



Approaching Cybersecurity Law

A Guide for Information Security Professionals

David Jackson

November 20, 2018

ISSA National Capital Chapter Meeting

Biography



Mr. Jackson is a member of the ISSA DC and NOVA chapters, and he holds CISSP, CEH, and CIPP certifications. He works as a regulatory attorney for a government contractor in the Washington DC area, and he is a regular contributor to the ISSA Journal. Mr. Jackson has a J.D. from the University of Kansas, and an LL.M. from the University of Arkansas.

Abstract

Approaching Cybersecurity Law - A Guide for Information Security Professionals

Cybersecurity law is a confusing subject. There are many different types of laws, which affect different organizations in different ways. This presentation provides insight in how to consider cybersecurity law as a discipline, and dispels the notion that law as a tool is all powerful. In fact, law can be quite limited, slow, and backward looking. Finally, the presentation ends with a discussion of the future of cybersecurity law, and how to identify the coming trends.

Tonight We Will Cover:

- How to View Cybersecurity Law
- Law is Not All Powerful – It's Imperfect
- Future of Cybersecurity Law

Topic 1

How to View the Cybersecurity Law Landscape

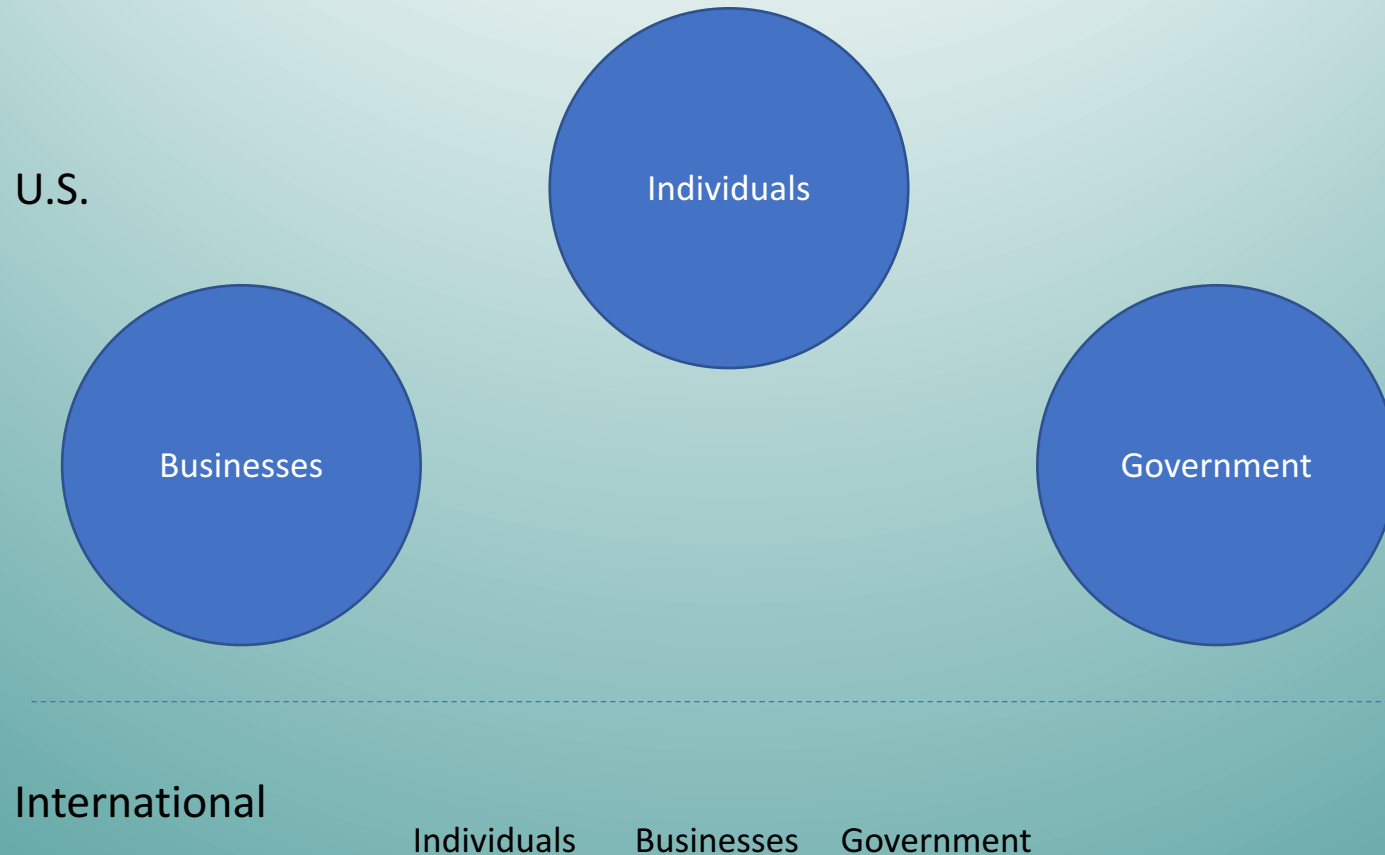
Most Cybersecurity Law is Learned for the CISSP Exam

- CISSP Domain 1 – Law
 - Cybercrime
 - Intellectual Property
 - Privacy
 - Different Legal Systems

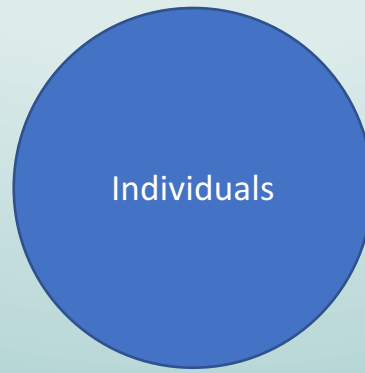
Challenges in Understanding the Law in CISSP Domain 1

- It's confusing. A hodgepodge of topics.
- It's overwhelming. A lot of foreign information.
- It needs some organization. A roadmap.

Better to View Cybersecurity Law by Who is Impacted



Laws that Impact Individuals



- 2 Categories of Individuals
 - General Public
 - Criminals
- Cybersecurity laws are designed to separate the Criminals from the General Public
- But also, perhaps, to encourage E-Commerce

Laws Separating Individuals and Criminals

- Hacking Governments or Banks
- Organized Crime
- Selling Trade Secrets
- Identity Theft
- Selling Passwords to Accounts

Laws Encourage E-Commerce?

- Why E-Commerce
 - Reduces Costs
 - Improves Accuracy
 - Faster
- Why Encourage
 - Framework for Global Electronic Commerce (90s)
 - Don't want to kill the "Goose that Lays the Golden Egg"
- Not Explicitly Stated
 - More of an Inference – I'm suggesting that the law encourages e-commerce.

Laws that Impact Businesses

Not all businesses are affected by all cybersecurity laws – Only Certain Businesses...



- Telecom
- Health Care
- Government Contractors
- Banks

Laws that Impact Businesses con'd

... And only Certain Types of Data

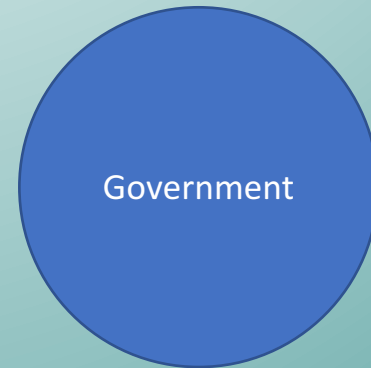
- Health Information
- Financial Information
- Video Records (Blockbuster to Netflix)
- School Records
- Government Data

Business and Government have a Bifurcated Relationship

- Partnership
 - Share Data
 - Work Together on Investigating Threats
- Regulation
 - Enforce Regulations
 - Penalize Violations
- The lines can get blurred!

Laws that Impact Government

- Specific Government Agencies
 - Law Enforcement
 - Military
 - Executive Agencies
- How laws impact the Government
 - Limit power within the US
 - Defend US Interests internationally



Which Parts of Government have their Power Limited

- Law Enforcement
 - Surveillance
- Military
 - Domestic Occupation
- Government Agencies
 - Privacy Act
 - Administrative Procedures Act

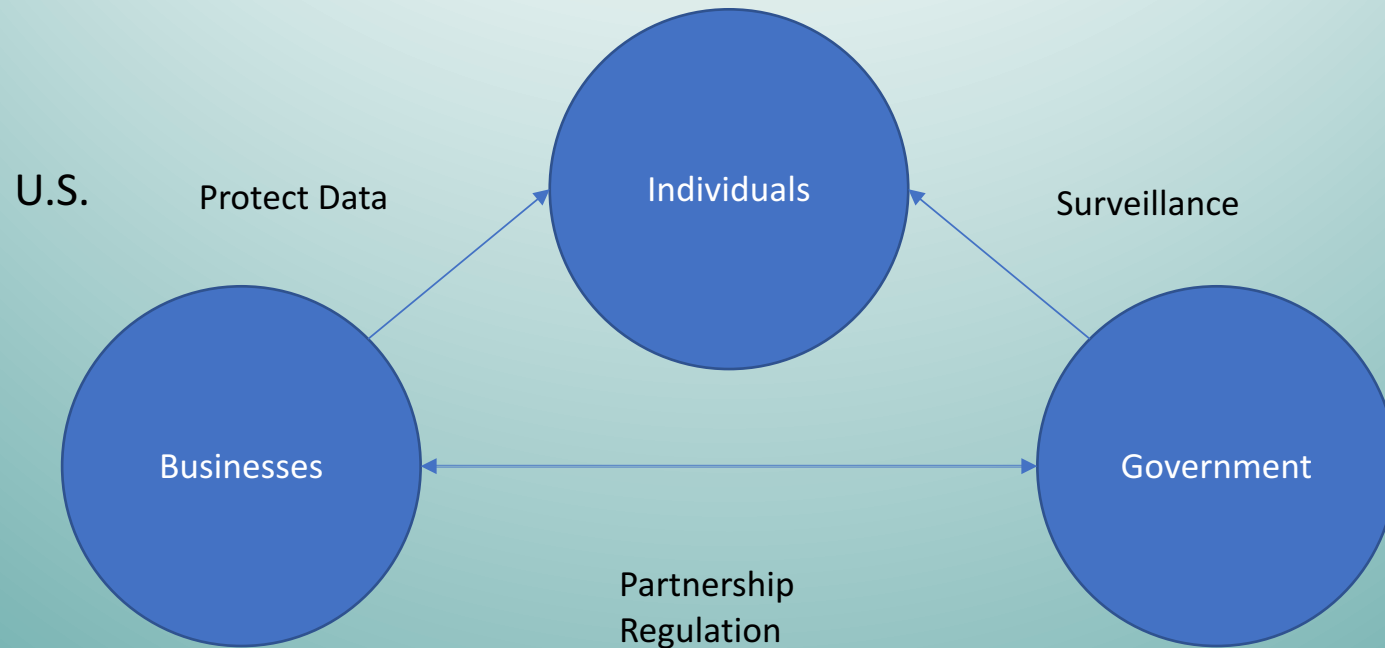
How does International fit into this model of Cybersecurity Law?

- In a global economy, and in an electronic world, the borders are less restrictive.
- Same group of participants
 - Individuals
 - Businesses
 - Government
- Primarily US Government facilitated relationship
- Can be difficult to enforce across borders

What Types of Legal Issues Impact International?

- Individuals
 - Extradition
- Businesses
 - Export Controlled Trade
 - Trade Secret Theft
- Governments
 - Cyberwar
 - Cyberterrorism
 - Cyberespionage

Putting it all together into a Cybersecurity Law Landscape



International

<u>Individuals</u>	<u>Businesses</u>	<u>Government</u>
Extradition	Export Control	Cyberwar

Topic 2

The law isn't All Powerful – It's Imperfect

Law isn't All Powerful – Let's Dispel some Myths

Myths

- Law can apply everywhere
- Law applies to any new situation
- Law keeps up with the changes of the times

Actuality

- Law is limited
- Law is backward looking (at first)
- Law is slow to change

The Law is **Limited** – How is it Limited?

- The law is limited to certain people and certain situations
- For our purposes, the journalism questions may be more useful to understand those limitations:
 - **Who** – the party / parties involved
 - **What** – the actions in question
 - **Where** – the jurisdiction
 - **When** – the circumstances around the actions
 - **How** – the enforcement mechanism
 - **Why** – the policy reasons

Let's use the Computer Fraud and Abuse Act as an Example

- Computer Fraud and Abuse Act (CFAA) was the first big cybersecurity law. (18 U.S.C. § 1030)
- Criminalizes unauthorized access to government and financial institution computers.
- The DOJ has a practice manual on CFAA to provide more guidance on prior case law.
- The actual law is somewhat convoluted, so I'm abridging the law slightly for our discussion.

Here's the CFAA in Simplified Form

- Whoever, intentionally accesses a computer without authorization, or exceeds authorized access,
 - and thereby obtains information contained in a financial record of a financial institution...
 - or information from a department or agency of the United States, ...
- shall be punished ...by a fine or imprisonment...
- The U.S. Secret Service, the FBI, the Secretary of Treasury and the Attorney General shall have the authority to investigate.

How the CFAA can be analyzed with the journalism questions

- **Who** – Whoever
 - Natural Person (versus a legal person – Corporation)
- **What** – Intentionally Accesses a Computer
 - Without authorization
 - Exceeds authorization
- **Where** – Federal (implied – 18 USC)
- **When** – obtain information from:
 - federal government
 - financial institution
- **How** – Fines Prison / Secret Service, Treasury, FBI/AG
- **Why** – not relevant – policy arguments are weaker
 - 1980s - movie War Games

Where is the CFAA Limited?

- The CFAA applies only to certain situations
 - Federal Government / Financial Institution computers
 - Without Authorization / Exceeds Authorization
 - Federal Law Enforcement Investigates

Where the CFAA Does Not Apply

- Not your neighbor's computer.
 - (not a federal or bank computer)
- Not filing your state tax return.
 - (authorized)
- Not mistyping a URL into your web browser.
 - (not intentional)

Law is Limited - In Conclusion

- Only certain :
 - People
 - Locations
 - Activities
 - Circumstances
- Policy – the “Why” Doesn’t Really Matter.
- Key is Understanding the Limits.

Law Looks Backward (before it looks forward)

- Our legal system is based on **precedent** – what decisions came before – “Stare Decisis” (let decision stand)
- This forces every legal analysis to start with what law came before.
- How does this new situation fit with a prior legal issue?

Let's Return to the 1990s for an Example – AOL and “Spam”

- AOL was a major target for “spam” (now known as unsolicited commercial email).
- In 1990s, AOL sued spammers as part of its anti-spam strategy.
- It was difficult because the laws didn't easily address this new phenomenon.
- Expensive to Prosecute.
- BTW, I worked at AOL fighting spam in the 1990s.

AOL Won Lawsuits in Part Using “Trespass to Chattels”

- Definitions
 - Tort – civil wrong – intentional - Old Common Law (from England)
 - Chattels are things.
 - Trespass in this case = **Interference** (“damages suffered by reason of the loss of its use.”)
 - See e.g., *America Online, Inc. v. IMS et. al.*, 24 F. Supp. 2d 548 (E.D. Va., 1998)
- So, the law that was violated was
 - Someone had interfered with the use and enjoyment of someone else’s things that caused damage that could be calculated. (this is highly simplified language)
- For AOL –
 - Spammers had interfered with AOL’s use and enjoyment of its mail servers to serve email to its user base, and cost AOL time and money to process the extra emails, and “burdened their equipment” (mail servers)

Challenges to this Legal Theory

- Spam email is just email. You provide the service of email to your users, it goes with the territory.
- 1st amendment violation? No state action.
- Increased cost of mail servers could be attributed to the increase in membership- more users, more mail servers – not this email.
- Interference required showing volume that damaged business – what caused the burden to the equipment?

The Law Looks Forward and Passes CAN-SPAM

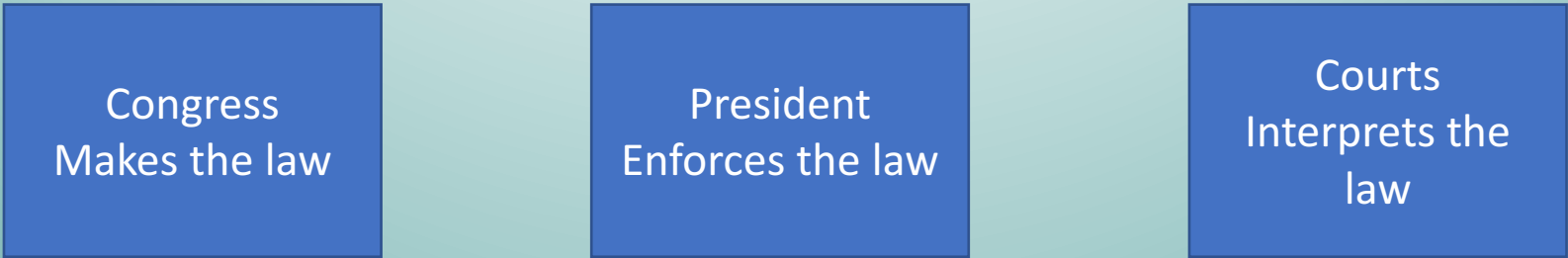
- A few years later, Congress passes CAN-SPAM (Pub. L. 108-187, 2003).
- Changes the legal question from interference to unsolicited.
- Drops the Volume analysis requirement.
- Unwanted is enough.
- Damages quantified by email as a unit and not in aggregate.
- But, Law looks backward before it can look forward.

The Law is Slow to Change

- One of the biggest challenges to addressing cybersecurity law needs, is that the lawmaking process is so slow.
- Cybersecurity threats arise quickly, and it can be frustrating to seek legal action only to find that there is no easy fix – no applicable law for a situation.
- In order to talk about why the law is slow to change we need to look at how laws are made.

How Laws are Made – a Civics Review

- U.S. Constitution: Three Branches of Government



Congress
Makes the law

The diagram consists of three blue rectangular boxes arranged horizontally. Each box contains text describing a branch of the U.S. government. The first box on the left is labeled 'Congress' and 'Makes the law'. The middle box is labeled 'President' and 'Enforces the law'. The third box on the right is labeled 'Courts' and 'Interprets the law'.

President
Enforces the law

Courts
Interprets the
law

- There's a Balance of Powers

How the Laws Are Made among the Three Branches

- But it is a serial process too:



- Of course, the process is not strictly serial - Courts can review statutes.
- The point is that making a law is a journey through the three branches and their law making processes.

Legislative Process – Why Are There so Many Laws in Congress?

- Let's review the numbers based on “cyber*” in this current Congressional session.
- Bill is proposed in House (491)
- Committee (132)
 - Hearing
 - Report
 - Vote
- Full Floor Vote (98)
- Same Process Senate (27)
- President signs (19) – then it becomes law.
- Many bills are proposed, but very few become law!

Regulatory Process – How Government Agencies Make Laws

- Federal Register as Paper of Record (www.federalregister.gov)
- The process to create a new regulation:
 - Unified Agenda (www.reginfo.gov)
 - Notice of Proposed Rule Making
 - Notice and Comment Period (www.regulations.gov)
 - Final Rule
- There are substeps within this process. The numbers vary depending on the issue and how many comments are received.
- Comments from the public can affect the regulation.
- Only the Final Rules matter! And only after their effective date!!

Judicial Process – How Courts Determine Whether a Law is Good?

- In order to sue- need a case or controversy
- There are three levels of review:
 - District Court
 - Court of Appeals
 - Supreme Court
- Start at District Court, then appeal, and appeal.
- This three level systems applies to State Courts and Federal Courts
- Note: State Supreme Court decisions can be reviewed by the U.S. Supreme Court. Miranda v. Arizona for example.

Judicial Process with Numbers

2409 Federal cases involving cyber (approximately)

- District Court (1,610) 67%
- Court of Appeals (562) 23%
- Supreme Court (237) 10%
- Only a few go to the Supreme Court.
- The key is that the case decision only applies to the jurisdiction of the court.

Law Making is a Slow Process

- Legislative – 2 year cycle
 - New Congress – starts over
- Regulatory – 4 -8 year cycle
 - New Administration – start over?
- Judicial – 6 – 15 years
 - Each case can take months/years to be decided at each level.
- Very, Very slow. 10 to 20 years in total.
- A lot of proposals, very few new laws.
- Very political too.

In Conclusion: The Law is Not All Powerful.

- The Law is Imperfect:
 - The Law is Limited – certain people, certain situations
 - The Law Looks Backward – precedent – what legal issues happened prior?
 - The Law Slow to Change – the lawmaking process can take years
- The reality is that the law is often the antithesis to technology
 - Technology can Apply Broadly
 - It Looks Forward
 - It is Very Quick to Change
- This dichotomy between Law and Technology creates tension between the Legal and Technology communities

Topic 3

What is the Future of Cybersecurity Law

The Future of Cybersecurity Law – Where do We Begin?

- In order to understand the future of cybersecurity law, we start with the relationship between technology, business, and law.

Technology

Business

Law

- As I mentioned technology changes quickly. The law slowly.
- There are actually 2 lags between law and technology.

1st Lag – If Change were to Start Simultaneously, Law would Lag Behind

- Technology changes quickly – Moore's Law 18 mo.
- Business changes a bit slower – 5 – 10 years to start a new business and achieve scale.
- Law changes very slowly – 10 – 20 years as previously discussed.

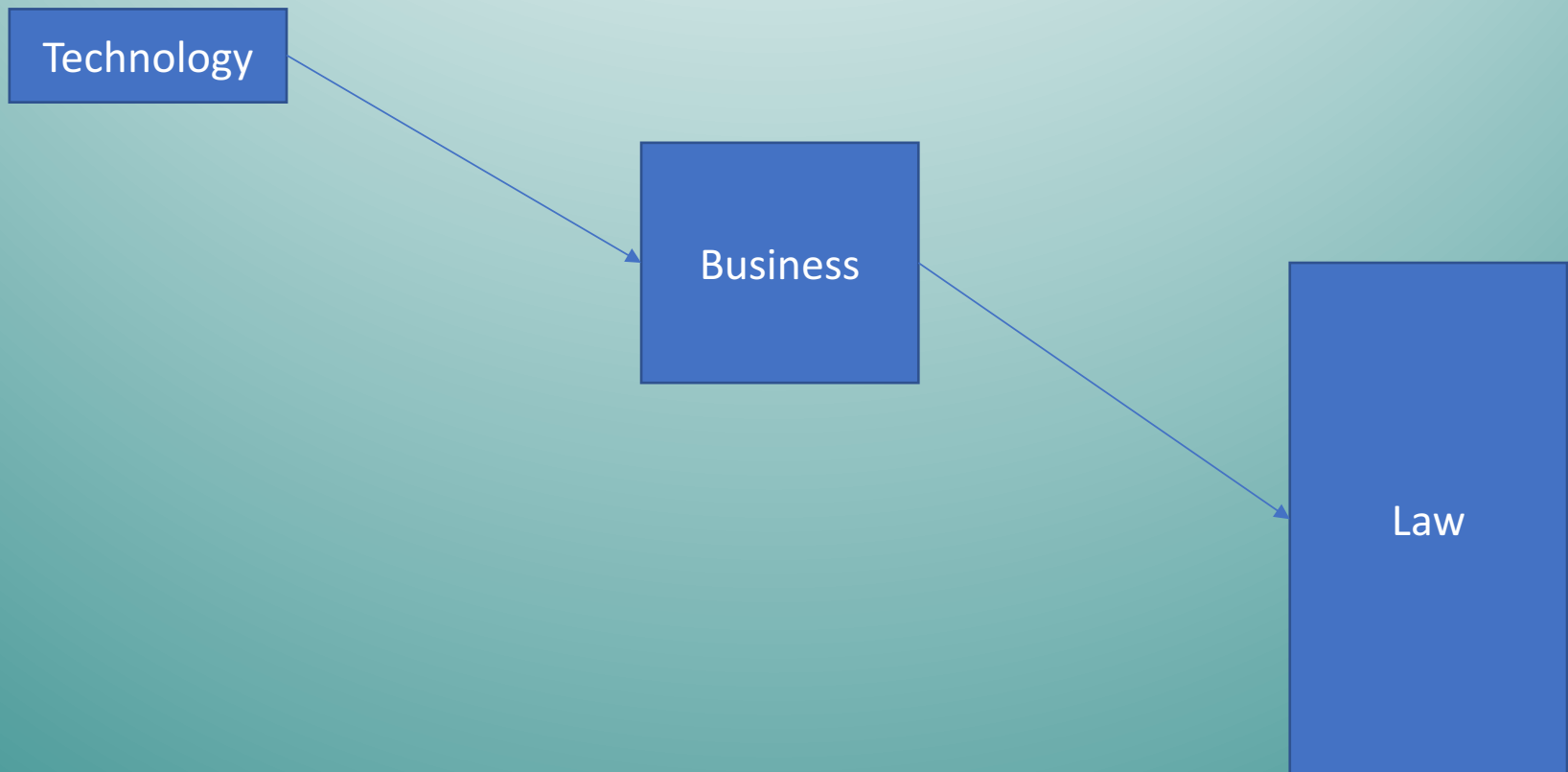
Technology

Business

Law

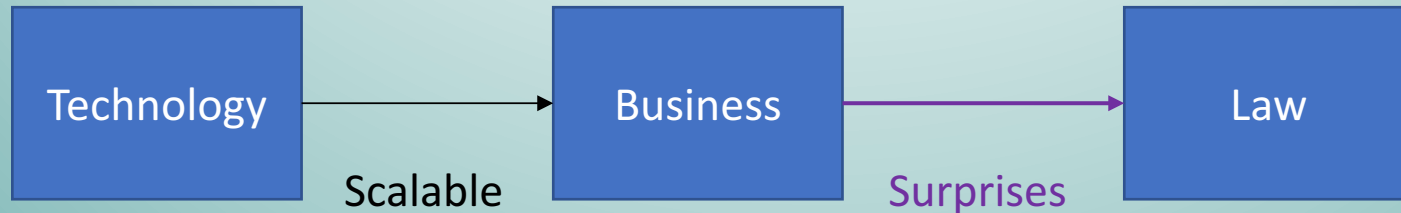
2nd Lag – Change is also Serial

- You have to have technological innovation first. So the lag is cumulative.
- Cybersecurity law development lags far behind technology innovation.



The future of Cybersecurity Law is in the Nexus of Business and Law

- Between technology and business is the idea of what can be monetized or commercialized. What is Scalable.



- What problems arise from scaling that Businesses can't address through technology? What are the **surprises**?
- That's the future of cybersecurity law. How to address the surprises.
- Email as an example- RFC822 (1980), ISPs (1990s), Spam (late 90s), CAN-SPAM (2003).

New Cybersecurity Laws to Know

By Jurisdiction:

- California
- Supreme Court
- FTC
- Regulatory Agencies
- Europe
- Congress

California – Pushing the Federal Envelope in 2018

- **Internet of Things law** (Security of Connected Devices, SB 327, Cal. Civ. Code, Title 1.81.26, § 1798.91.04 et. seq.)
 - Manufacturers (not distributors)
 - Connected devices (IP or Bluetooth)
 - Reasonable security feature (nature and function of device)
- **California Consumer Privacy Act** (AB 375, Cal. Civ. Code, Title 1.81.5, § 1798.100 et. seq.)
 - Effective 1/1/2020
 - Consumers can request that business disclose the personal information collected and what has been done with that information. GDPR like.
 - In response to Cambridge Analytica (Facebook is in California)
- **Net Neutrality law** (California Internet Consumer Protection and Net Neutrality Act of 2018, SB 822, Cal. Civ. Code, Title 15, § 3100 et. seq.)
 - Unlawful to block, impair, or degrade, lawful Internet traffic based on content, application, service, or device
 - For both fixed (broadband) and mobile Internet service providers

A few overall thoughts:

- California tends to be Progressive – embracing changes first.
- All technology roads lead to California. (Silicon Valley)
- Inferred Political Fight between California and the U.S. Government.

Supreme Court

- **Carpenter v. U.S.** (No. 16-402, 2018)
 - Cell Site Location Information (12,898 location points over 127 days)
 - Question – reasonable expectation of privacy - cell phones as electronic trackers in your pocket
 - Court Ruled: Law Enforcement needs a warrant for cell location data
 - Surveillance – 4th Amendment and “new” technology
- **CareFirst, Inc. v. Attias** (No. 17-641, 2017)
 - Cert Denied Feb. 20, 2018
 - Lower Court Ruling stands (Attias v. CareFirst, Slip. Op. 16-1708, DC Ct. App., 2017)
 - Court held that damages could be awarded for threat of future identity theft resulting from a data breach.
 - Unusual – courts HATE to speculate about future harm - the “maybes”
 - So, what does this mean for Cybersecurity Insurance claims / data breach costs?

FTC and Cybersecurity

- Unfair or Deceptive Acts or Practices in or Affecting Commerce is a broad umbrella of authority under §5.
- **FTC v. Wyndham** (3rd Cir. No. 14-3514, 2015)
 - FTC – has pursued cases against companies with deficient cybersecurity practices
 - Wyndham had three data breaches – it failed to use readily available security measures (like firewalls) – claimed to be the victim
 - Wyndham claimed FTC didn't have the authority to regulate cybersecurity matters.
 - Businesses must protect customer personal information, and FTC can pursue cases where the businesses don't.
- **LabMD v. FTC** (11th Cir., No. 16-16270, 2017)
 - Facts of this case are odd – billing manger for a lab with a file sharing program / security company downloaded personal data of 9,300 consumers / sent the information to the FTC
 - FTC claimed a broad failure of LabMD to protect personal data, but the claim was too broad. The cease and desist order must be specific to the case in point.
- Taken together, FTC has power to regulate cybersecurity in data breaches, but that power is proportional to the incident.

Regulatory Agencies

SEC

- Commission Statement and Guidance on Public Company Cybersecurity Disclosures (83 FR 8166, Feb. 26, 2018)
 - Must inform investors about cybersecurity incidents and risks based on:
 - Materiality of risk and
 - Importance of compromised information

DOD

- DOD Guidance for Reviewing Systems Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented (83 FR 17807, Apr. 24, 2018)
 - DOD drafted guidance for contractors to use in implementing 800-171 and is seeking comments. Admission that there are challenges with meeting these requirements? From both sides?
 - Consider the bifurcated role of Government and Business – sharing information as a partnership and regulatory enforcement.

Europe

General Data Protection Regulation (GDPR) (EU) 2016/679

- Implementation Date: May 25, 2018
- Privacy Shield – Current U.S. Data Sharing Scheme - being sued in European Court – like Safe Harbor?
- Data Security Concerns
 - Processing – broad
 - Pseudonymized/Anonymized Data – assumes traceability
 - General Security Requirement – Art 32, CIA Triad
 - Monitoring and Profiling (AI)

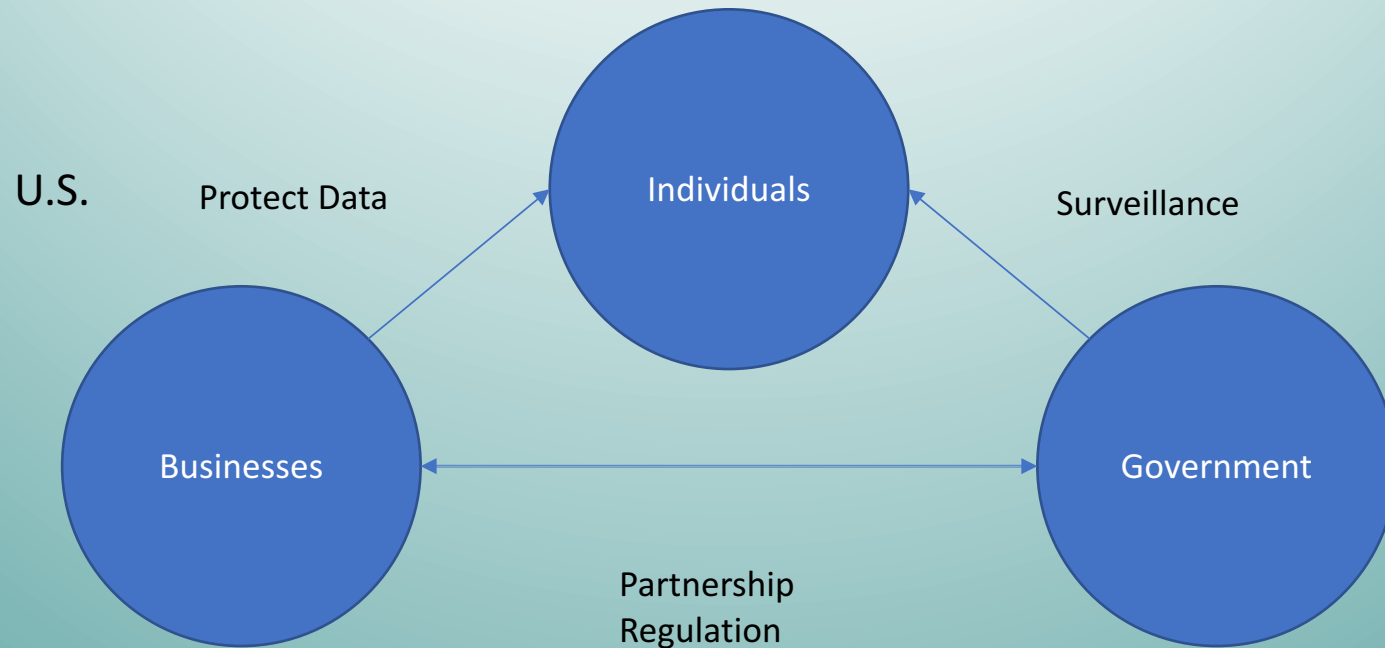
Congressional Actions

- In this Congress – No BIG changes
 - NIST Small Business Cybersecurity Act (Pub. L. 115-236, Aug. 14, 2018)
 - Congress directs NIST to develop Cybersecurity Framework for Small Businesses out of existing funding
 - DHS - Cybersecurity and Infrastructure Security Agency Act of 2018 (H.R. 3359, Pub.L. 115-TBD , Nov. 16, 2018)
 - Reorganize the DHS Cybersecurity departments (internal change in operations)
- In the previous Congress – a few changes
 - Cybersecurity Information Sharing Act 2015 (Pub.L. 114-113)
 - Creates framework for businesses to share cyber threats with the Government who can report back to the whole subscribership
 - Trade Secrets Act 2016 (Pub. L. 114-153)
 - Creates a federal right of action for trade secret theft cases.
- Point – laws change slowly and infrequently.

New Business Risks on the Horizon – Looking into a Crystal Ball

- CEH Army
 - Risk - Hack Back?
 - Private industry with offensive capability
- Botnets
 - How to assess liability – Masters, Bots, Networks?
 - DOJ Guidance 2015 easier prosecution – subpoenas can be filed centrally
- IoT
 - Risk of Insecurity – California ahead of time, or right on time?
 - Wearable tech – time and location information – cell phones as homing devices – what about Fitbits?
- Blockchain
 - Bitcoin - Financial Regulation- in a decentralized environment?
 - Supply chain / e-contracts – putting attorneys out of business?
 - Traceability / Integrity - Risk of unplanned forking?

Revisiting the Cybersecurity Law Landscape



International

<u>Individuals</u>	<u>Businesses</u>	<u>Government</u>
Extradition	Export Control	Cyberwar

Perennial Issues that Arise in the Cybersecurity Law Landscape

- Individuals
 - Surveillance – 4th Amendment – Warrants?
 - E-Commerce Encouragement – Risk of data breach
- Business
 - Regulation – how far to go to increase security
 - Partnership– how much sharing, what can change over time
 - International Business Transactions – exports, foreign policy
- Government
 - International Criminal Enforcement – extradition, international surveillance, protecting trade secrets
 - Just War in Cyber Times – borderless conflict - a time beyond the nation state?

In Conclusion

- Cybersecurity law can be organized by who is impacted by the law – Individuals, Businesses, Government, International
- Law as a cybersecurity tool is not all powerful – it's limited, backward looking, and slow to change. The opposite of technology.
- The future of Cybersecurity Law lies in the nexus between technology, business, and law. We discussed: (1) the new laws in 2018, (2) the what's coming next, and (3) the what's always at issue.

Additional Resources

- Habeas Data, Privacy vs. Rise of Surveillance Tech, Cyrus Farivar, Melville House Publishing, 2018.
- Cybersecurity Law, Jeff Kosseff, John Wiley & Sons, 2017.
- Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation, Eric A. Fisher, December 12, 2014, CRS Report R42114, Congressional Research Service.
- Websites
 - www.congress.gov (All Legislative Actions)
 - www.federalregister.gov (Daily Newspaper for Agencies)
 - www.ncsl.org (Cybersecurity Research at State Level)



Thank You!

David Jackson

davjackson@mindspring.com

202-423-6237