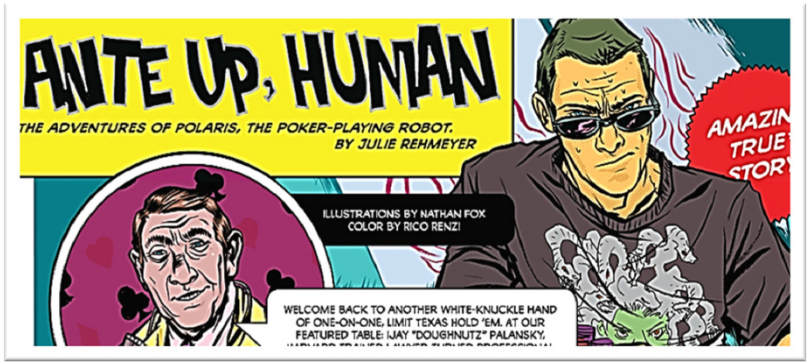
Legal Liability for IoT Vulnerabilities

IJay Palansky

About Me

- Trial lawyer at Armstrong Teasdale
- Complex commercial, consumer protection, class actions
- Mostly represent defendants
- Lead counsel for 220,000 member plaintiff class in the Jeep hack class action



About Armstrong Teasdale

- Top 200 law firm
- Top-ranked trial lawyers, strong IP practice

Armstrong Teasdale

Presentation Overview

- Background and policy
- IoT vulnerabilities in general
- Why a wave of IoT lawsuits is about to hit (Jeep hack)
- Corporate risks
- Legal principles
- How to prepare

Policy Considerations

- "What would make 'defense greater than offense'…?" – Jeff Motz
- Legal liability can play a crucial role in this calculus
- Purpose of tort law
- Accountability = change
- (Application of) the law hasn't caught up to technology

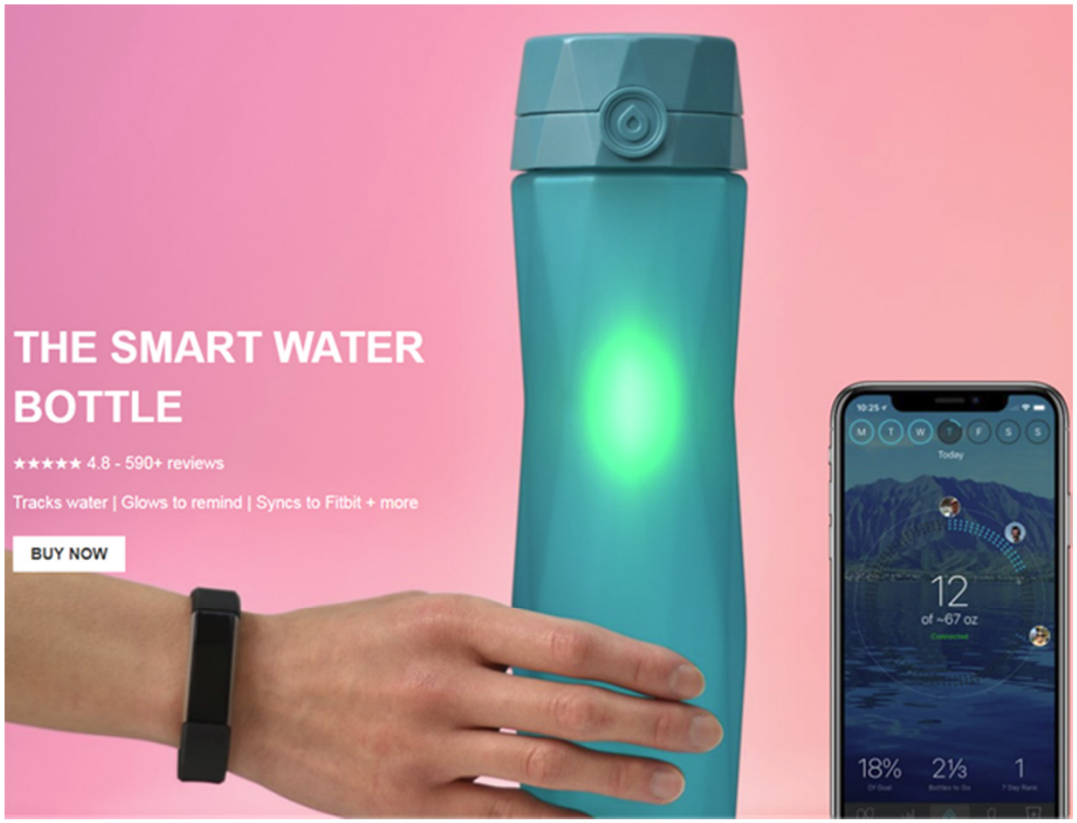

nest
COOLING
75
78

20+ BILLION


SMART TV
Featured
Recent
NETFLIX
3 NOW


amazon


CLEAN
iRobot
Roomba


THE SMART WATER BOTTLE
★★★★★ 4.8 - 590+ reviews
Tracks water | Glows to remind | Syncs to Fitbit + more
BUY NOW
Today
12
of ~67 oz
18%
2⅓
1

MOEN

BATHROOM KITCHEN INSPIRATION PARTS SERVICE

Innovations U by Moen FEATURES BENEFITS DEMO SUPPORT GALLERY SHOP NOW

U by Moen Digital Shower

Control Your Shower Your Way

U by Moen has forever transformed showering to create a personalized showering experience. Now with three ways to control your shower: **voice, phone, and controller.**

Replay

i.Con Smart Condom

Each: **$80.99**

Have you ever wondered how m
many thrusts? Speed of your thr
many different positions you use
wondered how you stack up to o

Welcome to the future of wearab

Welcome to i.Con.

We know you may have a lot of

Register your interest

Your Email Address:

IoT: Potential For Harm

- Processors and communication capacity.
- Weak to non-existent cybersecurity.
- Wide variety of code. Even different models of the same product may have different, proprietary software. Complicates detection and patching.
- So many devices, configurations, proprietary codes, etc., that ad hoc patching often isn't a viable option (suggests need for much improved designed cybersecurity).
- User error or inattention, e.g. patch lag.

How to hack a car—a quick crash-course

IoT Harm: Pathways

- Data breach
- IoT ransomware
- DDoS attacks
- Privacy-related
- Potential for cyber-physical

The Washington Post

Yes, terrorists could have hacked Dick Cheney's heart

By Andrea Peterson October 21, 2013

Dick Cheney currently has a pulse – which was not always the case. (AP Photo/Olivia Harris, Pool, File)

On "60 Minutes" this Sunday, former Vice President Dick Cheney revealed that his doctor ordered the wireless functionality of his heart implant disabled due to fears it might be hacked

Plaintiffs' lawyers are watching…waiting. Why haven't they pounced?

- Not many IoT hacks (with harm and attribution) – yet
- Few accepted standards of care
- Struggle of plaintiffs' lawyers and enforcement agencies to understand the tech and how the law applies to it
- Few precedents

With the mobile version of your site, you can check your messages while chasing an ambulance.

Interconnectedness Issues

- Not the first time product liability or other law has had to address new technology, but the interconnectedness involved in IoT is unique.

Who should be paying attention?
Everyone in the IoT supply chain

- Companies that **design** IoT products
- Companies that **manufacture** final IoT products
- Companies that manufacture cybersecurity-related **components** used in IoT products (e.g., Harman in the Jeep litigation)
  - Component manufacturers are generally liable only if their component is defective
  - There may be a ***duty to warn*** of foreseeable dangers if a component manufacturer is aware that the final product may be harmful/vulnerable

Some enforcement by regulators:

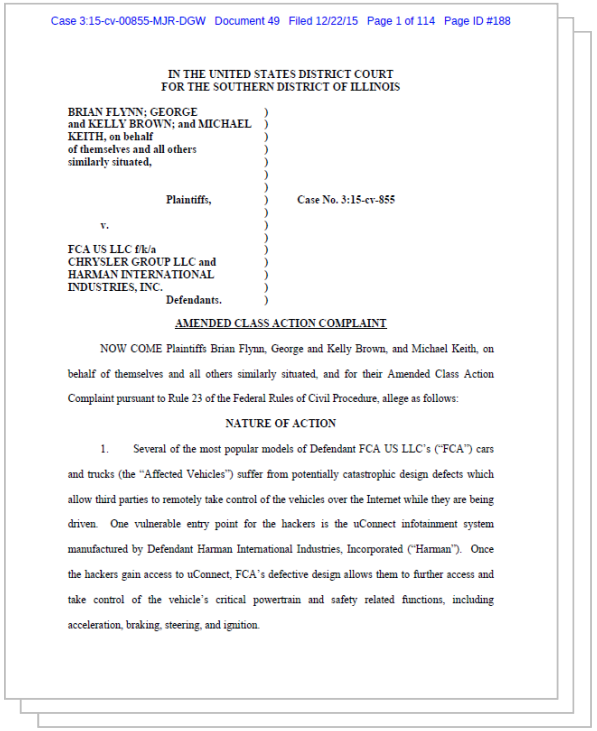
- TRENDnet Webcam hack: Hackers posted live feeds (video and some audio) from 700 webcams in January 2012
- September 2013: Settlement with the Federal Trade Commission
- Security architecture review
- Vulnerability and penetration testing
- Code review and software testing for security
- Implement reasonable training and guidance of employees involved in designing, coding, and testing
- Firmware updates, stopped all shipments, updated all models
- Mandatory bi-annual third-party security audits for 20 years

Jeep Hack


CAR HACK
RECALL
NBCNEWS.COM

Federal Class Action Litigation

- Filed August 2015
- Suing Fiat Chrysler and Harman International (manufacturer of the Uconnect head unit that Miller and Valasek hacked to gain access to the Jeep's CAN Bus)
- Still going today



Case 3:15-cv-00855-MJR-DGW Document 49 Filed 12/22/15 Page 1 of 114 Page ID #188

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

BRIAN FLYNN; GEORGE and KELLY BROWN; and MICHAEL KEITH, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

FCA US LLC f/k/a CHRYSLER GROUP LLC and HARMAN INTERNATIONAL INDUSTRIES, INC.

Defendants.

Case No. 3:15-cv-855

AMENDED CLASS ACTION COMPLAINT

NOW COME Plaintiffs Brian Flynn, George and Kelly Brown, and Michael Keith, on behalf of themselves and all others similarly situated, and for their Amended Class Action Complaint pursuant to Rule 23 of the Federal Rules of Civil Procedure, allege as follows:

NATURE OF ACTION

1. Several of the most popular models of Defendant FCA US LLC's ("FCA") cars and trucks (the "Affected Vehicles") suffer from potentially catastrophic design defects which allow third parties to remotely take control of the vehicles over the Internet while they are being driven. One vulnerable entry point for the hackers is the uConnect infotainment system manufactured by Defendant Harman International Industries, Incorporated ("Harman"). Once the hackers gain access to uConnect, FCA's defective design allows them to further access and take control of the vehicle's critical powertrain and safety related functions, including acceleration, braking, steering, and ignition.

Corporate Risks

Reputational Harm

NEW YORK POST

TECH

Roomba maker wants to sell your home's floor plan

By Natalie O'Neill July 25, 2017 | 1:04pm |

CBS NEWS

CBS/AP / *May 29, 2018, 11:07 AM*

How to keep Amazon Echo, other devices from listening to private chats

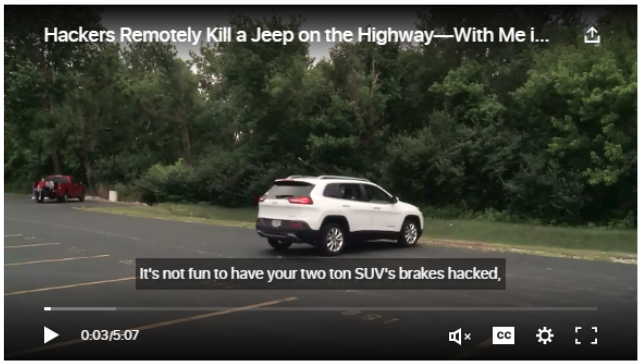
Share / Tweet / Reddit / Flipboard / Email

NEW YORK -- Revelations that an Amazon Echo smart speaker inadvertently sent a family's private conversation to an acquaintance highlights some unexpected risks of new voice-enabled technologies. A Portland, Oregon, woman told CBS Seattle affiliate KIRO-TV she had no idea her Echo listened to her and her husband and then shared their conversation with one of his employees.

WIRED

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



Remediation and/or Production Interruption

- Steps to eliminate the vulnerability, e.g., a product recall
- Software patches
- Firmware updates
- Production interruptions and engineering overhauls

Costs of Litigation

- Legal fees
- Burden on/distraction of key employees
- Disruption of operations
- Expensive experts
- Uncertainty

Liability

- Legal concepts
  - Damages
  - Claims

Damages

- Vary by legal claim (negligence, warranty, strict liability, fraud, etc.)
- Property damage
- Personal injury to anyone injured by the product, including bystanders
- Diminished value of, or overpayment for, the product
- Emotional distress (sometimes, in some jurisdictions)
- Cost of repair
- Contract-based damages
- Punitive damages (depending on the culpability of the defendant – e.g., fraud or reckless disregard of consumer safety)

Potential Claims

Claims

- Negligence
- Strict product liability (design defect)
- Breach of warranty (express and implied)
- Fraud and fraudulent omission
- Consumer protection statutes

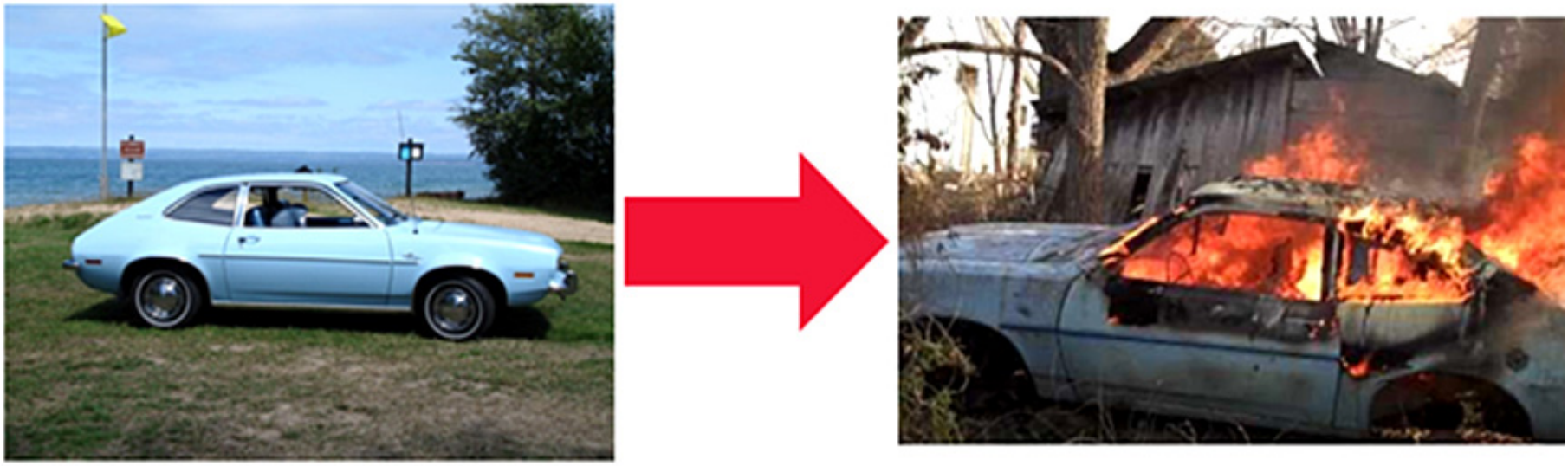
Bases for Liability

- Generally no federal law
- There may be variations among states, but the general principles are widely the same

Negligence

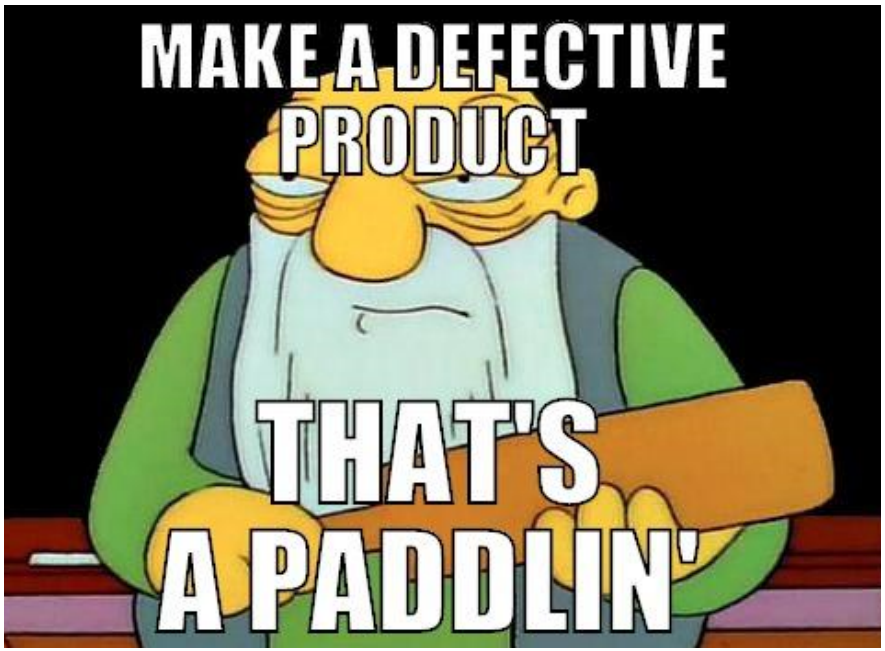
- A party may be liable for negligence if it causes harm after failing to take reasonable care
- Level of reasonable care is generally set according to industry standards, but tricky for IoT, since standards of care are not developed/established
- Duty of care applies to design, testing, manufacture, labeling, distribution, etc.

Strict Product Liability (Design Defect)



Design Defect: Examples

- Could be almost anything
- Hardware or software
- Inadequate segmentation, failure to use proper cybersecurity hardware devices or engineering practices
- Storing passwords in plain text, storing hardcoded admin password



Strict Product Liability: Elements

- Focus on the *product* rather than the *conduct of the actor*
- "Defective" if the product is dangerous beyond a consumer's expectations, or it is "unreasonably dangerous," considering state of the art, available alternatives, and a balancing of risks against the utility of the product.
- Physical harm to person or property

Breach of Warranty

- Express warranties (including marketing representations of safety/security)
- Implied warranties
  - *Implied warranty of merchantability*: a product is "fit for its ordinary purposes"
  - Fitness includes safety—if a product is unsafe when used as expected, then it is not fit for its ordinary purposes

Fraud/Fraudulent Omission

- ***Fraud***: Affirmative misrepresentations regarding the safety/security of the product or component
- ***Fraudulent omission***: Failure to disclose vulnerabilities that were known (or in some instances, that should have been known)

Consumer Protection Statutes

- State statutes, designed to be consumer friendly
- Broad definitions of actionable deception or unfair conduct
- Often provide for the recovery of attorneys' fees, statutory penalties, and punitive damages

Defenses

Economic Loss Rule

- Precludes recovery for "economic losses" for *torts*
  - "Economic losses" mean loss of value of the product or harm to a business
- Generally does not apply to fraud or consumer protection claims

"It's worse than you think, it goes down to the third floor."

Adherence to Standards as a Potential Defense

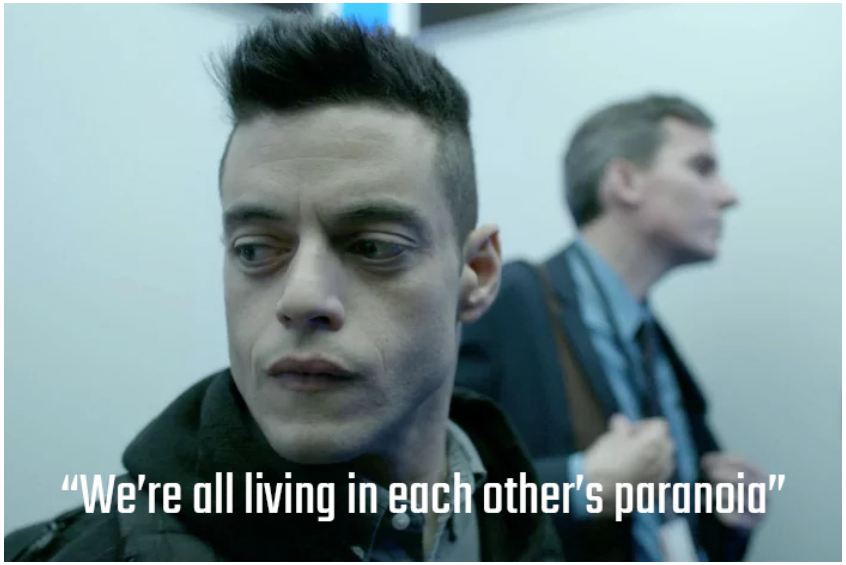
- Important start, but not necessarily a complete defense
- Compliance with government regulations
- Depends on foreseeability, standard of care, definition of a "defect," etc.

What Should Companies Do?

- Decisions about the right level of security should be informed by considerations of potential liability.
- Not chicken little or “security nihilists” who believe that any compromise on perfect security is a mortal flaw.

What Can be Done to Minimize Risk of Liability?

- Act responsibly
- Be paranoid (hazard analysis, risk analysis)
- Allocate risk (contracts with other parties upstream and downstream, warnings, instructions)
  - Hardware and software vendors, consultants, downstream users of the product, etc.

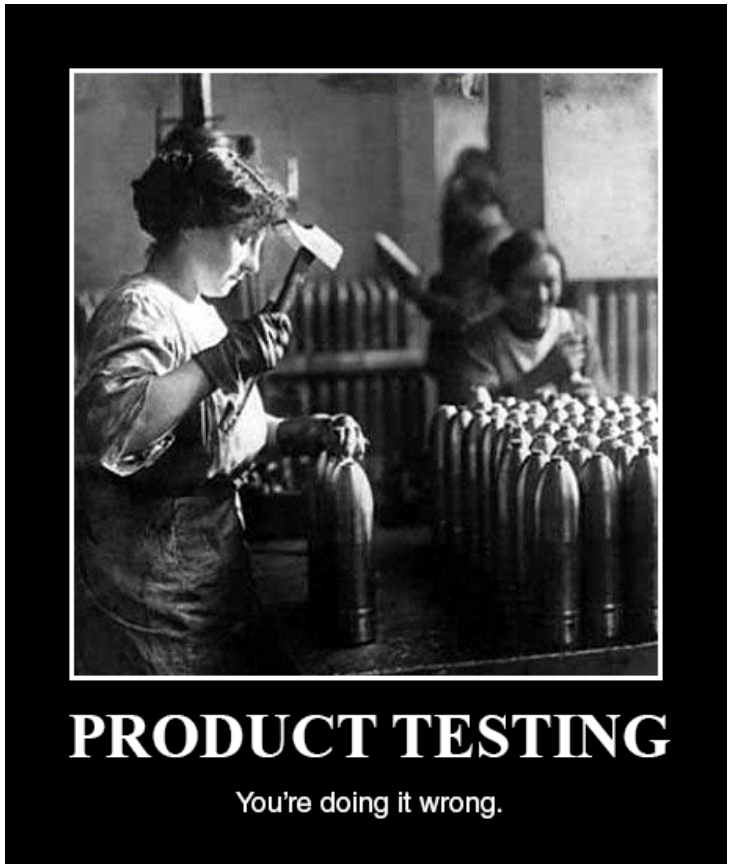


What Can be Done to Minimize Risk of Liability? *Design Review*

- Hazard analysis:
  - Identify all intended and unintended uses and misuses of the product
- Risk assessment: What are the magnitudes and likelihoods of the risks?
- Are there regulatory or industry standards? Are they adequately protective?
- Address identified risks

What Can be Done to Minimize Risk of Liability? *Testing*

- Test products to identify vulnerabilities
- Penetration testing, etc.
- "CYA": Memorialize the analysis and decision-making process.
  - Ultimately, in a lawsuit the design/manufacturing *process* is scrutinized, not just the end product or result
  - Prove that you acted responsibly, considered all foreseeable hazards, etc.



What Can be Done to Minimize Risk of Liability?

"Word Control" Programs

- Warnings (for all anticipated uses)
  - Substance
  - Language
  - Location (prominence)
- Instructions
- Manuals
- Marketing
  - Advertisements
  - Language that salespeople use
  - Don't say dumb s*#t

Insurance

- Review corporate insurance policies with IoT liability in mind
  - Scope of general liability insurance program
  - Exclusions for cybersecurity liability (data breaches)

What Should IoT Companies Do if Their Product is Involved in an "Event"?

- Hire a [good] lawyer!
- Investigate the cause, including discussions with engineers and business people
- Identify scope of the issue and consider whether and how to notify consumers
- Respond quickly and responsibly

Black Hat Sound Bites

- A wave of litigation over IoT liability is on the horizon. The threat may be existential for companies that haven't properly prepared.
- Sound cybersecurity design and engineering is paramount, but should be informed and guided by an understanding of liability risk.
- A clear process involving hazard identification, design response, risk assessment, word control programs, and testing, will go a long way to minimizing liability risk, and should help improve cybersecurity as well. Comprehensive. Followed. Memorialized.

Questions?

Contact Info

IJay Palansky
314.552.6682
ipalansky@armstrongteasdale.com