ROTHWELL FIGG

IP Professionals

IOT and IOS Technologies and the Evolving Data Privacy and Cybersecurity Landscape: *"Danger, Will Robinson!"*

IEEE Internet of Things Summit - 21 January 2019

Martin M. Zoltick, CIPP/US

Data Privacy and Cybersecurity – IOT/IOS Technologies

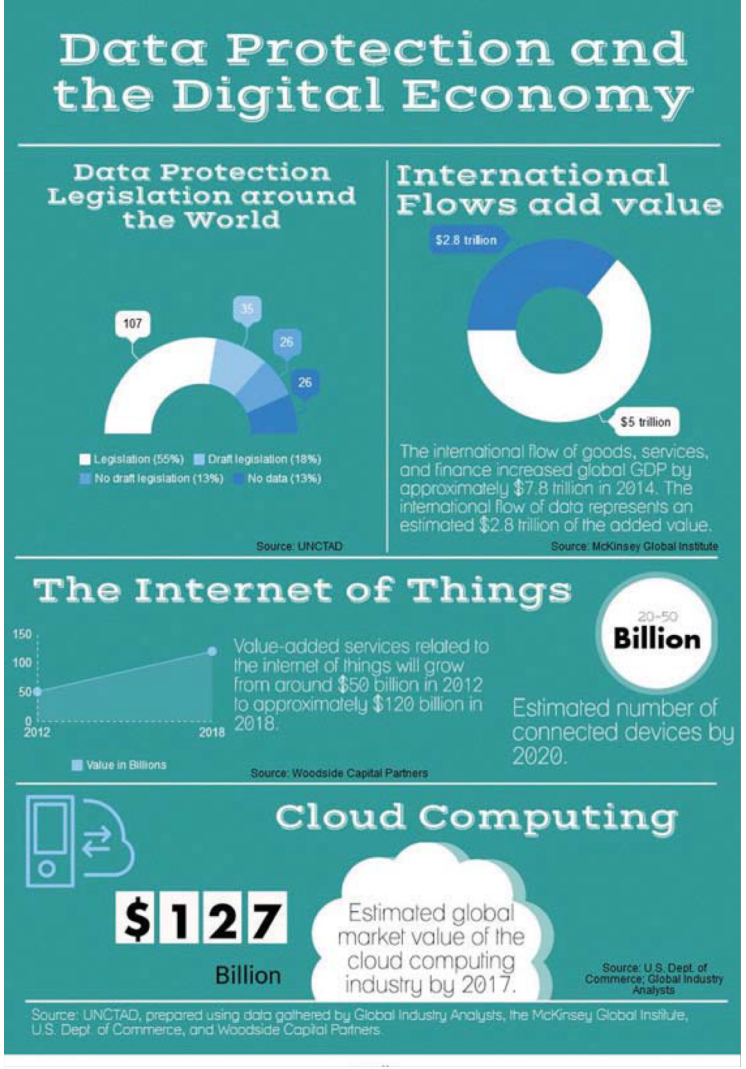
"The widespread incorporation of 'smart' devices into everyday objects is changing how people and machines interact with each other and the world around them, often improving efficiency, convenience, and quality of life."

Daniel R. Coates, Director of National Intelligence (appearing before the Senate Select Committee on Intelligence to provide the U.S. intelligence community report on Worldwide Threat Assessment (May 11, 2017).

Consider:

- The emerging Space infrastructure and deployment of space and terrestrial components, products, and services as an essential part of the ecosystem of interconnected devices and services

- The most significant challenge identified in enforcing data protection laws, rules, and regulations is difficulties dealing with cross-border issues (*e.g.*, cross-border flows of data)



ROTHWELL FIGG
IP Professionals

Data Privacy and Cybersecurity – IOT/IOS Technologies

"Their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks." (Emphasis added.)

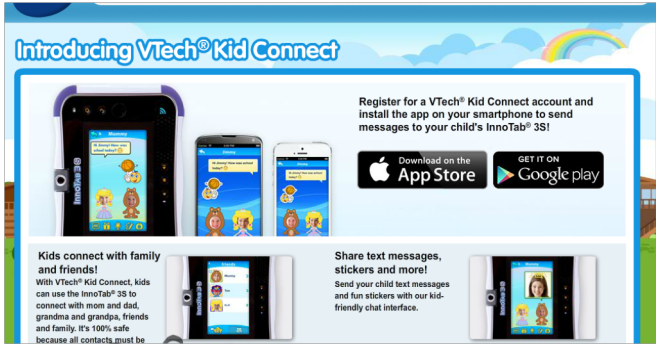
Daniel R. Coates, US Director of National Intelligence (appearing before the Senate Select Committee on Intelligence to provide the U.S. intelligence community report on Worldwide Threat Assessment (May 11, 2017).

Data Privacy and Cybersecurity – IOT/IOS Technologies

"*Increased connectivity via the internet of things ("IoT") provides fantastic opportunities for the UK. A key part of this Government's ambition is to expand on the aspirations set out in our Digital Strategy through enhancing our status as an international leader in the development and uptake of IoT. However, we must ensure that individuals are able to access and benefit from connected technologies safely, confident that adequate security and privacy measures are in place to protect their online activity. The recent Mirai and WannaCry attacks, which affected core public services and used internet connected devices to breach private companies, reinforce the need for effective cyber security as part of our digital economy*." (Emphasis added.)

Margot Janes, UK Gov't. Minister for Digital and Creative Industries (from "*Secure by Design: Improving the cyber security of consumer Internet of Things Report*" (2017).

Data Privacy and Cybersecurity – IOT/IOS Technologies



ROTHWELL FIGG
IP Professionals

Data Privacy and Cybersecurity – IOT/IOS Technologies

"*Unlike personal computers and smartphones, many IoT devices — such as security cameras, routers, light bulbs, and air conditioners — do not have screens, keyboards, or other user tools that enable owners to set passwords, adjust the default security settings, or install software-security patches. Moreover, manufacturers are loathe to drive up costs of these devices by designing and implementing additional security features; typically, IoT devices are protected by a simple default password, common to all of the devices a manufacturer sells, which could be easily guessed by hackers and exploited to amass an enormous network of bots*." (Emphasis added.)

Josephine Wolff (from "*Electrical Engineering: Attack of the Appliances*" Princeton University Alumni Weekly (Oct. 24, 2018).

Data Privacy and Cybersecurity – IOT/IOS Technologies

- U.S. -- Federal
  - ✓ FTC
- U.S. -- States
  - ✓ Calif. Senate Bill 327 & CaCPA
- EU -- GDPR
- Brazil -- GDPL
- India -- Personal Data Protection Bill
- Japan -- APPI
- Space – Int'l, Regional, and Nat'l Laws

Data Privacy and Cybersecurity – IOT/IOS Technologies

"*The present regulatory environment on protection of data is far from ideal. In fact, some countries do not have rules at all. In other cases, the various pieces of legislation introduced are incompatible with each other. Increased reliance on cloud-computing solutions also raise questions about what jurisdictions apply in specific cases. Such lack of clarity creates uncertainty for consumers and businesses, limits the scope for cross-border exchange and stifles growth.*"

Taffere Tesfachew, United Nations, Acting Director, Division on Technology and Logistics (from "*Data protection regulations and international data flows: Implications for trade and development*") (Apr. 2016).

Data Privacy and Cybersecurity – IOT/IOS Technologies

- Privacy and Data Protection Introduction
- Data Privacy Laws, Rules, and Regulations
  - EU – General Data Protection Regulation (GDPR)
  - US – California Consumer Privacy Act (CaCPA) / Senate Bill 327
  - Other countries (*e.g.,* Brazil, India, Japan)
  - Space
- Current Legal Landscape for IOT and IOS Technologies
- Best Practices and Compliance Programs

PRIVACY AND DATA PROTECTION INTRODUCTION

Privacy and Data Protection Introduction

- What is *Privacy*?
  - Right to privacy is the “right to be let alone”
  - The “appropriate” use of personal information under the circumstances
  - An individual’s right to control the collection, use, and disclosure of personal information, and to limit that information from becoming publically available
- What is *Data Protection*?
  - Handling, storing, and managing of personal information
  - Rights of individuals (notice, choice and consent, data subject access)
  - Controls on the information (information security, information quality)
  - Information lifecycle (collection, use and retention, disclosure, destruction)
  - Management (management and administration, monitoring and enforcement)

Privacy and Data Protection Introduction

- Information privacy
  - Concerned with establishing the rules that govern the collection, use, disclosure, retention, and disposal of personally identifiable information
  - An individual's right to determine how his or her personally identifiable information is collected, used, disclosed, retained, and destroyed

- Territorial Privacy
- Bodily privacy
- Communications privacy

Privacy and Data Protection Introduction

- What is *personally identifiable information (PII)*?
  - Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
  - GDPR refers to "personal data"
    - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Privacy and Data Protection Introduction

- Sensitive personal information – subset of PI requiring additional privacy and security limitations
  - Passport No, Driver's license No, SSN, Tax id
  - Financial Info and medical records
  - Racial or ethnic origin; political opinions; religious or philosophical beliefs;
  - Genetic data; biometric data (where processed to uniquely identify someone).
- Nonpersonal information (data elements that identify individual removed)
  - Anonymized data or aggregated data
- Pseudonymized data (not fully anonymous)
  - Process that detaches the aspects of the information attributed to the specific individual (*e.g.,* replace name of individual with artificial identifier -- a token)

Privacy and Data Protection Introduction

- **Comprehensive/Omnibus Law**
  - EU – General Data Protection Regulation (GDPR)
  - Brazil – General Data Privacy Law
  - India -- Personal Data Protection Bill
  - Japan - Act on the Protection of Personal Information (APPI)
- **Sectoral/Industry-Specific Law**
  - US – No single, comprehensive federal law regulating the collection and use of personal data – patchwork system of federal and state laws and regulations
    - Federal agencies that regulate privacy:
      - Federal Trade Commission (FTC)
      - Federal banking regulatory authorities
      - Federal Communications Comm (FCC)
      - Dept. of Health and Human Services
      - Dept. of Commerce
      - Dept. of Transportation (DOT)
    - States – Attorneys General

Privacy and Data Protection Introduction

- **Co-regulatory**
  - Combination of law and self-regulation codes of conduct and behavior
  - Australia – National Privacy Principles
- **Few/No general laws**
  - Cuba
  - China (but has now has enacted new national standard on personal information protection)

DATA PRIVACY LAWS, RULES, AND REGULATIONS

Data Privacy Laws, Rules, and Regulations

- EU – General Data Protection Regulation (GDPR)
  - Took effect on May 25, 2018
- - e Privacy Regulation (ePR)
  - Expected to take effect 2019
- US – California Consumer Privacy Act (CaCPA)
  - Signed into law June 28, 2018 - Set to take effect Jan 2020
    - California Senate Bill 327 – “Security of Connected Devices”
  - Signed into law Sept 28, 2018 - Set to take effect Jan 2020

Data Privacy Laws, Rules, and Regulations

- Brazil – General Data Privacy Law (GDPL)
  - Signed into law Aug 14, 2018 - Set to take effect Feb 2020

- India -- Personal Data Protection Bill
  - Released draft July 27, 2018 – Comments period

- Japan -- Japanese Act On The Protection Of Personal Information (APPI)
  - Amendments to APPI came into full force May 30, 2017

EU - GENERAL DATA PROTECTION REGULATION (GDPR)

General Data Protection Regulation (GDPR)

- EU regulation that protects:
  - Processing of personal data
  - Free movement of personal data
  - Fundamental rights and freedoms of persons
- Applies to:
  - Controllers and processors established in EU, regardless of where processing takes place
  - Controllers and processors not in EU where activities are:
    - Offering goods or services in EU
    - Monitoring behavior of data subject within EU

General Data Protection Regulation (GDPR)

- What organizations (controllers/processors) have to do:
  - Implement “Privacy by Default” and “Privacy by Design”
  - Maintain appropriate data security
  - Appoint a Data Protection Officer (DPO) (process lots of data or particularly sensitive data)
  - Conduct Data Protection Impact Assessments (DPIA) on new processing activities
  - Data breach reporting (to regulators and data subjects)
  - Get appropriate consent for most personal data collection and provide notification of personal data processing activities

General Data Protection Regulation (GDPR)

- What organizations (controllers/processors) have to do:
  - Keep records of all processing of personal information
  - Take responsibility for the security and processing activities of third-party vendors
  - Institute safeguards for cross-border data transfers
  - Consult with regulators before certain processing activities
  - Be able to demonstrate compliance on demand
  - Provide appropriate data protection training to personnel

General Data Protection Regulation (GDPR)

- What consumers (data subjects) can do:
  - Request personal data be erased and no longer processed (erasure)
  - Request removal of personal data (extends beyond controller records) (right to be forgotten)
  - Request a copy of all of their data and purpose of processing (access)
  - Request transfer of all of their data to a different organization (data portability)
  - Object to automated decision-making processes, including profiling
  - Request correction of personal data (rectification)
  - Request restriction on processing

General Data Protection Regulation (GDPR)

- What regulators (supervisory authorities) can do:
  - Ask for records of processing activities and proof of steps taken to comply with the GDPR
  - Impose temporary data processing bans, require data breach notification, or order erasure of personal data
  - Suspend cross-border data flows
  - Enforce penalties of up to 20 million Euro or 4 percent of annual revenues for non-compliance

US - CALIFORNIA CONSUMER PRIVACY ACT (CaCPA)

California Consumer Privacy Act (CaCPA)

- Landmark privacy bill that is being compared to GDPR:
  - Overarching approach and strong privacy protections
  - Potential impact on businesses around the World

- Already lots of amendments to address concerns voiced by industry and consumer groups

California Consumer Privacy Act (CaCPA)

- Applies to Covered businesses -- any for-profit entity that either:
  - Does $25 million in annual revenue;
  - Holds the personal data of 50,000 people, households, or devices *(e.g.,* website visitors)*;* or
  - Makes at least half of its revenue from the sale of PI (broadly defined)

- Protects individuals -- any "consumer" -- a natural person who is a California resident:
  - (1) every individual who is in the State for other than a temporary or transitory purpose, and
  - (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose.

California Consumer Privacy Act (CaCPA)

- What covered businesses will have to do:
  - Provide certain disclosures to consumers, such as categories of PI collected, purpose for collection, description of consumers' rights and online privacy policy
  - Provide at least two methods for receiving consumer requests (*e.g.,* toll-free number and website address)
  - Have a verification process so consumers can prove they are who they say they are when attempting to exercise their rights
  - Upon receiving a data access request, provide the information free-of-charge, within 45 days and in a portable format if delivered electronically
  - Include a special "Do Not Sell My Personal Information" button on their web sites to make it easy for consumers to object to the sale of their PI and disclose to consumers to whom their data is sold

California Consumer Privacy Act (CaCPA)

- What covered businesses will have to do:
  - Cannot "discriminate against a consumer" based on the exercising of any of the rights granted in the bill *(e.g., cannot* provide a different level or quality of service based on a consumer objecting to the sale of their data -- could offer higher tiers of service or product in exchange for more data as long as not "unjust" or "usurious")
  - Train certain employees on consumer rights pursuant to the law

California Consumer Privacy Act (CaCPA)

- What consumers can do:
  - Request a record of:
    - Types of PI an organization holds about the requester
    - Its sources and the specific PI that has been collected
    - Information about the use of data in terms of both business use and third-party sharing
  - Full right to erasure
    - Deletion of PI (with exceptions for completion of a transaction, research, free speech, and some internal analytical use)
    - Disclosure of this right to consumers
  - Opt-out option
    - Consumers can opt out of having their data sold to third parties

California Consumer Privacy Act (CCPA)

- What regulators can do/enforcement:
  - Enforced by State (CA) Attorney General
    - $7500 fine per violation (*e.g.,* could be per record in the database) not addressed within 30 days
  - Right to private action
    - For unauthorized access to a consumer's "nonencrypted or nonredacted personal information"
    - Can sue for $100-$750 per violation

US – CALIFORNIA SENATE BILL 327 -- “SECURITY OF CONNECTED DEVICES”

CA Senate Bill 327 -- “Security of Connected Devices”

- Specifies the security obligations of “manufacturers” of “connected devices”
  - “manufacturers” means “the person who manufactures, or contracts with another person to manufacture on the person’s behalf, connected devices that are sold or offered for sale in California.”
  - “connected device” means “any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.”

CA Senate Bill 327 -- “Security of Connected Devices”

- Covered manufacturers must equip the connected device with a reasonable security feature or features that are all of the following:
  - (1) Appropriate to the nature and function of the device.
  - (2) Appropriate to the information it may collect, contain, or transmit.
  - (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.
- If a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:
  - (1) The preprogrammed password is unique to each device manufactured.
  - (2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

CURRENT LEGAL LANDSCAPE FOR IOT AND IOS TECHNOLOGIES

Legal Landscape for IOT/IOS Technologies

- **US**
  - FTC focusing on data privacy and protection, and becoming increasingly aggressive in launching investigations and initiating enforcement proceedings
    - Including targeting IOT technology
  - Expect more States to pass laws directed specifically to privacy and data protection for IoT devices
  - US government agencies (*e.g.*, NIST, FTC, DHS, GAO, NTIA, NHTSA) and industry groups (*e.g.*, CTIA, GSMA, ISO) have issued guidelines and recommendations for best practices
  - Expect some companies to self-regulate by agreeing to comply with guidelines and recommendations

Legal Landscape for IOT/IOS Technologies

- **EU**
  - European regulators (Supervisory Authority) intensifying GDPR enforcement – serving enforcement notices and issuing fines in UK, Ireland, Germany, Austria, Portugal, Italy, and France
  - ePrivacy Regulation (ePR) is a complement to GDPR and focuses on the confidentiality and privacy of electronic communications
  - UK gov't issued *Proposed Code of Practice for Consumer IOT Products and Associated Services* -- expect other countries and industry associations to issue similar guidelines and recommendations for best practices
  - Expect some companies to pledge to comply with the proposed code and similar guidelines that are issued by governments and industry groups

Legal Landscape for IOT/IOS Technologies

- **US**
  - Laws, Rules, and Regulations specifically directed to IOT/IOS
    - California Senate Bill 327 – “Security of Connected Devices” (2018)
    - Developing Innovation and Growing the Internet of Things (“DIGIT”) Act (2017)
    - Internet of Things Cybersecurity Improvement Act of 2017
    - Securing the IoT Act of 2017
    - Cyber Shield Act of 2017
    - The IOT Consumer Tips to Improve Personal Security Act of 2017
  - Enforcement Actions -- Federal Trade Commission
  - Enforcement Actions – US Courts

Legal Landscape for IOT/IOS Technologies

- Federal Trade Commission Enforcement Actions
  - "When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.

See Federal Trade Commission, Privacy and Security Enforcement, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement

Legal Landscape for IOT/IOS Technologies

- Federal Trade Commission Enforcement Actions
  - Enforcement actions FTC has taken against manufacturers of systems/devices:
    - ***TRENDnet*** - in 2013, the FTC alleged that TRENDnet's SecureView cameras (IOT) were marketed as "secure" when in fact the cameras had faulty software that left them open to online viewing, and sometimes listening, by anyone with the camera's internet address.
    - Issued consent order – prohibiting TRENDnet is from misrepresenting the security of its cameras, or the security, privacy, confidentiality, or integrity of the information that its cameras or other devices transmit; barring TRENDnet from misrepresenting the extent to which a consumer can control the security of the information the cameras store, capture, access, or transmit; and TRENDnet also agreed to establish and maintain a comprehensive security program subject to independent audits for the next 20 years.

Legal Landscape for IOT/IOS Technologies

- Federal Trade Commission Enforcement Actions
  - Enforcement actions FTC has taken against manufacturers of systems/devices:
    - ***ASUSTek*** – 2016 - settled charges based on critical security flaws in its routers and that the routers' insecure cloud services led to the compromise of thousands of consumers' connected storage devices, thereby exposing consumers' sensitive personal information on the internet - accused of not taking reasonable steps to secure the software on its routers because: (i) hackers were able to exploit pervasive security bugs in the routers' web-based control panel to chance the router's security settings without the consumer's knowledge, (ii) users could retain the same default login credentials on every router: username "admin" and password "admin;" (iii) hackers could bypass the AiCloud services login screen and gain access to a consumer's connected storage device without any credentials simply by accessing a specific URL from a web browser; (iv) the AiDisk service did not encrypt the consumer's files in transit, and (v) the default privacy settings provide public access to the consumer's storage device to anyone on the internet.

Legal Landscape for IOT/IOS Technologies

- Federal Trade Commission Enforcement Actions
  - Enforcement actions FTC has taken against manufacturers of systems/devices:
    - ***VIZIO*** - February 2017 - agreed to pay $2.2 million to settle charges by the FTC and the office of the New Jersey Attorney General that it installed software on its TVs to collect viewing data on 11 million consumer TVs without consumers' knowledge or consent.
    - ***Lenovo*** - September 2017 - settled charges by the FTC and 32 State Attorneys General that the company harmed consumers by pre-loading software on some laptops that compromised security protections in order to deliver ads to consumers.
    - ***BLU Products*** - April 2018 - settled with the FTC over allegations that the company allowed a China-based third-party service provider to collect detailed personal information about consumers, such as text message contents and real-time location information, without consumers' knowledge or consent despite promises by the company that it would keep such information secure and private.

Legal Landscape for IOT/IOS Technologies

- Federal Trade Commission Enforcement Actions
  - **D-Link**:
    - *Jan. 2017* – FTC sued D-Link in US Federal District Court in the N.D. of CA for engaging in unfair or deceptive acts in violation of Section 5 of the FTC Act in connection with D-Link's failure to take reasonable steps to secure its routers and Internet-protocol cameras from widely known and reasonably foreseeable security risks. The FTC's complaint focused on D-Link's marketing practices, noting that D-Link's marketing materials and user manuals included statements in bold, italicized, all-capitalized text that D-Link's routers were "easy to secure" with "advanced network security." D-Link also promoted the security of its IP cameras in its marketing materials, specifically referencing the device's security in large capital letters. In addition, the IP camera packaging also listed security claims, such as "secure-connection" next to a lock icon as one of the product features.

Legal Landscape for IOT/IOS Technologies

- Federal Trade Commission Enforcement Actions
  - **D-Link**:
    - *Mar. 2017* – D-Link challenged the FTC's authority to regulate data security for IoT companies as an unfair practice under Section 5 of the FTC Act, and sought to dismiss claims against D-Link because the FTC failed to to provide any facts establishing actual harm to consumers.
    - *Case still pending*… was set to go to a bench trial Jan.14, 2019, but on hold as a result of the US Gov't shutdown…

Legal Landscape for IOT/IOS Technologies

- **EU**
  - General Data Protection Regulation (GDPR)
  - ePrivacy Regulation (ePR)
  - European Union Agency for Network and Information Security (ENISA) – “Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures” (Nov. 2017)
  - UK Gov’t – “Proposed Code of Practice for Security in Consumer IoT Products and Associated Services” (Mar. 2018)
  - UK Gov’t Dept. for Digital, Culture, Media & Sport – “Secure by Design: Improving the cyber security of consumer Internet of Things Report” (2018)
  - UK Gov’t Dept. for Digital, Culture, Media & Sport – “Code of Practice for Consumer IoT Security” (2018)

- Legal Landscape for IOT/IOS Technologies
- **Space** - Possible regime for applicability of privacy and data protection laws for Space-Based communications products and services
  - International Space Law -- Outer Space Treaty
  - Regional (EU) and National (US, Canada, Brazil, etc.) Laws

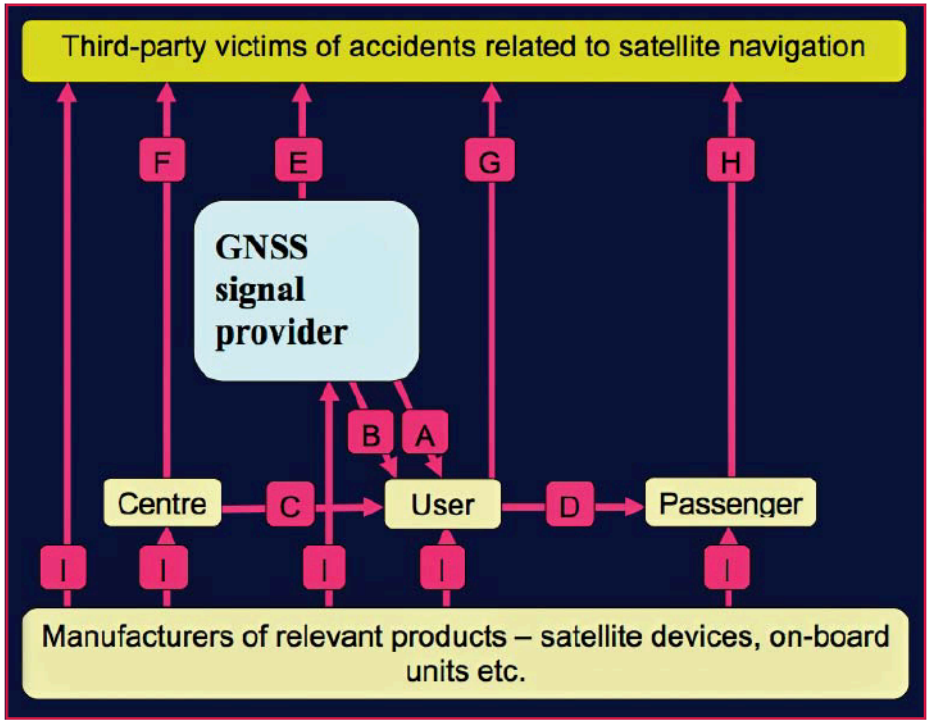


Figure 1: The Galileo Legal/Functional Model and liability in a multi-model context
Legend: A = No (or tort?) liability; B = Contractual liability (possibly including onward liability handling); C = contractual liability (normally, except for aviation); D = contractual liability (unless overruled by tort liability / national or international law imposing liability regime); E = International third-party liability; F = No (? or tort?) liability; G = Third-party liability (usually national, sometimes international); H = No liability (normally); I = Product liability as applicable (national or EU law)

Frans G. von der Dunk, "*Legal Aspects of Navigation: The Cases for Privacy and Liability: An Introduction for Non-lawyers,*" University of Nebraska - Lincoln DigitalCommons@University of Nebraska – Lincoln - Space, Cyber, and Telecommunications Law Program Faculty Publications, 5-2015

- Legal Landscape for IOT/IOS Technologies
- **Space** – Considerations for applicability of privacy and data protection laws to Space-Based communications products and services:
  - Region's/Country's Airspace
  - Launching country
  - Operating country
  - Where entity/business (*e.g.,* controller, processor, etc.) is established
  - Where activities were put into use
  - Citizenship of data subject/consumer whose PI is collected, used, retained

BEST PRACTICES AND COMPLIANCE PROGRAMS

Best Practices And Compliance Programs

- Recognition/understanding of importance of privacy across entire organization – concepts of “privacy by design” & “privacy by default”
- Development /implementation of privacy program
- Development of incident response program

Best Practices And Compliance Programs

- Conduct privacy assessment:
  - Privacy Impact Assessment (PIA)
  - Privacy Threshold Assessment (PTA)
- Evaluate/assess necessity of data collected, retention and disposal
- Data classification -- inventory of PI collected/used/stored/disclosed, classification, and segregate
- Evaluate/revise privacy notices and website functionality (consumer preferences (opt-in/opt-out), access, and correction)
- Communicate and conduct training in the organization's privacy policy

Best Practices And Compliance Programs

- Key considerations to address for demonstrating that "reasonable" privacy and data protection measures have been established and practiced

UNCTAD, "*Data protection regulations and international data flows: Implications for trade and development*." (2016)

ROTHWELL FIGG
IP Professionals

Best Practices And Compliance Programs

➢ Recommendations for companies developing IoT devices:

- ✓ build security into devices at the outset, rather than as an afterthought in the design process;
- ✓ train employees about the importance of security, and ensure that security is managed at an appropriate level in the organization;
- ✓ ensure that when outside service providers are hired, that those providers are capable of maintaining reasonable security, and provide reasonable oversight of the providers;

UNCTAD, "*Data protection regulations and international data flows: Implications for trade and development*." (2016)

Best Practices And Compliance Programs

➢ Recommendations for companies developing IoT devices:

- ✓ when a security risk is identified, consider a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk;
- ✓ consider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;
- ✓ monitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks.

UNCTAD, "*Data protection regulations and international data flows: Implications for trade and development*." (2016)

Best Practices And Compliance Programs

➢ Recommendations for companies developing IoT devices:

- ✓ Consider data minimization and limit the collection of consumer data, and retain that data for only a set period of time. Do not collect personal information you do not need;
- ✓ Hold on to information only as long as you have a legitimate business need;
- ✓ Notify consumers and give them choices about the security of their data and how their information will be used. Consider setting default settings at most protective levels;

Best Practices And Compliance Programs

➢ Recommendations for companies developing IoT devices:

- ✓ Control access to sensitive information. Store sensitive personal information securely and protect it during transmission;
- ✓ Require secure passwords and authentication;
- ✓ Use industry-tested and accepted methods;
- ✓ Update and patch third-party software

ROTHWELL FIGG
IP Professionals

Thank you!

Martin M. Zoltick, CIPP/US
mzoltick@rfem.com

607 14th Street, NW Suite 800 | Washington, DC 20005

202-783-6040 | www.rfem.com