IoT and Smart Homes: The Developing Legal Landscape

John Sperino, Vice President, General Counsel & Secretary

Emerson Commercial & Residential Solutions

EMERSON

Agenda

- Cybersecurity
- Privacy
- Contracts / Intellectual Property
- Product Liability

Cybersecurity

EMERSON

Landscape Continues to Expand in Geography, Variation & Complexity

- **Why governance of cyberspace is different and challenging?**
  - Cyberspace reaches across geo-political boundaries, and defies traditional governance
    - Who has authority to make law?
    - What is the applicable law?
    - Who has the power and authority to enforce it?
  - Different sets of rules to protect systems and data type
    - Critical infrastructure
    - Proprietary information
    - Personal data
    - Telecommunications data
  - Challenges of anonymity and attribution
  - Human rights dimension that transcends international boundaries
  - National interests, history and societal beliefs shape varying approaches
- **Result is widely varying (and often conflicting) national and regional approaches, priorities and tolerances**

- **October 21, 2016**
  - Mass disruption of the Internet
  - Commandeered IoT devices
  - Dyn acts as an Internet switchboard
  - Distributed denial-of-service attack
  - Coordinate many devices to bombard a company with more data than its circuits can handle
  - Is the Internet part of our nation's infrastructure?
  - Who is charged with the responsibility to protect it?

Cybersecurity Risk

Specific Cyber Vulnerabilities for IoT Devices

- An exploitation of the Universal Plug and Play protocol (UPnP) to gain access to many IoT devices
  - Hackers can use it to run commands on the devices, enabling the devices to harvest sensitive information or conduct attacks against homes and businesses, or engage in digital eavesdropping
- An exploitation of **default** passwords to send malicious and spam e-mails, or steal personally identifiable or credit card information
- Compromising the IoT device to cause physical harm
- Overloading the devices to render them inoperable

Cybersecurity Law

- **Federal & State civil laws**
  - Industry-specific regulations
    - Financial, health services, telecommunications, electric grid (GLBA, HIPAA, FCC, NERC-CIP)
    - Government contractors (DFARS, FARS)
  - Consumer protection regulation (FTC, FCC)
  - SEC disclosure requirements
  - Electronic Communications Privacy Act (ECPA)
  - Cybersecurity Act of 2015: Cybersecurity Information Sharing Act (CISA)
  - Critical infrastructure
    - Executive Order 13636 (Feb. 2013)
    - NIST Cybersecurity Framework & Critical Infrastructure Cyber Community (“C3”) (Feb. 2014)
  - State breach notification laws
  - State “data security” & identify theft laws
- **Federal criminal law**
  - Computer Fraud & Abuse Act

Focus in U.S. is on National Security, Economic Competitiveness and Consumer Protection

Primary Data Security Regulator in the U.S.

FTC has authority to take action against businesses that engage in certain "unfair or deceptive" trade practices in or affecting commerce. -15 U.S.C. §45(a)

- Does the FTC really have authority to regulate data security?
  - *FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 236 (3d Cir. 2015)
- Focus is **consumer protection** – not necessarily privacy
- Many companies settle with FTC via **consent order**
  - Equivalent of 20 years of annual/biannual FTC audits
  - Violations of consent order may result in significant monetary penalties (e.g. LifeLock -- $1M)
- A company's "practices" may be found to be "unfair" if they –
  - Caused or are likely cause
  - Substantial injury
  - To "consumers"
  - Where such injury is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers

FTC v. Wyndham Worldwide Corp. 799 F. 3d 236 (3d Cir. 2015)

- In 2008 and 2009, hackers successfully accessed Wyndham's computer networks, resulting in the unauthorized disclosure of 600,000 consumers' credit card data, leading to over $10.6M in fraudulent charges
- FTC brought an action against Wyndham alleging:

  (1) Wyndham's data security practices were unreasonable and therefore "unfair," and

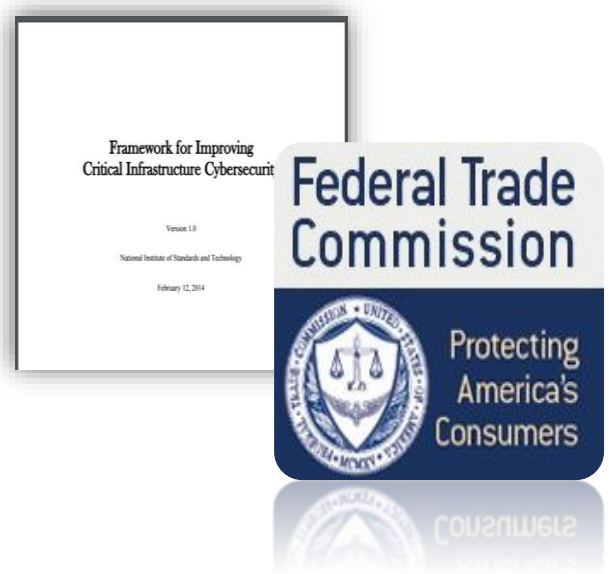
  (2) Wyndham's privacy policy was "deceptive"
- Wyndham moved to dismiss on the basis that the FTC had no authority to regulate cybersecurity, and even if it did, the FTC had not given companies fair notice of what data security practices constituted an "unfair" trade practice, nor did the FTC sufficiently allege consumer injury
- Third Circuit ruled against Wyndham:

  ✓ **FTC has authority to regulate companies' cybersecurity practices**

  ✓ **FTC's guidance, publications, announcements and consent decrees sufficiently put companies "on notice" around what may or may not constitute reasonable data security practices**

What Data Security Practices Constitute an "Unfair" Trade Practice?

- **No clear rules – "Know it when you see it"**
  - Must look at previous 60 rulings
  - Guidance publications provide over-generalized recommendations at best
  - Company's data security measures always evaluated in hindsight
  - FTC Workshops and FTC Chair's public comments indicate likely enforcement targets and FTC interpretation:



Q: Does compliance with NIST Cybersecurity Framework constitute "reasonable" data security under Section 5?

A: *Maybe…Maybe not.*

- *The NIST Framework is "not a standard or checklist"*
- *So "there's no such thing as 'complying with the Framework.'"*

"A company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might very well violate Section 5 of the FTC Act."

– FTC Chairwoman, Edith Ramirez (Sept. 7, 2016)

U.S. State Law

- Breach notification requirements – no national standard
  - "Personally identifiable information"
  - "Breach"
  - Notification obligations vary from state to state
  - Applicability determined by the residence of the individuals described in the compromised date
    - Not by the location of the data
    - Not by the location of the entity that experienced the breach
- State data security laws/identify theft laws
  - 10+ states require businesses to implement and maintain "reasonable" administrative, physical and technical data security practices
    - Massachusetts – most stringent – very specific
    - California – implementation of CIS controls = "reasonable" security
    - Washington, Minnesota – incorporates PCI-DSS requirements into statute
- State Unfair Trade Practices Laws ("Mini-FTC Laws")

State Laws Fill Gaps in Federal Law, but Can Set *De Facto* National Standards

Example: Massachusetts – (Mass. 201 C.F.R. 17)

Minimum Information Security Requirements

- Written "comprehensive information security program" containing administrative, technical and physical safeguards appropriate to the risk, cost and nature of the entity
- Ongoing program assessment and improvement
- Security policies & procedures
- Compliance with policies and procedures, including imposing disciplinary measures for violations of such security policies and procedure
- Employee trainings
- Regular monitoring to prevent unauthorized access to or unauthorized use of personal data and other means for detecting and preventing security system failures
- Preventing terminated employees from accessing records containing personal information
- Assessing third party security and obligating third parties to implement reasonable security measures
- Physical security measures
- Documenting responsible actions taken in connection with any incident involving a breach

Minimum Computer Security Requirements

- Secure user authentication protocols including
- Secure access control measures
- Encryption of data in transit
- Encryption of data at rest
- Monitoring of systems for unauthorized use of or access or personal information
- Up-to-date firewall protection and operating system security patches
- Up-to-date firewall protection and operating system security patches
- Up-to-date versions of system security agent software which must include malware protection
- Up-to-date patches and virus definitions set to receive the most current security updates on a regular basis
- Education and training of employees on the proper use of the computer security system and the importance of personal information security

"The safeguards…must be consistent with the safeguards for protection of personal information and information of similar character set forth in any state or federal regulations by which the [entity] may be regulated"

California Data Breach Notification Law & Information Security Statute

Statute requires *"reasonable security procedures and practices…to protect personal information from unauthorized, access, destruction, use, modification, or disclosure."*

"The 20 CIS Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal data should meet."

"Failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

The CIS Critical Security Controls for Effective Cyber Defense

CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

European Approach to Cybersecurity Law

- Protection of fundamental human rights, freedoms and civil liberties of paramount significance
- EU Single Digital Market Initiative & Cyber Public-Private Partnership (cPPP)
  - Data Protection Directive 46/95/EC → General Data Protection Regulation ("GDPR")
  - ePrivacy Directive (Directive on Privacy and Electronic communications) (under rev.)
  - EU Network and Information Systems Directive ("NIS Directive") (July 2016)
- Member State law
  - Data protection laws
  - Computer crime & data security laws
  - Labor laws
  - Telecommunications laws
  - National security laws

EU Cybersecurity Approach Contrasts with National Cybersecurity Policies Developed Both Within and Outside Europe

EU Cybersecurity Approach

Cybersecurity is an economic opportunity for the EU.

Key Objectives

- Enhance Europe's position as a world leader in the digital economy
- Creating a high level of consumer and personal data protection by defining minimum common digital security and privacy requirements across different sectors
- Increasing cybersecurity capabilities, cooperation and resiliency

Negligence Claims

- Historical hurdles in succeeding in post-breach negligence claims:
  - Failure to allege cognizable damages
  - Barred by economic loss rule (must allege personal injury or property damages)
  - Courts reluctant to create a legal duty to protect personal data in absence of legislative action
- Courts increasingly recognize a legal duty to protect information where it's foreseeable that unauthorized access is likely to result in harm
  - ***In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*** – A legal duty existed to "safeguard a consumer's confidential data entrusted to a commercial entity" (S.D. Cal. 2014)
  - ***In re Target Corp. Customer Data Sec. Breach Litig.*** – Target owed plaintiff financial institutions a duty of care"). (D. Minn. 2014)

Standard of Care: Regulatory Guidance, Standards Frameworks (e.g. NIST) and Industry Standard Practices

Class Action Lawsuits: Circuit Split

- Historically, data breach class actions have been largely unsuccessful in surviving dismissal for lack of standing
  - Plaintiff must allege an injury-in-fact that is *"**concrete, particularized, and actual or imminent**" (Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013))
  - Threatened injury must be ***certainly impending;*** *possible* future injury are not sufficient
  - *Reilly v. Ceridian Corp.* (3d Cir. 2011) – set high bar for establishing injury-in-fact in breach suits
- Recently, a **split** among circuits is emerging
  - Harm is "certainly impending" since no doubt hackers stole PII to commit fraud/identity theft
    - *Remijas v. Neimen Marcus* (7th Cir. 2015)
    - *Lewert v. P.F. Chang's China Bistro* (7th Cir. 2016)
    - *Galaria v. Nationwide Mutual Insurance, Co.* (N.D. Ga. 2016)

Privacy

Data Privacy (United States)

- **No comprehensive federal statute**

- **Sectoral approach (in general)**
  - Regulation based on ***type of data*** and ***type of entity*** holding the data
  - Health care, financial services, children
  - Federal agencies
  - Congressional committees
  - State statutes
  - Common law
  - Self-regulation/industry associations and standards

Sources of Law (Constitutional)

- **U.S. Constitution**
  - SCOTUS has found “penumbras” and “emanations of various Bill of Rights guarantees” as creating “a zone of privacy”
    - For example, child rearing, procreation, marriage, and termination of medical treatment
- **4th Amendment**
  - *Kyllo v. United States* 553 U.S. 27 (2001)
  - Thermal imaging of a home was a search protected by the 4th Amendment
  - Details of the home that would previously have been unknowable without physical intrusion, the surveillance is a “search”
- **States**
  - Alaska, California, Montana and Washington

Sources of Law (Statutes)

- **Gramm-Leach-Bliley Act**
  - Financial data and financial institutions
  - Notice of privacy policies and ability to opt out of information sharing
- **Fair Credit Reporting Act**
  - Credit reports
  - Accuracy and dispute resolution
- **Health Insurance Portability and Accountability Act (HIPPA)**
  - Medical data
  - Standards for use and protection
- **Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)**
  - Collection and use of email addresses
- **US Privacy Act (1974)**
  - Consent from individual required for most disclosure
- **Electronic Communication Privacy Act of 1986**

Sources of Law (Statutes)

- **Federal Trade Commission Act**
  - Unfair or deceptive trade practices
- **State security breach notification laws**
  - Inconsistent definitions of “personal information,” exemptions and coverage
- **California Online Privacy Protection Act (CalOPPA)**
  - Mandatory disclosure when personal information is shared
  - Reasonable security required
  - List of personally identifiable information that is collected
  - Right to be forgotten (under 18)

Sources of Law (Tort – Invasion of Privacy)

- **Misappropriation of the right of publicity**
  - Defendant's unauthorized appropriation of name, likeness or identity
  - For the defendant's advantage
  - Lack of consent
  - Resulting in injury

- **Intrusion upon seclusion**
  - Intrusion into the plaintiff's private affairs, solitude or seclusion
  - In a manner that is objectionable to a reasonable person

- **False light**
  - Defendant made public facts about plaintiff
  - Facts place plaintiff in a false light
  - False light is highly offensive to a reasonable person

Sources of Law (Tort – Invasion of Privacy)

- **Public disclosure of private facts**
  - Publicity of a matter concerning the private life of another
  - Highly offensive to a reasonable person
  - No legitimate concern to the public
  - Tension with 1st Amendment freedoms of speech and press
  - Disfavored

- **Consent is a defense**

- **Appropriation of name or likeness**

Sources of Interest

- **Charter of Fundamental Rights of the EU (2000)**
  - Article 8: Right to protection of personal data
- **United Nations: Universal Declaration of Human Rights (1948)**
  - Prohibits arbitrary interference with privacy
- **United Nations: Resolution on the Right to Privacy in the Digital Age (2013)**
  - Discusses the negative impact of surveillance on human rights
- **Consumer Privacy Bill of Rights Act**
  - 2015 Discussion Draft
  - Reasonable security required
  - Right to be forgotten (under 18)
- ***Microsoft v. Department of Justice***

FTC Guidance

- The FTC provided these recommendations for IoT device builders:
  - build security into devices ***at the outset***, rather than as an afterthought in the design process
  - ***train*** employees and vendors about the importance of security
  - consider a "***defense-in-depth" strategy*** with multiple layers of security
  - ***keep unauthorized users*** from accessing a consumer's device
  - ***monitor*** connected devices ***throughout*** their expected ***life cycle***, and where feasible, provide ***security patches*** to cover risks
  - consider ***data minimization: limit the collection of consumer data***, and retaining it only for a set period of time, and not indefinitely

FTC Action

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

FOR RELEASE

February 6, 2017

FTC Action

FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras

Device-maker's alleged failures to reasonably secure software created malware risks and other vulnerabilities

FOR RELEASE

January 5, 2017

Recent Class Actions

- **2016 class action lawsuit in Illinois**
  - Manufacturer allegedly collected and kept usage/tracking info (times of use, battery life and intensity level, tied to user and partner e-mails, without notice or consent
  - $3.75 million settlement

- **2017 class action privacy lawsuit against Bose**
  - Allegation is that by using a companion app, the Bose wireless headphones were secretly collecting, transmitting, and disclosing its customers' music and audio selections and selling that data to advertisers without notice or consent

Data Regulation (EU)

- **General Data Protection Regulation**
  - Replaces the 1995 Directive
  - Applies on May 25, 2018
  - Expanded territorial scope (Organizations outside the EU targeting citizens in the EU)
  - Data protection by design (data minimization)
  - Consent must be “explicit” for “sensitive” data
  - Data protection officers for large scale operations
  - Notice of data breach within 72 hours
  - Right to be forgotten
  - Right to object to data being used for marketing purposes
  - Data portability from one system to another
  - Under 16 requires parental consent to use services like Facebook, Snapchat and Instagram

Client Considerations

- **Massive cloud data servers now located in Europe**

- **European Commission**
  - Steps to create a “Digital Single Market” (interoperability)
  - European cloud
  - Trusted IoT label

- **The EU is “winning”**? (Daniel Solove)

Contracts / Intellectual Property

EMERSON

Contract Considerations

- **Default warranties**
  - Software generally viewed as a good under the Uniform Commercial Code
  - Implied warranties of “merchantability” and “fitness for a particular use”
  - Exposure to incidental and consequential damages

- **Terms of service**
  - If software is a service, what are the default terms of use?
  - Shrink wrap, browse wrap, click wrap
  - How do you obtain consent for products that do not have screens?

- **Extraterritorial jurisdiction**
  - EU Directive on data protection
  - Applies where an operator uses “equipment” situated on an EU member’s territory
  - Right to be forgotten
  - Jurisdictional limitation?

Contract Considerations

- **Terms**
  - Warranty disclaimers
  - Class action waivers
  - Jury trial waivers
  - Mandatory arbitration

- ***Starkey v. G. Adventures, Inc.* (2nd Cir.)**
  - Upheld disclosure of contract terms to consumers via email post-contract formation

Insurance

Cyber Coverage

- Insurers have begun excluding electronic data from Commercial and General Liability policies
- Coverage in heritage CGL policies is hotly contested
- Notice, opportunity to review and mutual assent

Considerations

- Role of cyber insurance policies
- Scrutinize policy exceptions
- Refine ambiguous aspects of the policy
- Coverage for FTC (i.e., gov't) action

Intellectual Property

- **Intellectual property infringement**
  - *Alice Corp. v. CLS Bank*
  - "A mere instruction to implement an abstract idea on a computer cannot impart patent eligibility"
  - Resulted in many software patents and business method patents being invalidated
  - Divided infringement (single actor must perform all elements of the claim)
  - Contributory infringement

- **Data ownership**
  - UCC is silent on data ownership
  - Can data be a trade secret?
  - Data must be (i) a secret, (ii) value is derived from it, and (iii) access is safeguarded or protected
  - Digital Millennium Copyright Act – prohibits people from circumventing encryption to access copyrighted work

Product Liability

Potential New Hazards Analysis

Loss of Connectivity

A fault in a device, such as a product serving as a communication hub for a household, may result in the loss of access or control to the internet

Data Integrity

If accurate data support a safety function, avoiding data corruption is important

Loss of a Safety Function

Products connected to the IoT may change their performance through software upgrades that are automatically pushed out over the Internet

Staff Report

Potential Hazards Associated with Emerging and Future Technologies

January 18, 2017

Software

- **Product liability**
  - Strict Liability: liable once defect is proven, even if all possible care was exercised in the preparation of the product
  - In contrast to contract law, software is generally not viewed as a “product” in product liability tort law
  - What about IoT that is a mix of product and software?
  - Is “bug” free software possible?
  - Is a negligence standard more appropriate?

Closing Thoughts

Cybersecurity

- Role of FTC
- Developing Negligence Law
- Standing

Privacy

- Evolving Norms
- State Leadership
- EU Competitive Advantage

Contracts / Intellectual Property

- Notice / Consent
- Data Ownership
- Encryption

Product Liability

- Monitor CPSC Developments
- Software