DIGITAL TRANSFORMATION (DT)

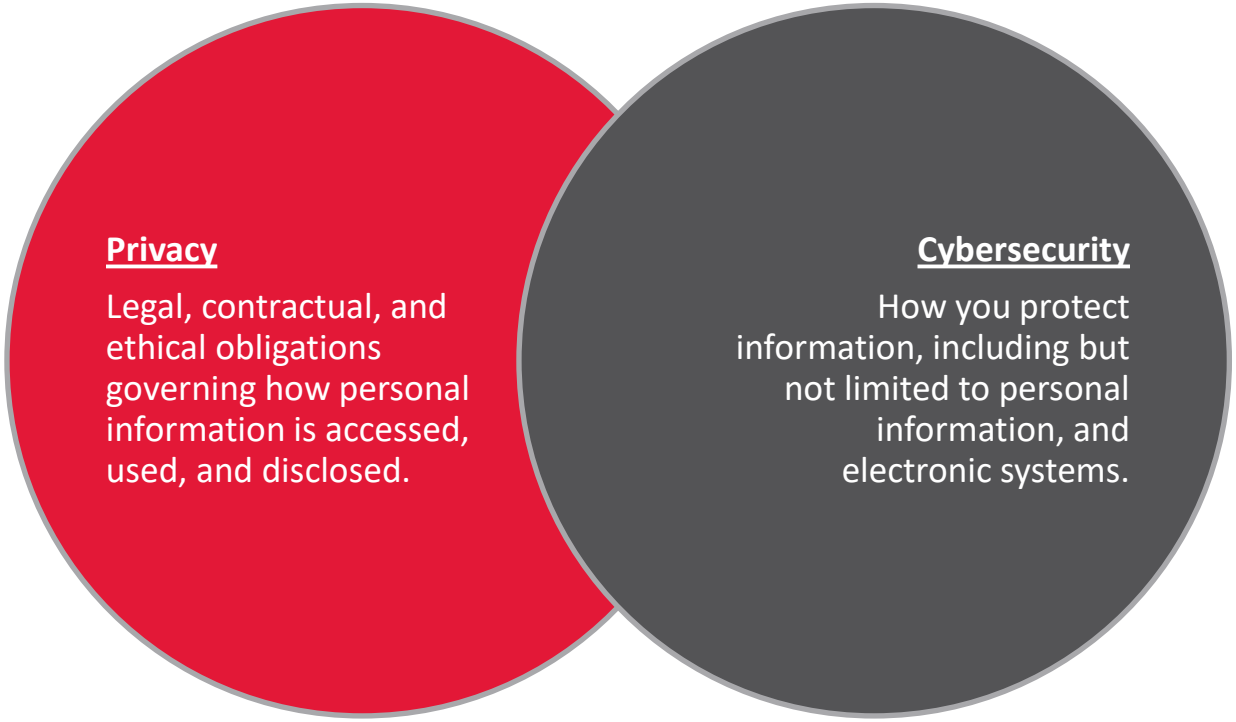
The Internet of Things and the Cybersecurity and Data Privacy Laws Implicated

DECEMBER 8, 2021

Lucas Amodio
Scott Galt
Romaine Marshall
Jeff Schultz

Always exceed expectations through teamwork and excellent client service.

Simple Definitions



Governed by a patchwork of legal, industry and regulatory standards

DT and the Pandemic

- **Digital Transformation (DT) is the process of leveraging technology, people and processes to innovate and stay competitive.**

- **DT has led to businesses managing more than 10 times the quantity of data they did five years ago per a recent poll of 1,000 execs.**

- ***"We've seen two years' worth of [DT] in two months."***
  - Satya Nadella (Microsoft CEO, April 2020)

ATDT Fall Series: Session 1 Recap

- ***Navigating the Patchwork of Cybersecurity and Data Privacy Laws that Govern***
- **"Common Threads" Emerge**
  - Cybersecurity
    - Incident Response Plans (IRPs)
    - Risk Assessments (RAs)
    - Written Information Security Programs (WISPs)
  - Data Privacy
    - Privacy Policies and Procedures
    - Privacy Reviews, Data Privacy Impact Assessments (DPIAs)

CYBERSECURITY

Federal Trade Commission:

Ask: "What are the industry standards? Are we meeting them?"

Patchwork Common Threads

- Incident Response Plans (IRPs)
- Risk Assessments (RAs)
- Written Information Security Programs (WISPs)

IRPs – Key Elements

- Phase 1 – Accountability
  - Identify the Incident Response Team (IRT) and its duties.
- Phase 2 – Response Procedures
  - Define incident response procedures and incident severity classifications
- Phase 3 – Reporting and Notification
  - Identify legal and contractual obligations
- Phase 4 – Post-incident Response
  - Make sure IRP training, testing and review happens at least every six months

RAs – Key Elements

- Assess electronic systems at least once every 12 months and any internal and external risks to the security, confidentiality, or integrity of personal or sensitive information and systems

WISPs – Key Elements

- Evaluate and adjust the WISP in light of any changes to operations or business arrangements

DATA PRIVACY

General Data Protection Regulation (GDPR):

"The law asks you to make a good faith effort to give people the means to control how their data is used and who has access to it."

Patchwork Common Threads

- There is quite a lot at stake
  - The California Consumer Privacy Act (CCPA) has been amended by the California Privacy Rights Act and becomes operative in January 2023
  - New state laws have passed, Colorado Privacy Act (CPA), Virginia Consumer Data Protection Act (CDPA), and more are being considered
  - Federal laws continue to evolve and enforcement is expanding (e.g., SEC recently settled with app developer for $10 million)

Data Privacy Protections and Responses

- Privacy "readiness" assessments
  - Applicability analysis of state, federal and international privacy laws
  - Privacy risk assessment
- Legally defensible GDPR/CCPA compliance programs
  - Review and update existing policies and procedures
  - Prepare data protection impact assessments (DPIAs)
- Updates to Data Processing Agreements that reflect patchwork, including new EU Standard Contractual Clauses
- Regulators take cooperation into account
- Clarity is essential
- Both legislation and the technology to help address it will continue to evolve

ATDT Fall Series: Session 2 Recap

- ***Supply Chain Risk Management: a Cybersecurity and Data Privacy Imperative***

Source: OCC

Recent guidance from the Federal Reserve, FDIC and OCC, recommends certain best practices, including:

PLANNING

- Assess the nature of the vendor interaction and potential impact on your customers, employees, and partners
- Explain to the vendor how the organization will select, assess and oversee the vendor

DUE DILIGENCE

- Evaluate the vendor's ownership structure, and its legal and regulatory compliance history and capabilities
- Assess the vendor's financial condition – review financial statements, annual reports and public filings

CONTRACT NEGOTIATION

- Data protection agreements (DPAs) are the best ways to ensure vendors protect your data
- Cover all your data – not just personal data
- Embed a standards-based security questionnaire to learn about the vendor's security program
- Use straightforward language so that business and technical professionals on both sides of the deal can understand their obligations
- **Red flags:** low liability limits for cybersecurity incidents, a lack of transparency, or vague commitments to cybersecurity and data privacy

MONITORING

- Approve, or delegate, the responsibility of managing vendor contracts and reporting their status to management or the board
- Review the results of management's ongoing monitoring of third-party relationships involving critical activities

TERMINATION

- Evaluate the third party's financial condition and changes
- Review the adequacy of the third party's insurance coverage
- Review relevant audits and other reports from the third party

ATDT Fall/Winter Series

- ***The Internet of Things and the Cybersecurity and Data Privacy Laws Implicated***
  - Wednesday, Dec. 8, 2021
- ***ATDT Winter Series Preview***
  - February, March, April 2022 (dates TBD)
    - Blockchain, cryptocurrencies, and cybersecurity legal risks
    - Artificial Intel., digital assets, and data privacy legal risks
    - A roadmap to data privacy readiness, *e.g.*, the Cal. Privacy Rights Act, VA and CO's new laws, and updates from abroad (the EU and China)

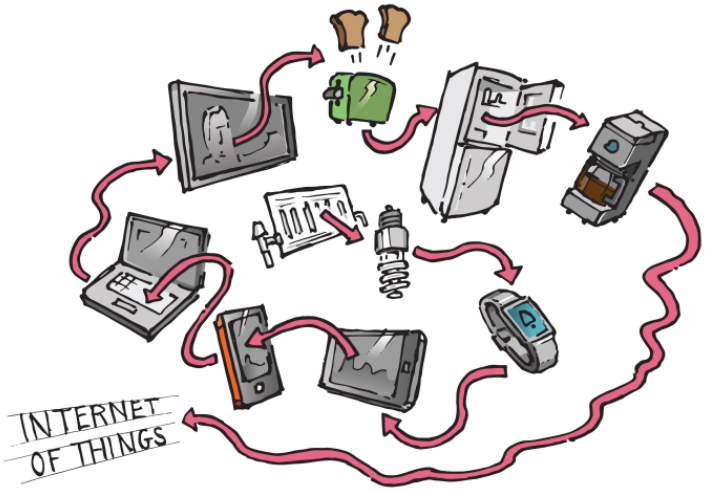
The Threat

Internet of Things

FTC Definition:

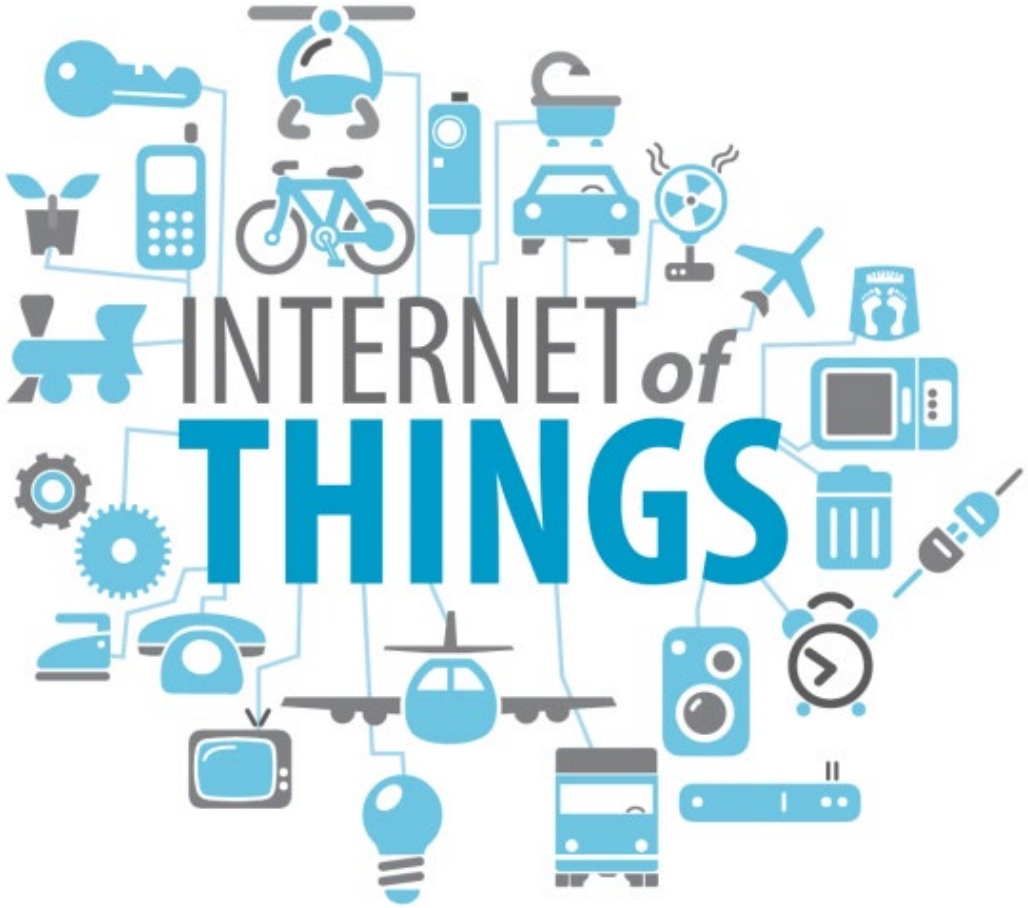
> ***The ability of everyday objects to connect to the Internet to send and receive data.***

- **Physical Objects**
- **Consumer Goods**



IoT: Benefits

- Data Collection
- Convenience
- Coolness Factor
- Others?



IoT Drawbacks, History

- **Zombiebots**
- **Opening holes in security**
- **Privacy Issues**
- **Product Liability Laws?**

***

- **Started off with Sensors**
  - Carnegie Melon Coke Machine
- **Then to switches**
  - Remote locations
- **Gradually more and more complicated machines**

IoT Attacks – Cyber-Physical

- **Stuxnet**
  - Centrifuges
- **German Steel Mill**
  - “Massive damage to the system.”
  - “Unable to shut down a blast furnace in a regulated manner.”

What Happened?

- October 21, 2016: Massive Distributed Denial of Service (DDoS) attack
- Targeted a domain name system (*aka* translator)
- Massive amounts of junk data and traffic transmitted from multiple machines (256 billion bits per second)

IoT and Things to Keep in Mind

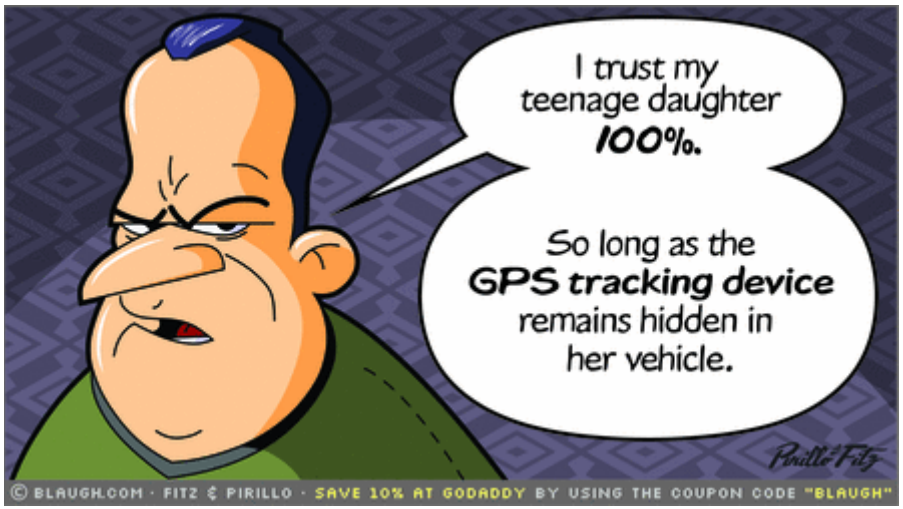
- **IoT is collecting extensive personal information about users:**
  - Location
  - Patterns of movement; speed
  - User preferences
  - Video
  - Audio
- **This information is useful and potentially available to others.**

IoT Data as Evidence

- Criminal Cases
- Divorce and Custody Cases
- Personal Injury Cases
- Noncompete Cases
- Employment Disputes
- Commercial Lawsuits

Laws and Regulations

IoT as a *Legal* Concern



Location: The Subject of Many Discovery Disputes

- **Installing a GPS tracking device on a vehicle to monitor the vehicle's movements constitutes a search under the Fourth Amendment.** *U.S. v. Jones*, 132 U.S. 945(2012)
- **New Jersey Court says it's okay for a wife to plant a GPS tracker in her soon to be ex-husband's vehicle.**
- **OnStar was tracking former subscribers until Senators publicly criticized.**
- **Insurance companies give discounts for voluntary GPS tracking.**

Why IoT Devices?

- Have processor and communication capability
- Usually, no internal security scanners
- Usually, minimal security
- Hard to detect compromise

Audio and Video: The Next IoT Frontier

- Bentonville, AR police sought a warrant for Amazon to had over audio records from an Echo device for use in a first-degree murder trial.
- Amazon declined; police say they were able to pull data off of the speaker itself.
- However, Amazon later provided the information after the Defendant agreed.
- SIDE NOTE: Another smart home device showed that 140 gallons of water were used between 1 a.m. and 3 a.m. the night of the incident in question (to wash away evidence?).

Big Difficulty in this Area of the Law:
Lack of Understanding of the Technology

"If I'm applying the First Amendment, I have to apply it to a world where there's an Internet, and there's Facebook, and there are movies like ... *The Social Network*, which I couldn't even understand ."

— Justice Stephen Breyer

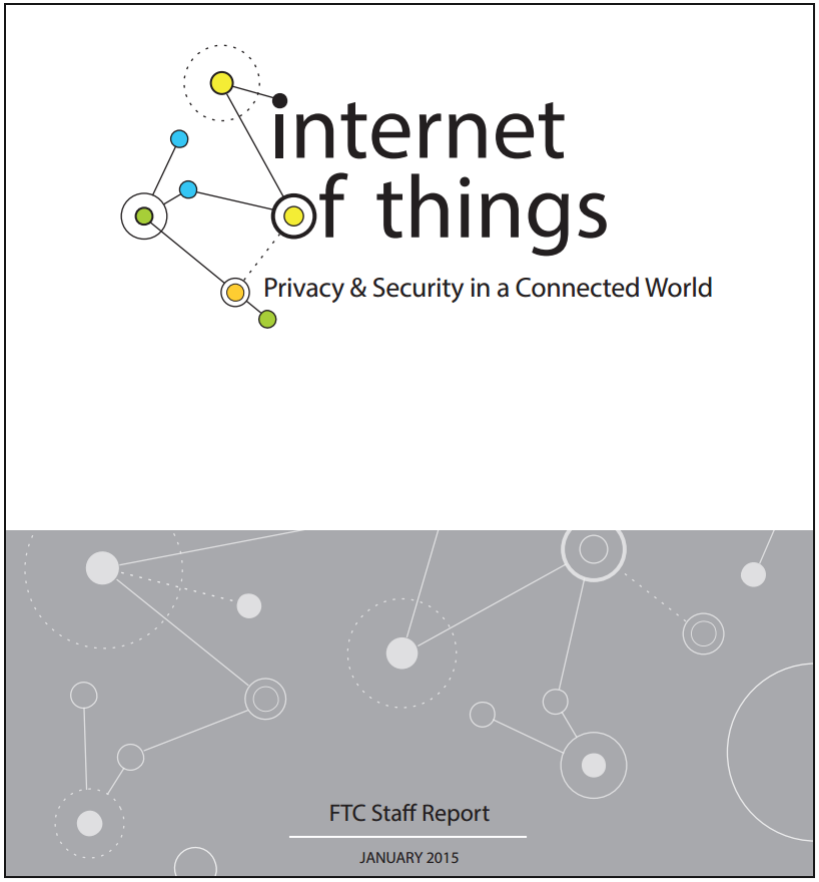
***Justice Roberts*:** "I thought, you know, you push a button; it goes right to the other thing."

***Justice Scalia*:** "You mean it doesn't go right to the other thing?"

— Justice John Roberts to Justice Antonin Scalia Regarding How a Text-Messaging Service Works

The Federal Trade Commission

- Hosted a workshop in 2013
- Published a Staff Report in January 2015
- Monitoring the issues, but not ready for legislation
- Sued for violations



IoT Cybersecurity Improvement Act

- Enacted Dec. 4, 2020.
- Mandates cybersecurity Standards and Guidelines for the acquisition and use of IoT devices capable of connecting to the Internet.
- While directly limited to those devices used by the Federal Government, also affects government contractors.
- Expected to have major spillover effect to private industry as well.
- National Institute of Standards and Technology (NIST) - SP800-213 – Issued November 2021.

What about the States?

- **In 2019, CA and OR passed IoT laws requiring reasonable security, including:**

  (a) a means for authentication from outside a local area network, including a:

  - preprogrammed password that is unique for each connected device; or
  - requirement that a user generate a new means of authentication before gaining first-time access; or

  (b) compliance with requirements of federal law or regulations that apply to security measures for connect devices.

Protections

You Should Implement

Incident Response Plans (IRPs)

- **Why it's necessary**
  - FTC: a reasonable plan, reasonably followed, may be the difference for a regulatory action.
  - SEC: recent enforcement actions have analyzed IRPs.
  - Federal Reserve/OCC/FDIC: 36-hour rule.
  - Insurance: an IRP is becoming mandatory by underwriters.
  - Reputational harm: consumers and other third parties increasingly intolerant of a botched response.
  - Business continuity: responding as important to survival than defending.

Risk Assessments (RAs)

- **FTC investigations typically ask:**
  - "Describe in detail any type of hacking incident or system compromise — including your internal or external network, and any other network configuration, devices, [and IoT]."
  - "Describe your RA process, including but not limited to how the nature and level of the risk is assessed and recorded, the frequency of RA, and how you respond to . . . identified risks [including for IoT]."

Responses

You Should Have Ready

Written Information Security Programs (WISPs)

- **Cybersecurity Laws**
  - Ohio, New York and Utah laws have WISP requirements as a 'safe harbor'
  - Oregon, Massachusetts and Rhode Island require WISPs, and that includes administrative, technical and physical safeguards
- **Organizations required to**
  - "evaluate and adjust the [Written] Information Security Program *in light of any changes to [your] operations or business arrangements* ...." i.e., emerging technologies, like IoT.

About Armstrong Teasdale

The A(T) Team

ARMSTRONG TEASDALE'S PRIVACY AND DATA SECURITY TEAM

Jeffrey Schultz
ST. LOUIS | PARTNER
jschultz@atllp.com
314.259.4732

Scott Galt
ST. LOUIS | PARTNER
sgalt@atllp.com
314.259.4709

Romaine Marshall
SALT LAKE CITY | PARTNER
rmarshall@atllp.com
801.401.1604

Lucas Amodio
ST. LOUIS | SENIOR ASSOCIATE
lamodio@atllp.com
314.259.4722

Dustin Berger
DENVER | SENIOR ASSOCIATE
dberger@atllp.com
720.722.7197

Gabriela Baeza-Stout
ST. LOUIS | ASSOCIATE
gbaezastout@atllp.com
314.386.6871

Jared Keetch
SALT LAKE CITY | ASSOCIATE
jkeetch@atllp.com
801.401.1615

Casey Waughn
ST. LOUIS | ASSOCIATE
cwaughn@atllp.com
314.259.4766

Overview of Armstrong Teasdale – Firm Information

For 120 years, Armstrong Teasdale has forged long-term relationships with clients large and small around the globe.

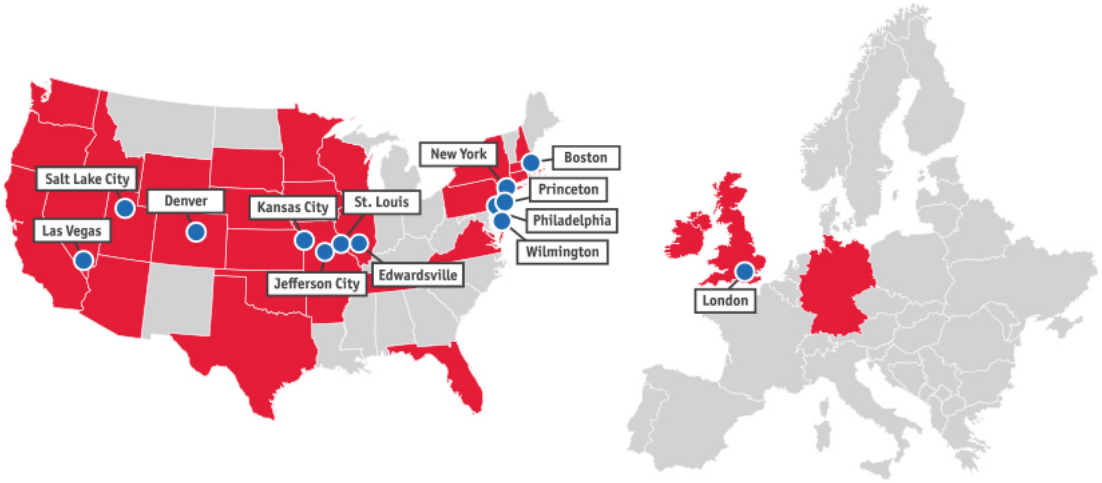
360+
— LAWYERS —

300+
— STAFF —

— SERVING OVER —
125+
FORTUNE 500 COMPANIES

— AM LAW —
200

With 13 offices across the U.S. and in London, our lawyers are licensed to practice in 30 states plus Washington, D.C., as well as in the U.K., Germany and Ireland.



**As of Dec. 2021*

Lucas Amodio

314.259.4722
lamodio@atllp.com

Scott Galt

314.259.4709
sgalt@atllp.com

Romaine Marshall

801.401.1604
rmarshall@atllp.com

Jeff Schultz

314.259.4732
jschultz@atllp.com