Feeling Insecure? What the IoT Community Needs to Know to Navigate the Evolving Legal and Regulatory Landscape Requiring "Reasonable Security" Features for IoT and Connected Devices

IEEE IoT Vertical and Topical Summit at RWW2021

January 13, 2021

Martin M. Zoltick, CIPP/US

Rothwell, Figg, Ernst & Manbeck, PC

Privacy
Data Protection
Cybersecurity

Agenda

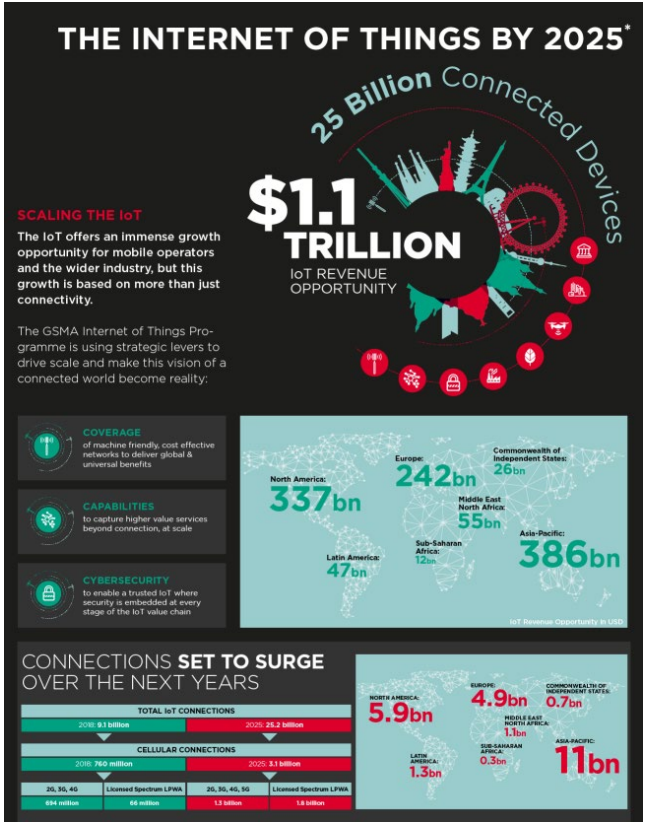
IoT and Connected Devices Technology Use Cases

Legal and Regulatory Framework Surrounding IoT and Connected Devices Technologies

Best Practices – Building a Compliance Program and Framework for Risk Management

ROTHWELL FIGG
IP Professionals

IoT Devices and Data Generated and Transmitted



Massive growth in the number of IoT devices deployed and in use, coupled with use of AI-enabled technologies (AIoT), presents new/complex challenges from legal and regulatory perspective

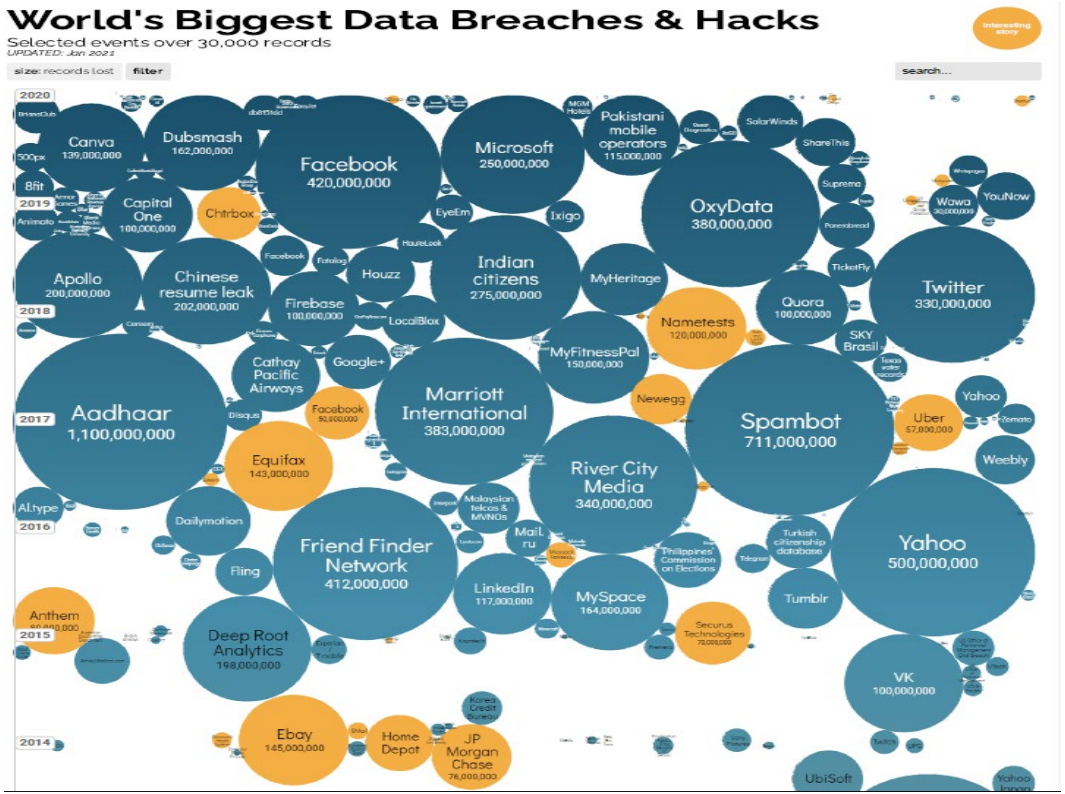
Vast amounts of data, including personal data, being generated, collected, transmitted, stored, and processed creates major challenges from the standpoint of security, privacy, and data protection

Regulators, policymakers, and the public at large have taken notice of IoT devices and AI-enabled technologies

Source: https://www.gsma.com/iot/resources/the-gsma-iot-infographic

ROTHWELL FIGG
IP Professionals

Rise in the Number of High Profile Data Breaches



- Increasing lack of trust – collection, use, protection of data
- Concerns regarding security vulnerabilities, automated-decision making, limited user interface, integration into IS and infrastructure
- Driving increased focus - policymakers/govt, public and private sector businesses, individuals/society-at-large

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

IoT and Connected DevicesTechnology Use Cases

Internet of Things (IoT) & Connected Devices – Use Cases

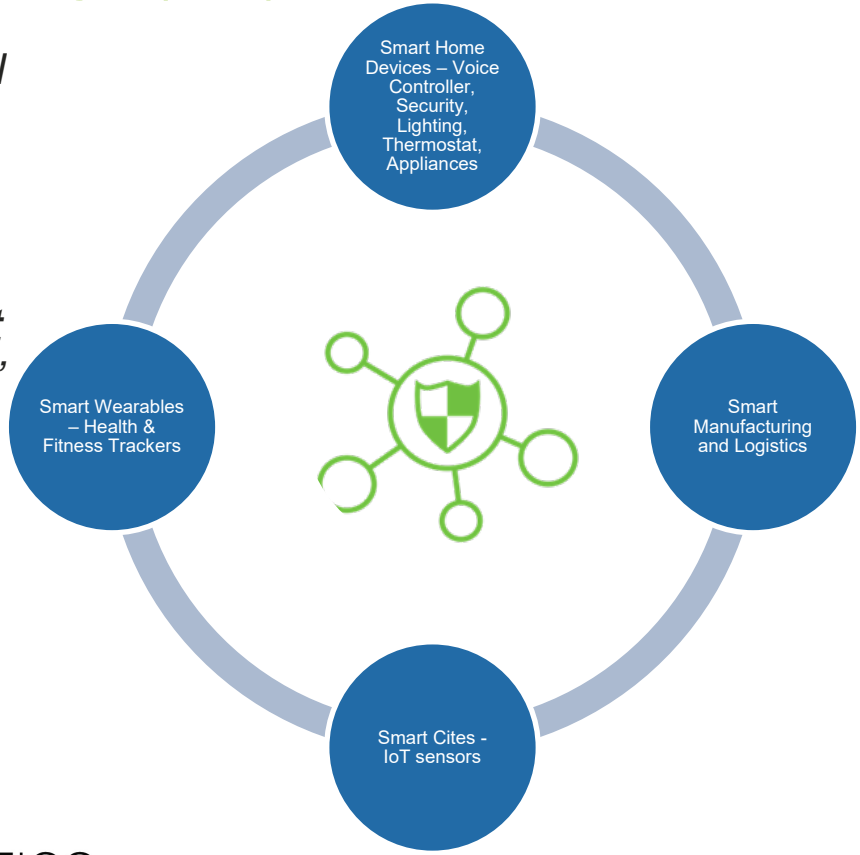
- *"Internet of Things devices are devices that--*

> *(A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and*
>
> *(B) can function on their own and are not only able to function when acting as a component of another device, such as a processor*

Internet of Things Cybersecurity Improvement Act of 2020 (Dec 2020)

Internet of Things (IoT) & Connected Devices – Use Cases

- *"a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making"*



- IoT devices
- IoT device management
- IoT device connectivity and networking
- IoT device security

ROTHWELL FIGG
IP Professionals

Internet of Things (IoT) & Connected Devices – Use Cases

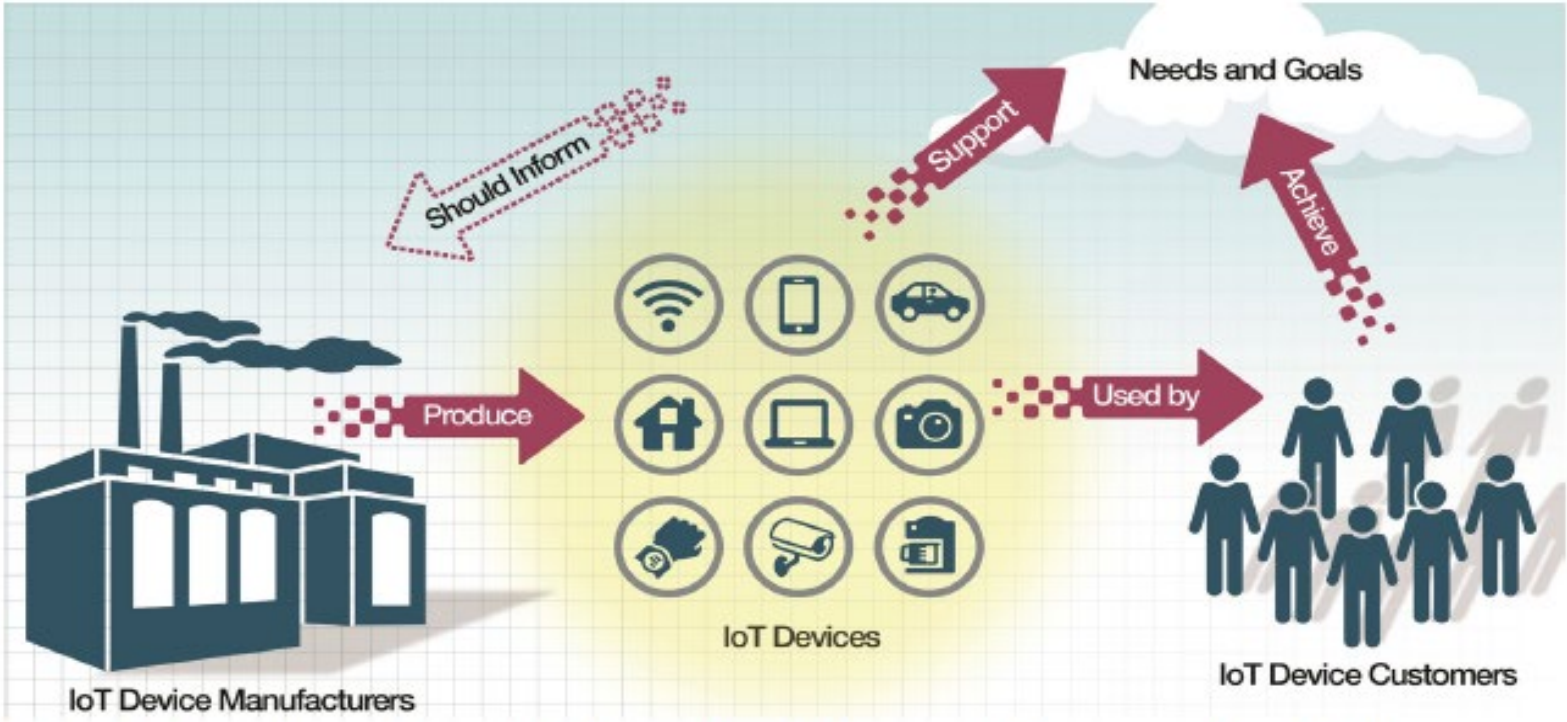


Figure 2: Connections Between IoT Device Manufacturers and Customers Around Cybersecurity

Legal and Regulatory Framework Surrounding IoT and Connected Devices Technologies

Privacy Considerations – “Reasonable” Security Features

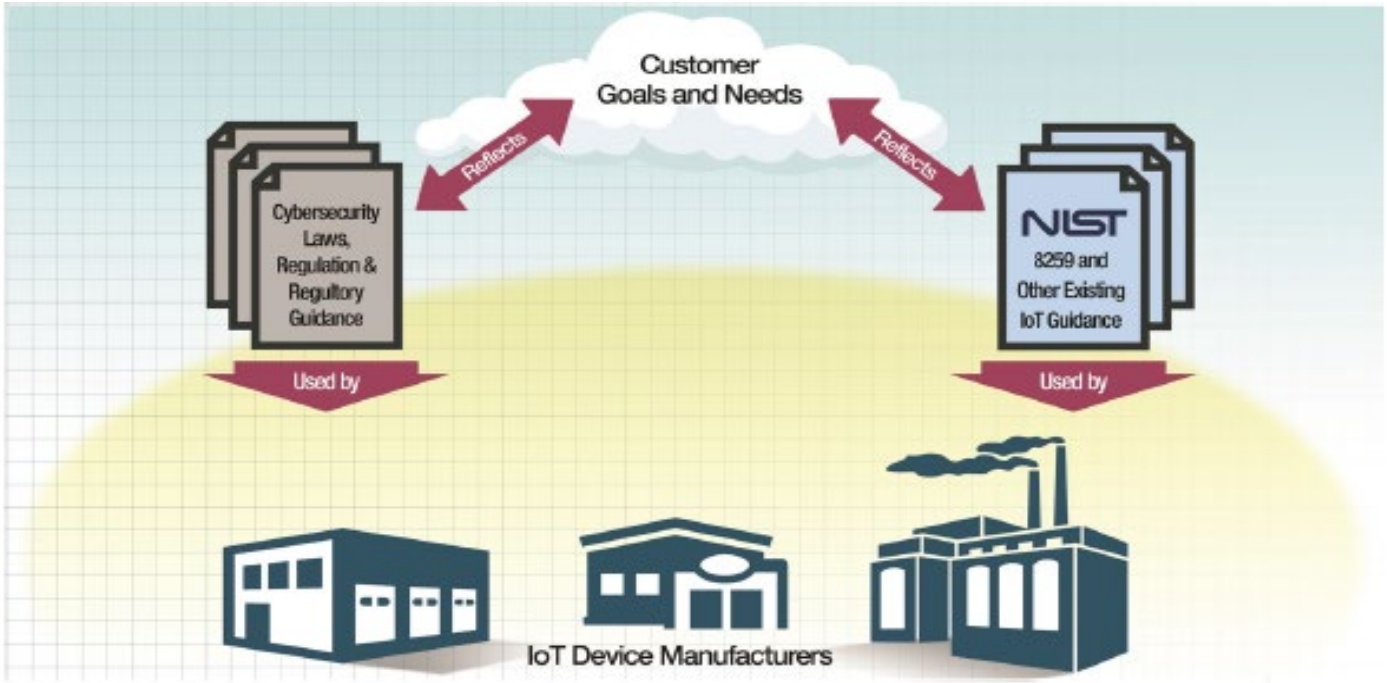


Figure 3: Customer Cybersecurity Needs and Goals Reflected in and Informed by Many Applicable Regulations and Guidance Documents

Privacy Considerations – “Reasonable” Security Features

US

- Internet of Things Cybersecurity Improvement Act of 2020 (Dec 2020)
- National Institute of Standard and Technology (NIST)
  - Workshop Summary Report for “Building the Federal Profile for IoT Device Cybersecurity” Virtual Workshop (Jan 2021)
  - IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (DRAFT NISTSP 800-213) (Dec 2020)
  - IoT Non-Technical Supporting Capability Core Baseline (DRAFT NISTR 8259B) (Dec 2020)
  - Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline (DRAFT NISTR 8259C) (Dec 2020)
  - Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government (Draft NISTIR 8259D) (Dec 2020)
  - Foundational Cybersecurity Activities for IoT Device Manufacturers (NISTIR 8259) (May 2020)
  - IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A) (May 2020)

Privacy Considerations – “Reasonable” Security Features

US

- California Senate Bill 327 – “Security of Connected Devices” (Effective Jan 2020)
- Oregon House Bill 2395 – “Relating to security measures required for devices that connect to the Internet” (Effective Jan 2020)
- Similar legislation currently under consideration in Illinois, Kentucky, Maryland, Massachusetts, New York, Rhode Island, Vermont, and Virginia
- Comprehensive State Privacy Laws (i.e., California (CCPA), Maine, Nevada)
- Industry groups (*e.g.*, CTIA, GSMA, ISO) issuing guidelines and recommendations for best practices
- Companies self-regulating by agreeing to comply with guidelines and recommendations

Privacy Considerations – “Reasonable” Security Features

EU

- Council of the EU Conclusions on the Cybersecurity of Connected Devices (Dec 2020)
- EU Cybersecurity Act (Jun 2019)
- European Union Agency for cybersecurity (ENISA) mandate (Jun 2019)
- European cybersecurity certification framework (Jun 2019)
- ENISA Good Practices for Security of IoT
- ENISA Good practices for IoT and Smart Infrastructures Tool
- ENISA Baseline Security Recommendations for IoT
- Comprehensive Privacy Laws (i.e., GDPR, ePrivacy Regulation)

Privacy Considerations – “Reasonable” Security Features

UK

- UK Department for Digital, Culture, Media & Sport Policy paper - Proposals for regulating consumer smart product cyber security - call for views (Updated Oct 2020)
- UK Code of Practice for consumer IoT security (Published Oct 2018)
- Comprehensive Privacy Laws (i.e., UK GDPR)

Privacy and Data Protection

Privacy and Data Protection

- What is *Information Privacy*?
  - The “appropriate” use of personal information under the circumstances
  - An individual’s right to determine how his or her personally identifiable information is used
  - An individual’s right to control the collection, use, processing, storage, disclosure, sale, and retention/deletion of personal information; to notice, choice and consent, and access; and to limit that information from becoming publicly available
- What is *Data Protection*?
  - Handling, storing, and managing of personal information
  - 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

- 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

- CCPA refers to "Personal Information"
  - information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular Consumer or household, including (but not limited to):
    - Personal Identifiers (*e.g.*, name, postal address, email address, online IP address, social security number);
    - Internet or other electronic network activity information; and
    - Employment, educational, and commercial information.

Privacy and Data Protection

- 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)

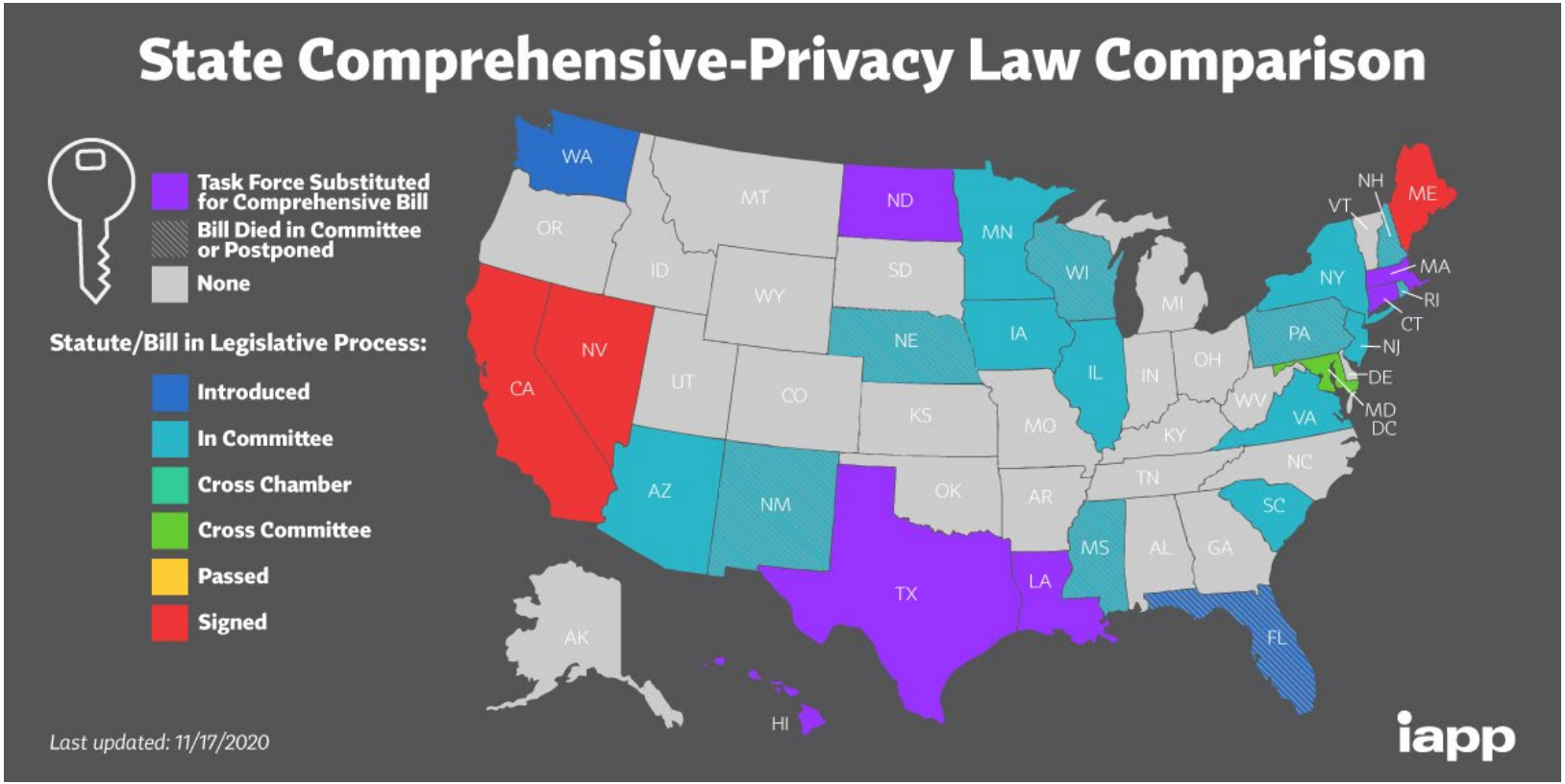
Privacy and Data Protection

- 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 Commerce
      - Dept. of Transportation (DOT)
    - States – Attorneys General
- Co-regulatory – Few/No Laws

General Privacy Laws and Regulations - US

- **California Consumer Privacy Act (CCPA)**
  - Signed into law June 28, 2018 – Took effect Jan 2020
- **Maine – Act to Protect the Privacy of Online Consumer Information**
  - Signed into law June 6, 2019 – Took effect July 2020
- **Nevada – Senate Bill 220 (SB 220) - Nevada Privacy of Information Collected on the Internet from Consumers Act (NPICICA)**
  - Signed into law May 29, 2019 – Took effect Oct 2019
- **IAPP State Comprehensive Privacy Law Comparison (2020-11-17)**

General Privacy Laws and Regulations - US



IoT and Connected Devices Specific Laws and Regulations

IoT & Connected Devices Specific Laws and Regulations - US

- **IoT Cybersecurity Improvement Act (Dec 2020)**
  - "To establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes."
  - Requires the development, adoption and implementation of security standards for IoT devices by the federal government
  - Requires security standards and guidelines to be published by the National Institute of Standards and Technology (NIST) by March 4, 2021
  - Directs NIST to ensure the consistency of its publication pursuant to the Act with its existing guidance regarding IoT vulnerabilities and considerations about how they should be managed, including in the domains of secure development, identity management, patching and configuration management.
  - NIST standards and guidelines will then be incorporated into federal government information security policies and principles as well as Federal Acquisition Regulations by September 4, 2021

IoT & Connected Devices Specific Laws and Regulations - US

- **IoT Cybersecurity Improvement Act (Dec 2020)**
  - Requires guidelines on IoT vulnerability information sharing and resolution for IoT devices owned or controlled by an agency to be published by NIST by September 4, 2021
  - Requires guidelines for government contractors providing IoT systems and any subcontractor thereof at any tier providing such information system to such contractor to be published by NIST by September 4, 2021
  - Subject to limited exceptions, government agencies are prohibited from buying or using IoT devices that do not comply with the NIST standards and guidelines
  - Act requires contractors providing IoT devices to the U.S. government to adopt coordinated vulnerability disclosure policies, so that if a vulnerability is uncovered, that information is disseminated

IoT & Connected Devices Specific Laws and Regulations - US

- **National Institute of Standards and Technology (NIST)**
  - Released draft guidance on IoT device cybersecurity - recommendations to federal agencies and manufacturers concerning effective cybersecurity (Dec 2020)
    - IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (DRAFT NISTSP 800-213)
    - IoT Non-Technical Supporting Capability Core Baseline (DRAFT NISTR 8259B)
    - Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline (DRAFT NISTR 8259C)
    - Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government (Draft NISTIR 8259D)
  - Workshop Summary Report for “Building the Federal Profile for IoT Device Cybersecurity” Virtual Workshop (Jan 2021)

IoT & Connected Devices Specific Laws and Regulations - US

- **National Institute of Standards and Technology (NIST)**
  - Workshop Summary Report for “Building the Federal Profile for IoT Device Cybersecurity” Virtual Workshop (Jan 2021)
    - *The mission of the NIST Cybersecurity for the Internet of Things (IoT) program is to cultivate trust in the IoT and foster an environment that enables innovation on a global scale through standards, guidance, and related tools. The Cybersecurity for IoT program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.*

IoT & Connected Devices Specific Laws and Regulations - US

- **National Institute of Standards and Technology (NIST)**
  - Core Baseline - list of six recommended security features that manufacturers can build into IoT devices, and that consumers can look for on a device's box or online description while shopping:
    - Device Identification: The IoT device should have a way to identify itself, such as a serial number and/or a unique address used when connecting to networks
    - Device Configuration: Similarly, an authorized user should be able to change the device's software and firmware configuration. For example, many IoT devices have a way to change their functionality or manage security features
    - Data Protection: It should be clear how the IoT device protects the data that it stores and sends over the network from unauthorized access and modification. For example, some devices use encryption to obscure the data held on the internal storage of the device

IoT & Connected Devices Specific Laws and Regulations - US

- **National Institute of Standards and Technology (NIST)**
  - Core Baseline - list of six recommended security features that manufacturers can build into IoT devices, and that consumers can look for on a device's box or online description while shopping:
    - Logical Access to Interfaces: The device should limit access to its local and network interfaces. For example, the IoT device and its supporting software should gather and authenticate the identity of users attempting to access the device, such as through a username and password
    - Software and Firmware Update: A device's software and firmware should be updatable using a secure and configurable mechanism. For example, some IoT devices receive automatic updates from the manufacturer, requiring little to no work from the user
    - Cybersecurity Event Logging: IoT devices should log cybersecurity events and make the logs accessible to the owner or manufacturer. These logs can help users and developers identify vulnerabilities in devices to secure or fix them

IoT & Connected Devices Specific Laws and Regulations - US

- **Internet of Things and Connected Devices**
  - California Senate Bill 327 – “Security of Connected Devices” (Effective Jan 2020)
  - Oregon House Bill 2395 – “Relating to security measures required for devices that connect to the Internet” (Effective Jan 2020)
  - Illinois, Kentucky, Maryland, Massachusetts, New York, Rhode Island, Vermont, and Virginia currently considering similar legislation

United States – 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.”

United States – 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.

United States – CA Senate Bill 327 “Security of Connected Devices”

- 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.

United States – OR House Bill 2395 "Relating to security measures required for devices that connect to the internet"

- Similar to California's Security of Connected Devices law, including the same reasonable security features language

- Narrower definition of "connected device" as a device or other physical object that:
  - (A) Connects to the Internet and is used primarily for personal, family or household purposes; and
  - (B) Is assigned an Internet Protocol address or another address or number that identifies the connected device for the purpose of making a short-range wireless connection to another device.

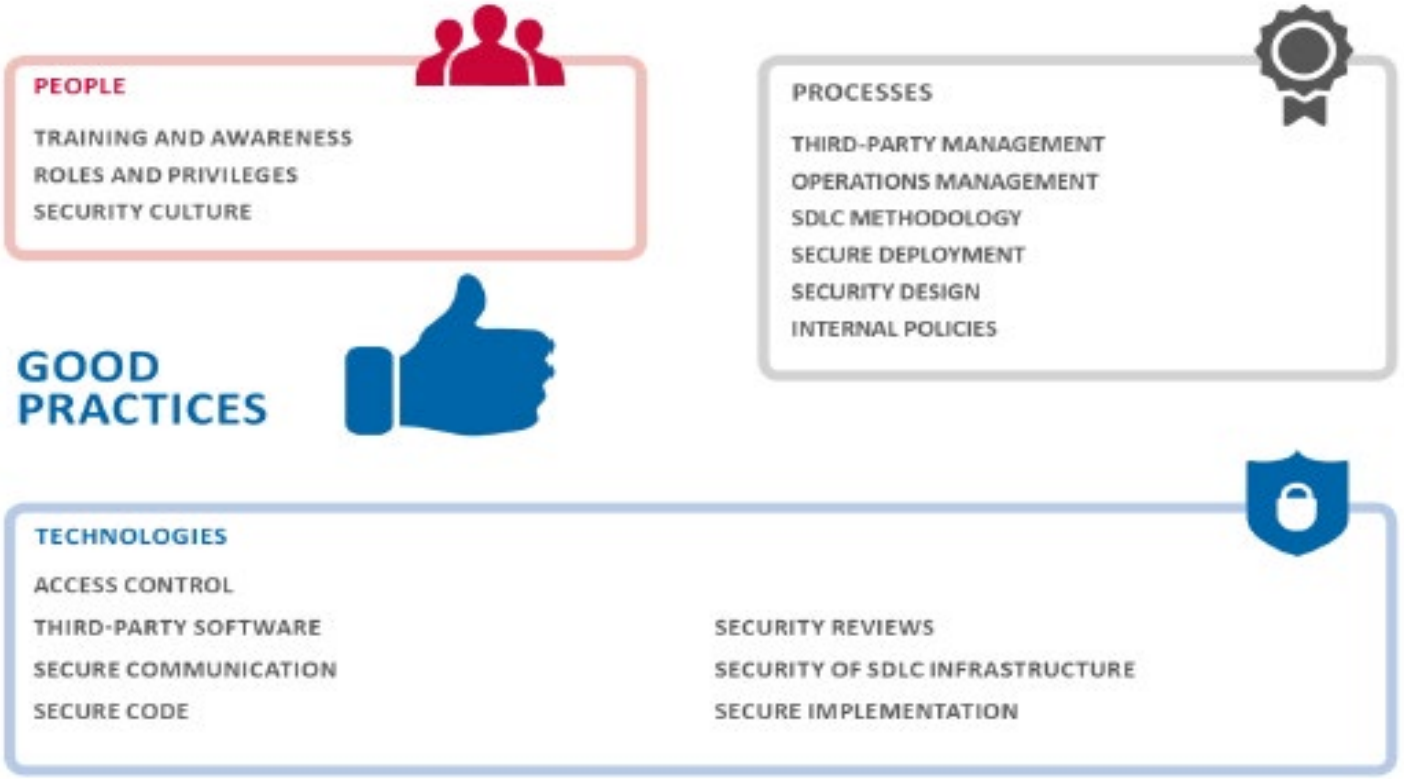
EU – Baseline Security Recommendations for IoT & Connected Devices

Phases	Security considerations	Description
Analysis and requirements	Security Requirements	Identification of security requirements according to data classification, business requirements and legislative or standardisation objectives.
	Hardware limitations	Alignment of security requirements with hardware limitations taking into consideration additional aspects resulting from software requirements.
	Protocols	Identification of the appropriate protocols for the solution, taking into account its security features and the IoT solution's security requirements.
	Threat modelling	Application of threat modelling methodologies to identify the software threats and the associated countermeasures to mitigate them.
Software design	Attack surface analysis	Identification of the IoT solution's attack surface by taking into consideration architecture aspects and utilising security user stories.
	Secure design	Use / application of secure design patterns and principles. Security architectures determine when and where to apply them.
Development / Implementation	Frameworks	Use of known security guidelines to ease the implementation of security controls during the software development process in order to enhance security throughout the software lifecycle.
	Libraries	Use of trusted security libraries when third-party resources are used, ensuring that they are widely tested based on certain security criteria so as to not compromise the software.
	Built-in Security	OS as well as communication protocols come with built-in security functions which can be leveraged to implement security features in applications.
	Guidelines	Use of the Secure Code guidelines and standards to alleviate from most common application layer vulnerabilities.
	External checks	Use of mechanisms to ensure that external libraries, tools or APIs used during the SDLC phases such as development, deployment and maintenance are proven, secure and updated.

EU – Baseline Security Recommendations for IoT & Connected Devices

Testing / Acceptance	Design review	Activities aimed at verifying that the design used follows the specifications defined during the design stage so that all security requirements are met
	Code verification	Review of the code/quality of the code, preferably using automated tools in order to look for errors introduced in the implementation phase.
	Security requirement tests	Performance of security tests to ensure that software is free of known vulnerabilities and to detect risks related to security requirements.
	Penetration tests	Testing to identify potential vulnerabilities that could exist in IoT solutions and could be exploited by an attacker.
Deployment / Integration	Hardening environment	Secure the environment adding protection layers as a part of the in-depth defence strategy in order to reduce the system's attack surface.
	Configuration and Vulnerability management	Use of the control activities to guarantee an artefact's quality, monitoring and controlling changes made during the development lifecycle, and identifying and repairing potential flaws affecting the software.
	Change management	Definition of the procedure to document, monitor and track all changes that may be made in the software development process
Maintenance / Disposal	Incident management	Procedure to address the steps to be taken in order to ensure a normal operation when a security issue takes place in the SDLC process.
	Management of the end of life-disposal	Secure management process of software components, artefacts and data once the IoT solution is going to be retired from production.
	Remote SW updates	Delivery management to push new versions of software in a remote environment securely when it is necessary to apply an update, either to add new functionalities or to mitigate vulnerabilities.

EU – Baseline Security Recommendations for IoT & Connected Devices



Best Practices – Building a Compliance Program and Framework for Risk Management

Best Practices/Framework for Risk Management - IoT & Connected Devices

- Review the regulatory landscape: Monitor IoT regulatory developments worldwide, including laws, industry standards, guidelines and enforcement cases
- Develop IoT review framework: Create a cross-functional data review board to get input from various stakeholders and demonstrate to regulators a thoughtful decision-making process
- Initiate a security assessment: Run an assessment to identify whether a new IoT product implicates any regulatory security requirements and incorporates appropriate security safeguards
- Privacy by Design: Engage with product team early and stay involved during the development lifecycle
- Continuous Compliance Monitoring

Compliance Strategy & Framework for Risk Management

- Develop and implement a compliance strategy and framework for risk management to establish best practices for legal/regulatory (*e.g.*, GDPR, CCPA, etc.) compliance

ROTHWELL FIGG
IP Professionals

Establish Governance Structure

- Company defines, documents, communicates, and assigns accountability for its privacy policies and procedures

Assign Ownership – establish ownership of risk for privacy program – buy-in from C-Suite/Level Execs

Establish Steering Committee – include reps from bus units most heavily impacted by privacy obligations

Define Roles and Decision-making – Define roles of privacy professionals (CPO, CISO, DPO)

Personal Data Inventory, Retention, & Transfer

- Key foundational step in establishing privacy compliance strategy and developing program is understanding what data (PI) is being managed

Best practice to create “data map” for understanding PI collected and tracking flow (*i.e.,* collection→use→processing→storage→ sale→deletion)

Document processes/procedures, incl sources of PI and how collected, location(s) PI stored, how PI used by bus, what PI retained, deleted, and transferred to TP

Implement and maintain reasonable data security practices and take appropriate measures for each point on the data map and understand potential vulnerabilities

Data Privacy Policies & Notices

- Company needs to develop privacy notices applicable to each type of data subject and internal privacy policies for the organization

Develop privacy notices or review existing ones to ensure/verify they meet each requirement of applicable privacy laws/regs (*e.g.,* GDPR, CCPA, APPI)

Develop internal privacy policies that establish accountability, roles, and responsibilities (*e.g.,* Enterprise-wide, Legal, Employee)

Review and update existing privacy notices (at least every 12 mo and as necessary) to conform with any changes to legal/reg reqts and bus practices

Individual Rights/Consumer Preference Management

- Organization needs to be prepared to manage requests from individuals to provide the type of PI collected, sold, or disclosed, to provide a copy of the PI, and to maintain and honor consent preferences

- Required to make available at least 2 (VCR) submission options (*e.g.,* through website, by toll-free telephone)
- Develop ID verification process to ensure PI being provided to correct person
- Develop standard data retrieval procedures, reporting formats, and tracking systems, and ensure PI transferred in secure manner
- Establish and maintain program to support consumer rights and preferences related to their PI (*e.g.,* consent, opt-in, opt-out, forgotten)

Vendor/Third Party Management

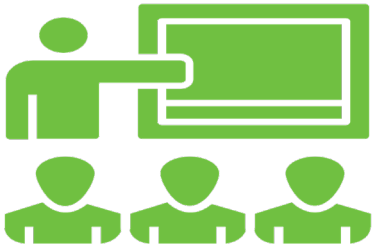
- Critical for organization to understand where PI is being shared with vendors, service providers, and other third parties, and establish oversight

Conduct detailed assessment to determine what PI is being shared with vendors, service providers, & other TPs

Track and document any disclosure of PI to a vendor, service provider, or other TP

Ensure written contract with vendor, service provider, or other TP limiting use of PI to conform with legal/regulatory requirements

Training & Awareness Program



- Everyone who handles PI, including decisionmakers, should receive training in organization's privacy programs and policies

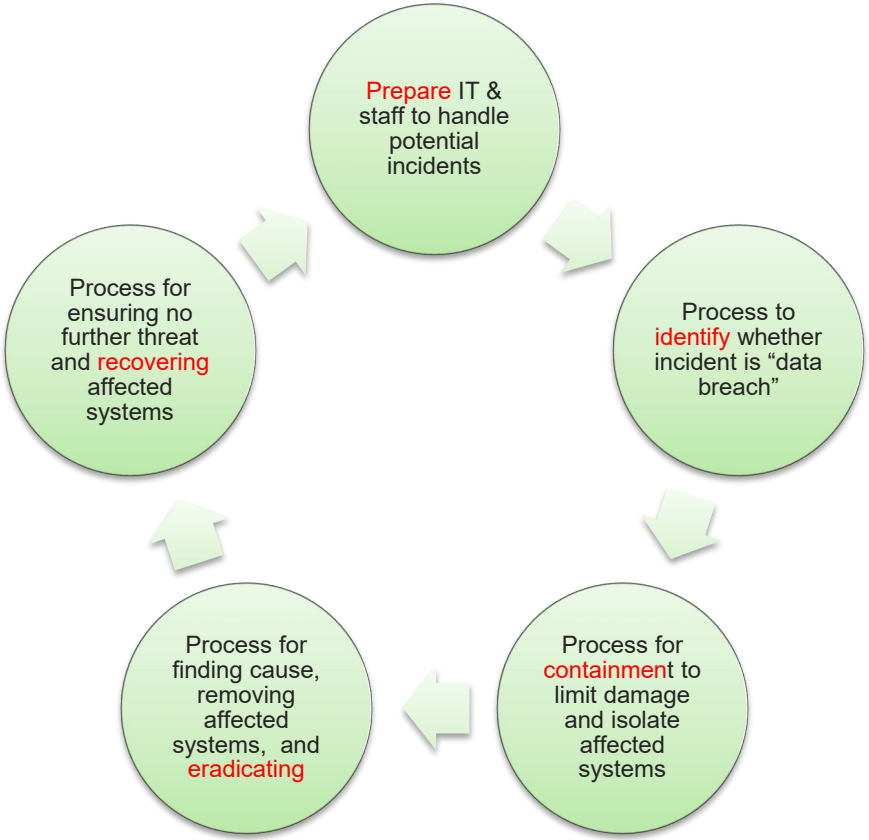
Documenting training and awareness program, providing training materials, maintaining records of training, providing scripts for cust svc reps

Organization will need to provide different training for different groups within organization and consider specific training based on types of PI handled

Training and awareness is an ongoing process and key to successful privacy program deployment and sustainability

Data Privacy Breach Management Program

- Company defines an organized approach to managing the occurrence and aftermath of a data privacy incident, security breach, or cyberattack



ROTHWELL FIGG
IP Professionals

Continuous Compliance Monitoring

- Company defines a compliance monitoring framework to support current and new operational practices, address future laws, and demonstrate ongoing compliance

Establish periodic reviews of compliance strategy and framework for risk management, updating data inventory/mapping, notices and policies

Seek to enhance framework and program by utilizing more automation, governance, risk & compliance (GRC) software/tools

Monitor compliance and incidents, revise policies and procedures as needed, and adapt based on new and changing laws/regulations

ROTHWELL FIGG
IP Professionals

Privacy
Data Protection
Cybersecurity

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

MARTIN M. ZOLTICK

- Technology lawyer with more than 30 years of experience, with degree in Computer Science and experience working as a software engineer
- Practice is focused primarily on intellectual property (IP) matters, transactions, and privacy, data protection, and cybersecurity
- Certified Information Privacy Professional in the United States (CIPP/US)
- Regularly counsels clients on understanding and navigating rapidly evolving area of privacy and data protection law
- Working with clients to prepare, integrate, and implement best practices for CCPA, other state's laws, and GDPR compliance
- Providing thought leadership on the application of data protection laws and industry/technology-specific data privacy and security considerations for IoT devices, biometric data, and in outer space

AREAS OF CONCENTRATION

- Counseling
- Privacy, Data Protection, and Cybersecurity
- Licensing and Transactions
- Litigation
- Patent Prosecution (Registered US PTO)
- Post-Grant Trial Practice

EDUCATION

- J.D., Catholic University of America, Columbus School of Law – 1989
- B.S., Computer Science, Northeastern University, College of Computer Science – 1985 (*cum laude)* Cybersecurity

Certified Information Privacy Professional/United States CIPP US iapp

iam 1000

Managing Intellectual Property IP STARS
THE GUIDE TO THE WORLD'S LEADING IP LAW FIRMS AND PRACTITIONERS

Super Lawyers

Martindale-Hubbell AV PREEMINENT Peer Rated for Highest Level of Professional Excellence 2019

ROTHWELL FIGG
IP Professionals