hard against the airline that their corrective action plan would receive so little praise.

“

What United needed to do is to purchase breathing room in the first moments after the incident came to public light.

”

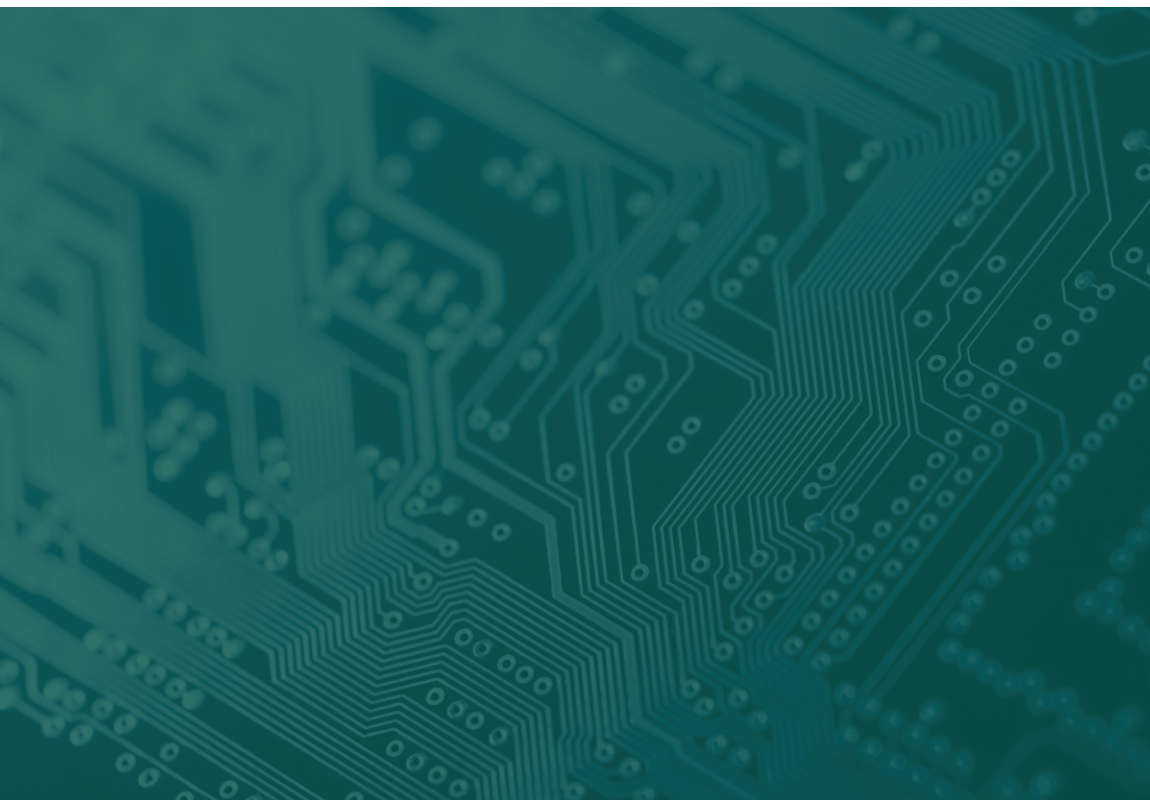
April 12, 2017. Three days after the incident Oscar Munoz went on national television to express “shame” as his predominant feeling, and apologized that the event does not reflect “who United is.”⁹² Munoz pledged that the episode will never happen again. He comes across sincerely contrite and resolute that he will fix the problem and takes ownership that it “is on him” to fix. Later in the same day, United offered to issue every passenger a full refund.

Analysis: United would receive the A+ grade one would expect from PRWeek’s champion communicator if it were the message Munoz was prepared to give in the first 24 to 48 hours immediately following the event.

But this message of contrition did not emerge until three days after the event. In the real world, of course, there’s no pause button to hit while communications and marketing professionals, legal teams, the HR department, and investor relations cobble together considered responses that hit

just the right note with every key audience of an enterprise’s community.

As a strategic communications professional, it seems clear to me that by the third day, the keepers of United’s brand—the marketing and public relations team—had not only joined the battle, but also were becoming the dominant influence on the CEO’s thinking about highest priorities for safeguarding United’s reputation.





April 11, 2017. Two days after the incident, United faced a full-blown PR nightmare and congressional hearings had already been scheduled. At that point, United took full responsibility for the “horrific event” based on a statement from Munoz.

The statement exhibited empathy for the victim and recognized the sense of anger that had welled within the public.

Munoz’s statement read as follows:

The truly horrific event that occurred on this flight has elicited many responses from all of us: outrage, anger, disappointment. I share all of those sentiments, and one above all: my deepest apologies for what happened. Like you, I continue to be disturbed by what happened on this flight and I deeply apologize to the customer forcibly removed and to all the customers aboard. No one should ever be mistreated this way.

I want you to know that we take full responsibility and we will work to make it right.

It’s never too late to do the right thing. I have committed to our customers and our employees that we are going to fix what’s broken so this never happens again. This will include a thorough review of crew movement, our policies for incentivizing volunteers in these situations, how we handle oversold situations and an examination of how we partner with airport authorities and local law enforcement. We’ll communicate the results of our review by April 30th.

I promise you we will do better.⁹⁵

Analysis: Munoz’s April 11 statement was the first evidence of cooperation between the lawyers, the HR team and the marketing and PR team. Had this customer-centric, non-blame-shifting, response been the original statement within the first 24-48 hours, United might have avoided the broadcast and on-line parodies lampooning its brand reputation. Its shareholder value might not have been temporarily sheared by \$1 billion in intraday trading. And its CEO might not have lost his planned promotion to Chairman.

This second response shows a balancing of the HR department’s desire to not blame flight attendants that were following (even if robotically and without compassion or common sense) the company’s procedural guidelines, with the brand keeper’s imperative to not blame the customer.

April 10, 2017. Monday evening, approximately 24 hours after the incident, Munoz issues a second statement in the form of a letter to reassure United employees that he was with them. His April 10 statement read as follows:

Like you, I was upset to see and hear about what happened last night aboard United Express Flight 3411 headed from Chicago to Louisville. While the facts and circumstances are still evolving, especially with respect to why this customer defied Chicago Aviation Security Officers the way he did, to give you a clearer picture of what transpired, I've included below a recap from the preliminary reports filed by our employees.

As you will read, this situation was unfortunately compounded when one of the passengers we politely asked to deplane refused and it became necessary to contact Chicago Aviation Security Officers to help. Our employees followed established procedures for dealing with situations like this. While I deeply regret this situation arose, I also emphatically stand behind all of you, and I want to commend you for continuing to go above and beyond to ensure we fly right.

I do, however, believe there are lessons we can learn from this experience, and we are taking a close look at the circumstances surrounding this incident. Treating our customers and each other with respect and dignity is at the core of who we are, and we must always remember this no matter how challenging the situation.”

Oscar⁹⁴

Analysis: The issuing of the employee eye-witness accounts of what transpired was an effort to show solidarity with employees, but reiterated what, at best, could be called biased descriptions that painted a scenario of a passenger that was refusing a \$1,000 in compensation and becoming more and more disruptive and belligerent.

United's human resources team may have succeeded in ensuring the employees felt loved and supported and were not being hung out to dry by anything the CEO might say. After all, it had to be embarrassing for United attendants and pilots to greet passengers on Monday morning and they needed to know the CEO was in this with them and that they would pull together as a family. But what Munoz's statement may have won in employee loyalty-building had the opposite effects on the flying public, which saw the statement as an Us-vs.-Them mentality pitting United against its 145 million customers.

April 10, 2017. Monday Morning following Sunday's incident, Munoz issued his first statement:

This is an upsetting event to all of us here at United. I apologize for having to re-accommodate these customers. Our team is moving with a sense of urgency to work with the authorities and conduct our own detailed review of what happened. We are also reaching out to this passenger to talk directly to him and further address and resolve this situation.⁹⁵

Analysis: United's legal team seems to have gone out of its way to ensure that there was no admission of wrongdoing in the initial statements and reiterated the uncertainty of the situation as facts remained unclear. But the statement's narrow, inconclusive focus was devoid of sincerity or empathy. It left the impression that United was unsure if it had done anything inappropriate, and that perhaps the blame might lay in part with the 69-year-old doctor or the Chicago Aviation Police. This statement is a "nonpology" in that it follows the form – but not the substance – of an apology. United expresses no regret for disrupting passengers, much less concern for the physical

safety of its customers. "Re-accommodating" is an annoying euphemization that added insult to injury because no one felt accommodated in the least. Had United at least explained the "re-accommodation" process in plain language as a "rebooking," United could perhaps have built some measure of trust for being straightforward.

The worst part of this statement, however, is that the injured passenger does not even get a "nonpology." United's legal advisors seem to have driven the company's initial response without any understanding of the business risks this approach imposed. Out of caution to do nothing that would establish legal fault on behalf of United, an overly narrow legal response may have increased the odds of litigation and the scope of the liability. In a sign of just how far United's communications strategy impaired its legal strategy, public sentiment created an atmosphere that ultimately led to an undisclosed settlement with Dr. Dao.



“
Unfortunately, public
opinion in the digital era is
like quick-set cement.
”

Who's in the "Situation Room" when the Crisis Hits Makes All the Difference

What's to be learned from this series of events? United's response was pilloried in the public eye not so much for what Munoz said, but for what he *didn't* say. His legal and human resources team played commanding roles in the first 24 hours of crisis response, but it came at the expense of how United needed to speak to customers. Had United managed public and customer sentiment at the same time that it was working to manage legal and human resource concerns it is likely it would have settled with Dr. Dao under more favorable circumstances.

United's communications-minded CEO and his team eventually got a solid message in place roughly three days after the event, and had implemented, or set the course to implement, solid reforms and financial compensation for those affected within approximately three weeks. Unfortunately,

public opinion in the digital era is like quick-set cement. And hardened public sentiment metes out punishment in the first 24-48 hours. It is very easy to envision an alternative and much improved outcome had United been prepared with a situation room where legal, HR, marketing and public affairs all reported to their duty station and had equal voice in developing a joint response.

Integration of Strategic Communications and Legal Teams

United's mistakes are replicated countless times by companies the world over, but not because these enterprises lack talented professionals to handle adverse events. To the contrary, United displayed its professional talent eventually with a sincere apology and the adoption of an extensive corrective measures program. Rather than judge United as not up to the task of containing a business crisis, think about the small measures that could have turned disaster into brilliance.

United's crisis would have tested any company, but imagine how much more deftly United could have weathered the storm if it had:

- Felt confident enough to respond to a desperate and uncertain situation with language that showed human emotion;
- Delivered a consistent, coherent message throughout a fast-changing and developing story; and
- Tempered a cold-eyed assessment of risk with an acknowledgment of an elderly man in an emotionally trying crisis.

Corporate leaders improve their companies' odds in a crisis by giving public relations, lawyers, human resources and the business leaders seats at the table. Had United implemented an integrated "Situation Room" approach to crisis preparedness, the company could have ensured that its efforts for a legal "win" did not result in a loss in the court of public opinion.



Mark Irion

Head, Strategic Communications, Washington, D.C.
T +1 202 637-5731
mark.irion@hoganlovells.com

References

- 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-google-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. DEPT 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. DEPT 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/>
- ⁷⁶ <https://www.fcc.gov/document/restoring-internet-freedom-notice-proposed-rulemaking>
- ⁷⁷ <https://www.dotecon.com/news/european-commission-publishes-report-on-zero-rating/>
- ⁷⁸ http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/7180-berec-chair-speech-at-the-speech-at-the-_0.pdf
- ⁷⁹ <https://www.pressesdesmines.com/produit/smarter-internet-regulation-through-cost-benefit-analysis/>
- ⁸⁰ The Data Localization Requirement was introduced by Federal Law No. 242-FZ of 21 July 2014 "On Amendments to Certain Legislative Acts of the Russian Federation in Relation to Clarifying the Procedure for Processing Personal Data on Information and Telecommunication Networks", which introduced amendments into the Personal Data Law and the Federal Law No. 149-FZ of 27 July 2006 "On Information, Information Technologies and Protection of Information".
- ⁸¹ The clarifications of the Ministry of Communications (in Russian): at <http://minsvyaz.ru/ru/personaldata/>. The clarifications are not legally binding.
- ⁸² Please see our alert on this case at: http://www.hldataprotection.com/2016/11/articles/international-eu-privacy/moscow-court-upholds-ruling-to-block-linkedin-in-russia-for-non-compliance-with-data-localization-law/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ChronicleOfDataProtection+%28HL+Chronicle+of+Data+Protection%29
- ⁸³ News in Russian: <https://rkn.gov.ru/news/rsoc/news41551.htm>
- ⁸⁴ See <https://www.fda.gov/MedicalDevices/DigitalHealth/ucm567265.htm>.
- ⁸⁵ See 21st Century Cures Act, available at: <https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf>; see also <https://www.hoganlovells.com/publications/president-obama-signs-21st-century-cures-act-into-law-exempting-certain-types-of-medical-software-from-fda-regulation>.
- ⁸⁶ See *General Wellness: Policy for Low Risk Devices – Guidance for Industry and Food and Drug Administration Staff* (July 29, 2016), available at: <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf>.
- ⁸⁷ See Section 513(f)(1) of the Food, Drug, and Cosmetic Act, 21 U.S.C. 360c(f)(1), available at: <https://www.gpo.gov/fdsys/pkg/USCODE-2011-title21/pdf/USCODE-2011-title21-chap9-subchapV-partA-sec360c.pdf>.
- ⁸⁸ See generally <https://www.fda.gov/aboutfda/centersoffices/officeofmedicalproductsandtobacco/cdrh/cdrhreports/ucm301912.htm>.
- ⁸⁹ See <https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm568751.htm>.
- ⁹⁰ *United Airlines CEO Oscar Munoz Named PRWeek's Communicator of the Year*, United Airlines (Aug. 8, 2017, 12:13 PM), <http://bit.ly/2os5O9i>.
- ⁹¹ *United Express Flight 3411 Review and Action Report*, United Airlines (Aug. 8, 2017, 12:15 PM), <http://bit.ly/2plgzbu>.
- ⁹² Michael E. Haydeb and Erin Dooley, *United CEO feels 'shame,' passengers will be compensated*, ABC News (Aug. 8, 2017, 12:21 PM), <http://abcn.ws/2o6tkpj>.
- ⁹³ *Statement from United Airlines CEO Oscar Munoz on United Express Flight 3411*, United Airlines (Aug. 8, 2017, 12:23 PM), <http://bit.ly/2o1vANZ>.
- ⁹⁴ Erin McCann, *United's Apologies: A Timeline*, New York Times (Aug. 8, 2017, 12:25 PM), <http://nyti.ms/2um2OeG>.
- ⁹⁵ *Id.*

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
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
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2017. All rights reserved. 11947_EUn_1117