

Compliance and Vendor Management

September 19, 2023
Washington, D.C.



Panelists



Bernadette Chala
Chief Legal Officer,
Arbonne



Shea Leitch
Of Counsel,
Data Privacy, Cybersecurity &
Digital Assets

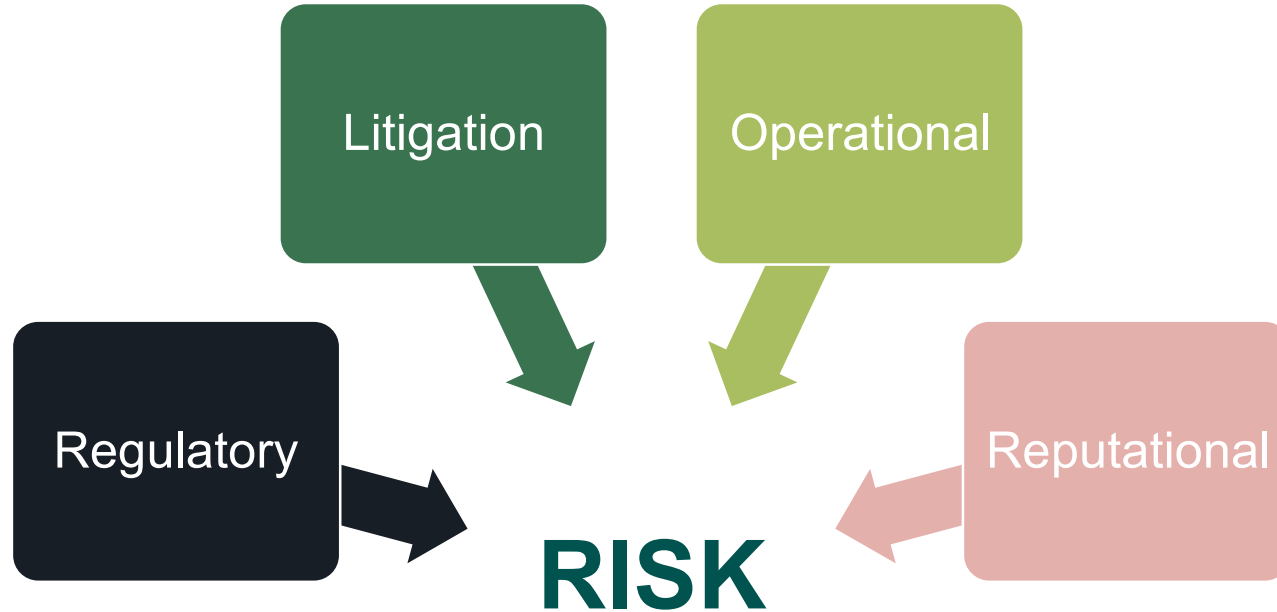


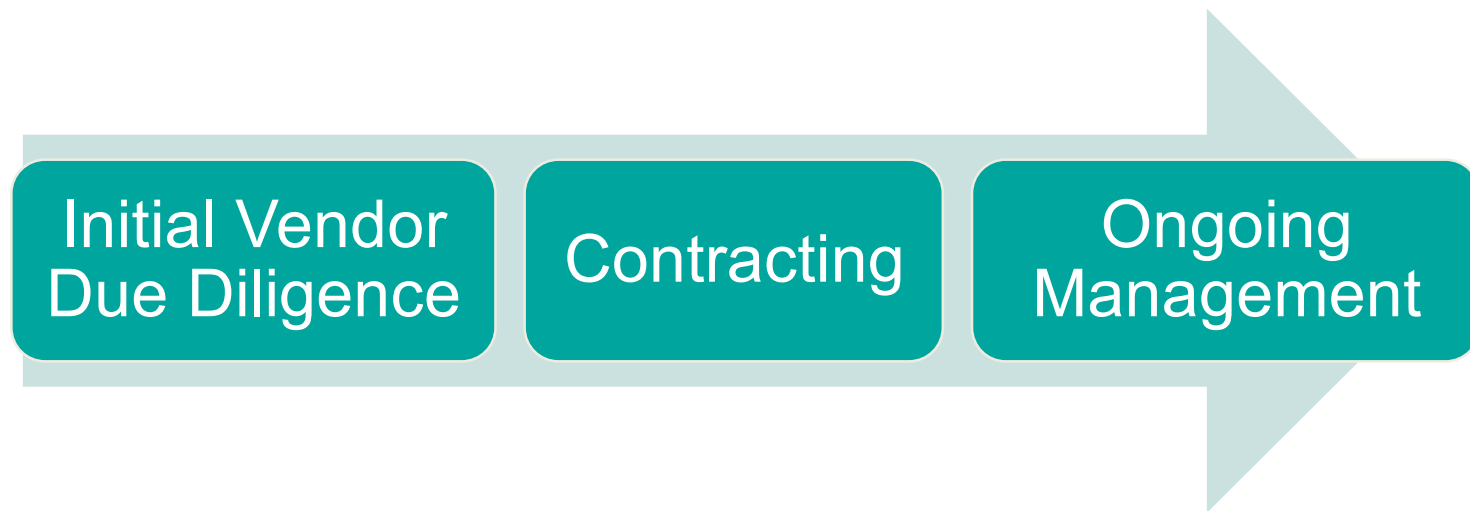
Elizabeth A. Spencer Berthiaume
Associate,
Data Privacy, Cybersecurity &
Digital Assets



Meghan Quinn
Senior Associate,
Litigation

Why does this matter?



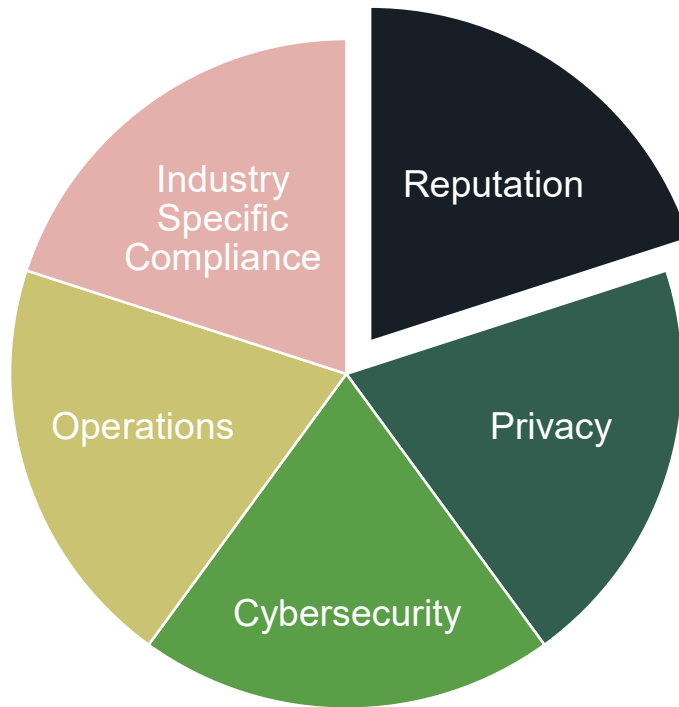


Initial (Pre-Contract) Vendor Due Diligence

Why should I vet my vendors?

- Practical considerations
 - Identify and allocate risk
 - Risk-based decision making
- Legal Requirements
 - State omnibus privacy laws
 - State or federal legal or regulatory security requirements
 - Industry-specific requirements
 - Contractual requirements
- Risk Mitigation
 - Reduce risk of data breach
 - Industry best practices

Topics in a Vendor Due Diligence Review



■ Vendor Security Controls

- Does vendor have appropriate security controls in place?
 - Consider requiring proof of recognized security certifications:
 - ISO 27001
 - SOC 2, Type II

■ Vendor Data Use Practices

- Is vendor secondary use permitted / expected?
- Will data be combined with other parties' data?
- Whether these are permissible practices will depend on:
 - What secondary uses are anticipated
 - Laws applicable to data processing activities

- State Omnibus Privacy Laws:
 - Specific audit requirements
 - Contractual requirements
 - In effect: CA, CO, CT, & VA
 - Upcoming: FL, IA, IL, IN, MT, OR, TN, TX, & UT
- Non-U.S. Jurisdictions:
 - Generally more complex requirements
 - Potential extraterritorial reach
 - Examples: UK-GDPR, EU-GDPR, LGPD (Brazil), PIPEDA (Canada), etc.
- Industry Specific Requirements:
 - Financial Institutions
 - Healthcare
 - Insurance
 - Critical Infrastructure
 - Etc.
- Industry Standards & Best Practices:
 - NIST
 - ISO

- Create a Vendor Management Program
 - Written vendor management policies and procedures
 - Appropriate to the size, industry, and type of data handled by the organization
 - Internal Vendor Onboarding Form
 - Include Key Review Topics
 - Identify Risks & Mitigation Steps
 - Example: SPI processing vendor has resources operating out of a non-U.S. jurisdiction. Mitigate risk by only allowing those resources to access Company systems through a virtual desktop that doesn't permit downloads or screenshots. Document this mitigation step.
 - Internal Vendor Management Team
 - Representatives from various stakeholders groups like: Operations, IT, Cybersecurity, Privacy, Procurement, Legal, etc.
 - Clear approval process.
- EARLY PREVIEW: Contracting Standards

Scenario 1: The Rogue Business Team

The mobile app development team found a great online “whiteboard” collaboration tool. A manager on that team creates an account, accepted all the click through agreements, and created sub-accounts for her team members without consulting any other group.

Her team now has access to the online tool where they upload various types of non-public information related to their company (pre-launch materials) as well as personal information of employees.

Contracting

Scenario 2: Embedded Hyperlinks

A SaaS provider's standard form is a Purchase Order that incorporates hyperlinks to the provider's online Terms of Service and Privacy Policy. Legal is concerned that these online documents can change at any time without notice to the organization and later incorporate unfavorable terms.

- Description of Services
 - Remedies if Services do not meet expectations
- Data Handling
 - Processing and use limitations/destruction of data
- Data Breach Response
- Audit Rights
- Key Addenda: Cybersecurity Standards & DPAs
- Representations & Warranties
 - Compliance with laws
- Indemnity
- Limitation of Liability
- Termination

Scenario 3: The Moving Target

The Customer Experience team is rushing to sign an agreement with a service provider to build out a new product for customers. The proposed use case is narrow and includes access to customer personal information such as name and email.

However, if the service provider performs well, there is an expectation for additional use cases to be added that includes sensitive personal information such as government IDs and financial information. If the agreement is not signed ASAP, the organization will lose out on a hefty discount.

The service provider's form agreement is light and not favorable to the organization.

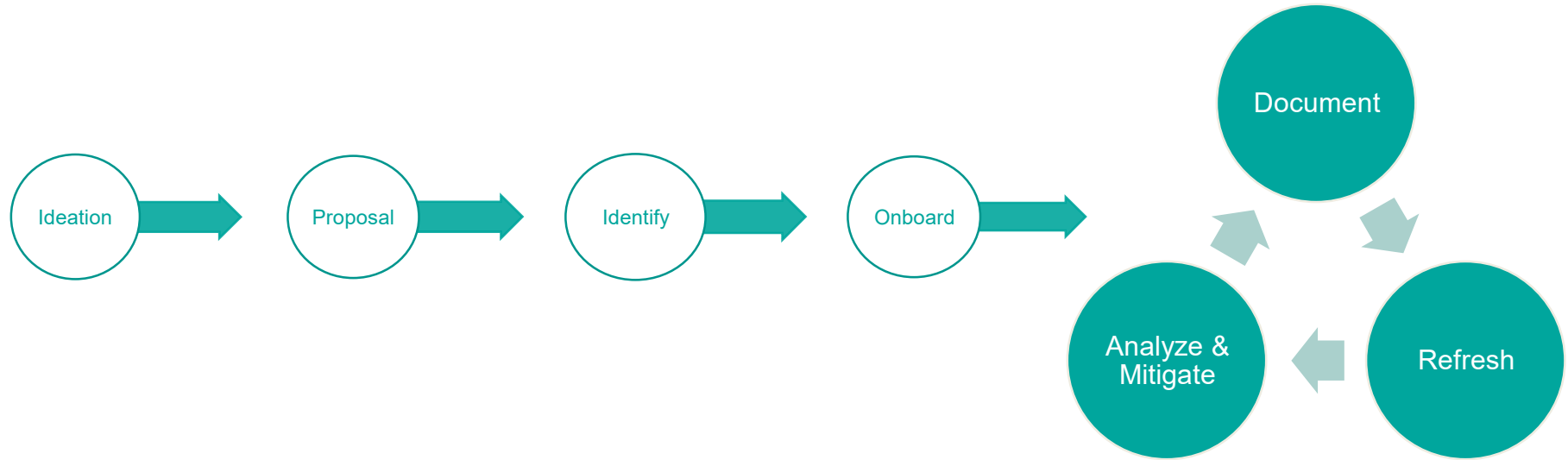
- Contract manager or team
- Form material provisions and Data Protection Addendum
- Vendor “levels” with corresponding contract “levels”
 - The more high risk the vendor or data processing, the stronger the contract / more stringent vetting requirements.
- Contract Logging
 - Know when renewals are due
 - Incorporate the latest required language at the most advantageous time
 - Roadmap for compliance with statutory requirements
 - Store historic copies of agreements

Scenario 4: Not Enough Spend

The procurement team is attempting to negotiate an agreement with a new data analytics provider. The provider is refusing to negotiate their form agreement because the organization only bought an entry-level package so the cost of the services does not exceed \$20,000.00.

Ongoing Management

Basic Vendor Management Program



ANALYZE

- Identify Changes in Scope
 - Data Types & Data Quantity
 - Data Uses
- Changes in Cybersecurity Posture
 - Did they experience a breach?
 - Did one of their subprocessors (a 4th party) experience a breach?
- Changes in Contract Language
 - Has the contract language changed? For the better? Worse?

MITIGATE

- Are new technical controls needed?
- If vendors are classified in tiers by risk level, should the internal vendor classification be changed?
- Does a new more stringent review need to be performed?
- Is stronger contract language needed?
- Does a new business use case need to be “walked back”?

- Annual or Bi-Annual Reviews
 - “Right Size” the program
 - For Riskier Vendors
 - Review more often
 - Take a closer look at documents
 - Test Vendor Systems & Processes
 - For Less Risky Vendors
 - Consider written confirmation that there are “no changes” from original review
- Ad Hoc Reviews
 - Example: Vendor experiences a data breach
- Create dedicated review personnel to avoid bogging down other teams

Scenario 5: “No.”

During contract negotiations, a potential HR service provider is refusing to agree to annual or bi annual reviews. They are otherwise okay with undergoing an initial onboarding review.



Thank You!

Abu Dhabi

Atlanta

Beijing

Berlin

Birmingham

Böblingen

Bratislava

Brussels

Cincinnati

Cleveland

Columbus

Dallas

Darwin

Denver

Dubai

Dublin

Frankfurt

Hong Kong

Houston

Leeds

London

Los Angeles

Madrid

Manchester

Miami

Milan

New Jersey

New York

Palo Alto

Paris

Perth

Phoenix

Prague

San Francisco

Santo Domingo

Shanghai

Singapore

Sydney

Tampa

Tokyo

Warsaw

Washington DC

Africa

Brazil

Caribbean/Central America

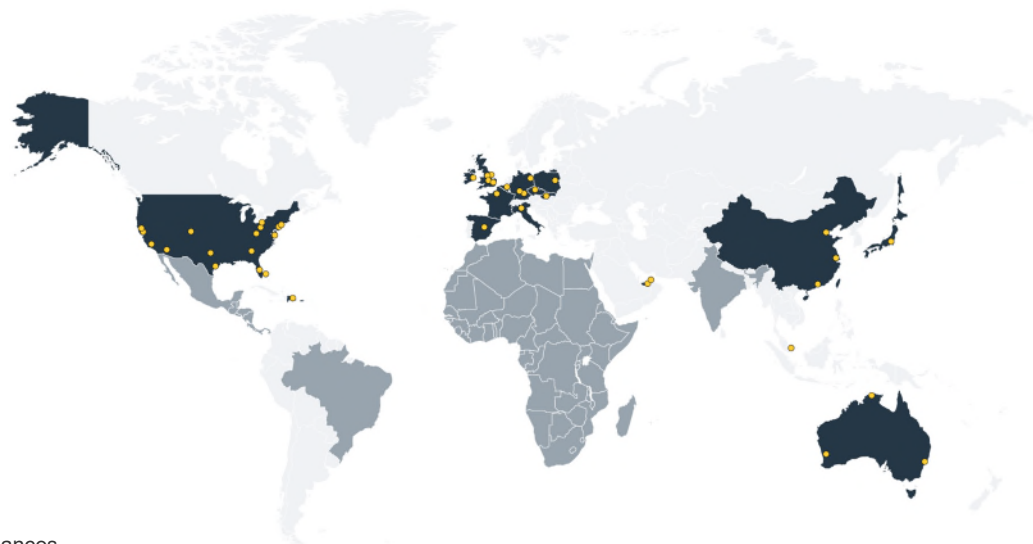
India

Israel

Mexico

Office locations

Regional desks and strategic alliances



Achieving Cybersecurity Resilience – Preparing Your Organization for Today's Regulatory and Threat Landscape

September 19, 2023



Your Presenters



Shea Leitch

Of Counsel, Washington, D.C.

T 614.917.7522

E shea.leitch@squirepb.com



Simon Taylor

Executive Vice President, Scottsdale, AZ

T 602.748.0957

E staylor@packetwatch.com



Ericka A. Johnson

Attorney, Washington, D.C.

T 1 608 772 7441

E ericka.johnson@squirepb.com

- Current Threat Landscape
- Legal and Regulatory Landscape
- Proactive Cybersecurity Preparedness
- Responding to Cybersecurity Incidents

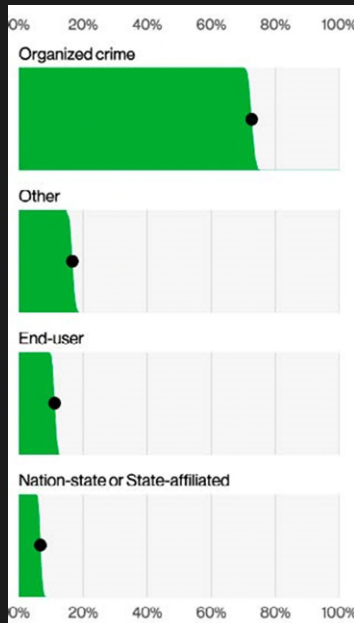
Current Threat Landscape



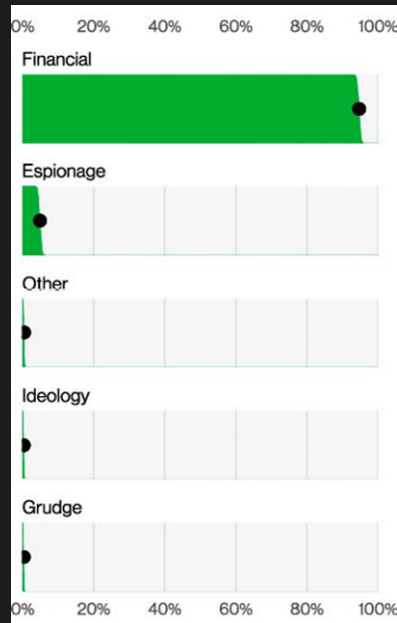
Threat Actor Landscape

- 200+ tracked adversaries – 33 newly identified in 2022
- Targeting Technology, Financial Services, Healthcare, Telecoms, Manufacturing, Academia, Government
- China adversaries the most active targeted intrusion groups
 - Intellectual property focus
- Russia adversaries continue military, psychological and hacktivist attacks
 - Affiliates still financially motivated
- Initial Access Broker (IAB) ads up 112%
- Majority of attacks still opportunistic

Types of Threat Actors



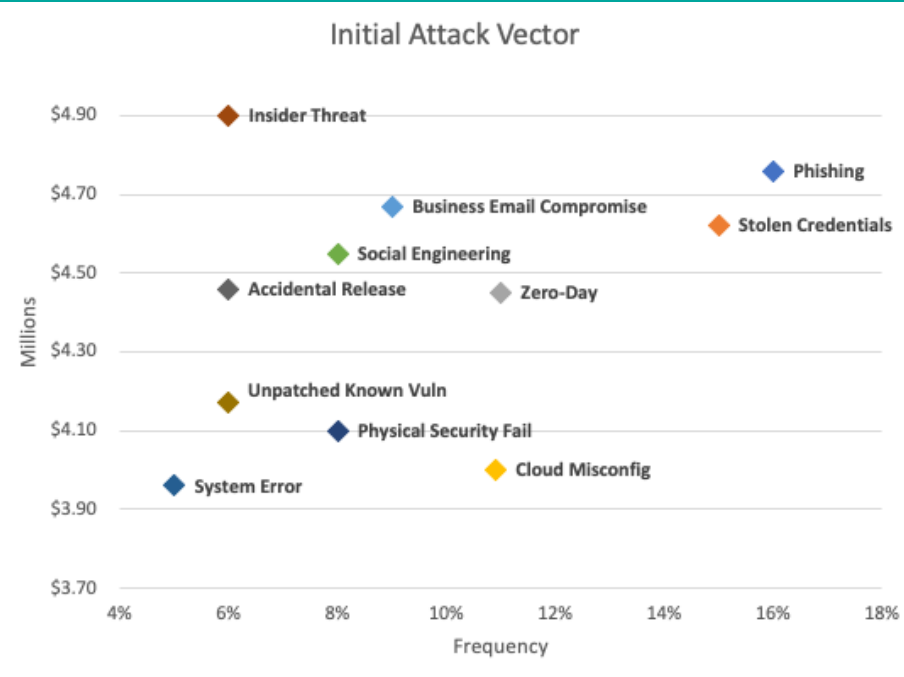
Threat Actors Motives



Source: Verizon DBIR 2023

Adversary Operations Increasingly Hard to Defend

- Adversarial breakout (achieve lateral movement) now averaging 79 minutes
- 71% of attacks are malware free
 - Prolific abuse of valid credentials
 - 50% increase in “hands-on-keyboard”
- Ability to quickly exploit zero-day/N-day vulnerabilities
 - Deep skills and deep pockets
 - Log4j, SolarWinds, Microsoft, Citrix, SonicWall, Fortinet, MoveIT, Apple
- MFA bypass becoming more common
 - Legacy protocols, social engineering, token capture, MFA fatigue, SIM swap



Source: Ponemon Institute LLC 2023

- Data theft and “double-extortion” campaigns
 - “Double extortion” model most common tactic among big game hunting (BGH) adversaries
 - 20% increase in data theft extortion without deploying Ransomware
- Cloud exploitation exploits grown by 95%
 - Cases involving cloud-conscious threat actors nearly tripled from 2021
- Growth in ‘Destructionware’
 - Remember Stuxnet (2010) and NotPetya (2017)
 - Russian *Prestige* and *RansomBoggs* wipers disguised as ransomware (Ukraine and supporters)
 - Amateurs using RaaS services and simply poor ransomware code effectively destructionware



Legal and Regulatory Landscape



Legal and Regulatory Cybersecurity Puzzle

- Patchwork of legal and regulatory security requirements:
 - Federal Security Requirements:
 - SEC Cybersecurity Disclosure Regulations
 - GLBA Safeguards Rule
 - HIPAA Security Rule
 - FCRA Security Requirements
 - CMMC
 - CIRCIA Critical Infrastructure Notification
 - State Security Requirements:
 - NYDFS Cybersecurity Regulations
 - Insurance Data Security Model Laws
 - Massachusetts Data Security Law
 - Connecticut and Ohio safe harbor laws
 - State laws requiring “reasonable” security
 - CCPA cybersecurity audit requirements



The “Reasonable” Security Approach

- Approximately twenty-two (22) states follow the “reasonable security” approach to data security in that they require businesses to maintain reasonable security procedures and practices to protect certain “personal information” from unauthorized access, destruction, use, modification, or disclosure. Examples:
 - California: Cal. Civ. Code § 1798.81.5
 - Florida: § 501.171(2), Fla. Stat.
 - Texas: Tex. Bus. & Com. Code Ann. § 521.052(a)



The Prescriptive Approach

- Massachusetts Standards for the Protection of Personal Information
- Oregon and New York (SHIELD Act)
- Minnesota, Nevada, and Washington - PCI DSS
- Amended FTC GLBA Safeguards Rule
- NY DFS Cybersecurity Regulations



**Proactive
Cybersecurity
Preparedness**



Assessing Cybersecurity and Implementing Appropriate Security

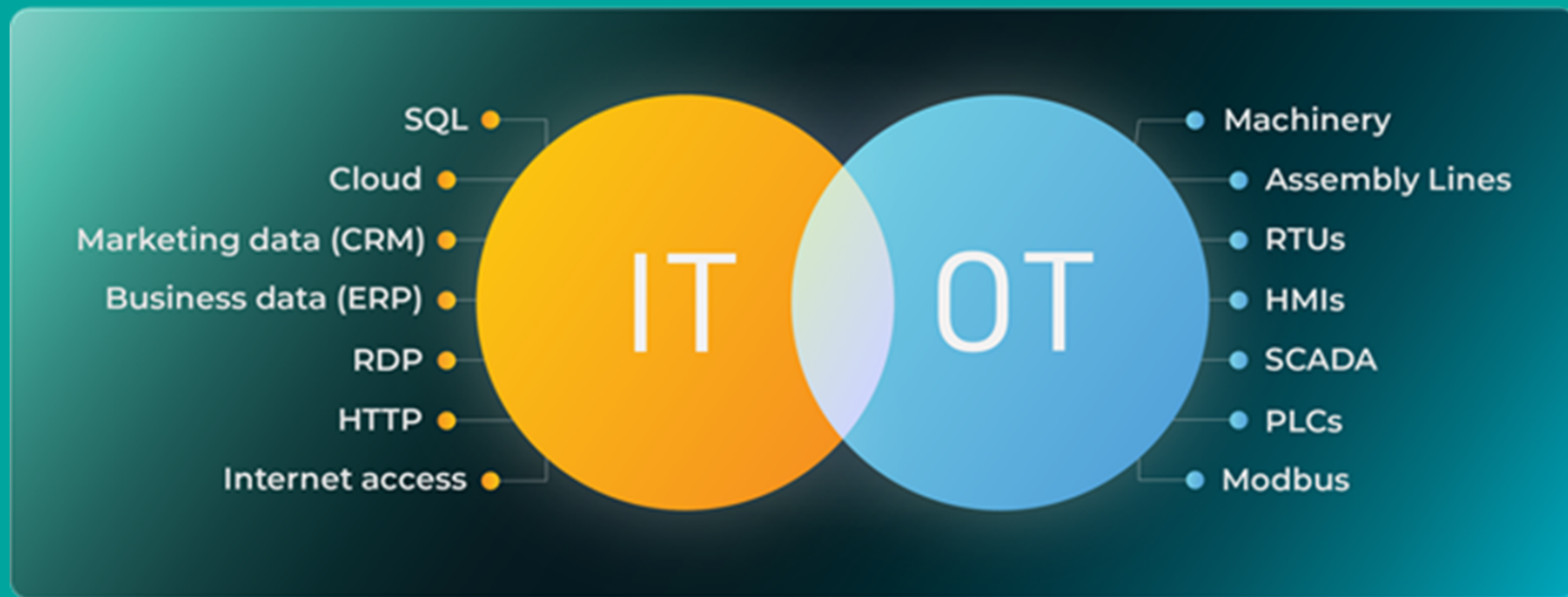
- Identify Assets
 - Hardware
 - Software
 - Third-Party
- Identify Regulatory Requirements
- Choose a Framework
 - NIST CSF
 - NIST 800-171
 - CIS Critical Security Controls
 - ISO/IEC 27001, 27002
 - CMMC
- Ensure Operational and Situational Awareness
- Conduct Assessments
- Identify Desired Target State for Continual Improvement
- Develop and Test Incident Response Capabilities



...don't forget

- Shiny security tools aren't the whole picture
 - People, process, and technology
- Ensure your policies are operationalized
- Assess your cyber coverage
- Ensure third-party contracts contain appropriate privacy and security provisions
 - Data Protection Addenda
 - Who bears the risk? Check your limitations of liability and indemnification provisions.
- Determine your organizational risk tolerance
- Ensure you have the appropriate organizational governance structure
- Push security down throughout your organization
- Do you have enough resources / budget?
- Leadership / Board of Directors oversight

Don't Forget OT!



Source: Otorio

Create a Culture of Security

- Cybersecurity is good business
- If done right, you likely meet or exceed the baseline requirements
 - Regs constantly change
- Privacy / Security by design
- Good faith effort is always the best approach
- Practice your Incident Response Plan

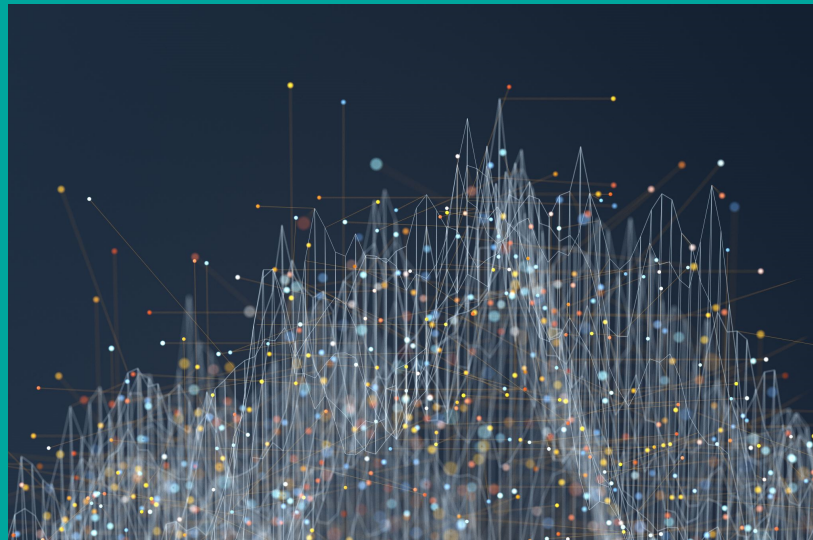


Responding to a Data Breach



Incident Response Preparation

- Biweekly meeting with CISO to discuss incidents and trends
- Info Security and Privacy vetting, contracts for personal data obligations and for info security obligations
 - Reporting incidents to us in a timely manner
 - Cooperation in incident



- Response Plan
 - When activated, incidents come into the Security Operations Center. Often won't be escalated.
 - Initial severity matrix, and then severity matrix as the incident unfolds. This guides internal and external communications.
 - Defines the roles each person will play
- Cybersecurity Incident Response Team
 - Person from IT most knowledgeable about the information system and from the business who is responsible for the information system
 - Legal
 - Corporate Communications
 - Senior Executives
- Who needs to know?
 - Escalation Matrix
 - Outside Counsel and Forensic Vendor
- Privilege

Assembling Your Response Team

- First 48 Hours are critical
 - Get the right people in the right place right away.
- Incident response team/plan
- Outside counsel
- IT forensic firm
- Threat actor communication firm
- \$2.66M average cost savings



- Communication to Business Partners
- Communication to Employees
- Communications to the Board of Directors
- Communication to Auditors



- Data Mining
- Notifications to Individuals
- Notifications to Regulators
- Notifications to Business Partners



Preserving Privilege over a Forensic Report

- Definition
- General content
- Assistance to counsel
 - Determine notification obligations
 - Manage legal risks
 - Anticipate and defend against claims
- SPB Handout





Shea Leitch

Of Counsel, Washington, D.C.

T 614.917.7522

E shea.leitch@squirepb.com



Simon Taylor

Executive Vice President, Scottsdale, AZ

T 602.748.0957

E staylor@packetwatch.com



Ericka A. Johnson

Attorney, Washington, D.C.

T 1 608 772 7441

E ericka.johnson@squirepb.com



Privacy and Cybersecurity Through Litigation and Enforcement Lens

September 19, 2023



Jeffrey Sallet

Partner and Crisis Management
Leader, EY LLP, Forensic &
Integrity Services
(prior associate deputy
director for FBI)



Amy Brown Doolittle

Partner, Washington DC
amy.doolittle@squirepb.com
T +1 202 626 6707




Kathleen McGovern

Partner, Washington DC
kathleen.mcGovern@squirepb.co
m
T +1 202 457 6558



Katherine Spicer

Partner, Washington DC
katy.spicer@squirepb.com
T +1 202 457 6000



Privacy Enforcement and Response Best Practices

Kathleen McGovern and Jeffrey Sallet

Regulators are increasing their focus on and more broadly interpreting existing cybersecurity regulations

- FTC's emphasis on the importance of breach disclosures (May 20, 2022)
- SEC - rules require registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance.
- DOJ - Civil Cyber Fraud Initiative; potential prosecution for material misstatements or omissions in company's financial statements

Chegg (Jan 2023): Found that Chegg failed to protect personal information that it collected from users and employees. Required Chegg to implement a comprehensive info security system, limit the data it can collect and retain; and allow users to request access and deletion of their own data.

Drizly LLC (Jan 2023): Issued order that its CEO failed to secure customers' data after being alerted to vulnerability two years prior leading to breach exposing personal info of 2.5m consumers; required to take remedial measures including public disclosures of collection of data and implementing comprehensive info security system.

CaféPress (June 2022): Fined former owner \$500K for failure to implement reasonable security measures to protect information on its network, including Social Security numbers, and for covering up breach.

- DOJ

- Oct 2021- Announced the launch of its Civil Cyber-Fraud Initiative aimed at combating “new and emerging cyber threats to the security of sensitive information and critical systems” specifically targeting accountability of cybersecurity obligations for federal contractors and federal grant recipients
 - **Verizon Business Network Solutions** (Sept 2023)
 - **Jelly Bean Communications Design LLC** (March 2023)- Jelly Bean and its manager paid \$293,771 to resolve allegations that they failed to secure personal information on a federally-funded Florida children’s health insurance website called HealthyKids.org, which was created, hosted, and maintained by Jelly Bean.
- Prosecuted Uber’s former Chief Security Officer for covering up data breach, involving millions of user records (October 2022) - Coordinated with the FTC

- U.S. Securities & Exchange Commission (“SEC”)
 - Increasing focus on mounting focus on cyber disclosures as an enforcement priority
 - **Blackbaud** (April 2023)- The cloud computing company agreed to pay a \$3-million civil penalty for alleged materially misleading disclosures about a 2020 ransomware attack
- U.S. Health and Human Services (“HHS”)
 - HHS- OIG formed a multidisciplinary Cybersecurity Team focused on combatting cybersecurity threats within HHS and the healthcare industry.
 - **Lifetime Healthcare Companies** (Jan 2021)- Fined \$5.1 Million to settle data breach affecting over 9.3 million people.

- Investigative Demands- Include voluntary requests, subpoenas, etc.
- Understand relationships among all regulators, including FTC and DOJ
 - Ability to share information usually through access requests
 - Run parallel investigations and coordinated resolutions
- Conduct internal investigation and remediate any issues as soon as possible
- Talking to regulators- understand different applicable statutes, policies for cooperation, remediation and resolution
- Keep investigation narrowly focused as possible- regarding interviews and discovery
- Be proactive



Defending Data Breach and Privacy Class Actions: Arbitration and Standing

Amy Brown Doolittle

Key Benefits of an Arbitration Agreement

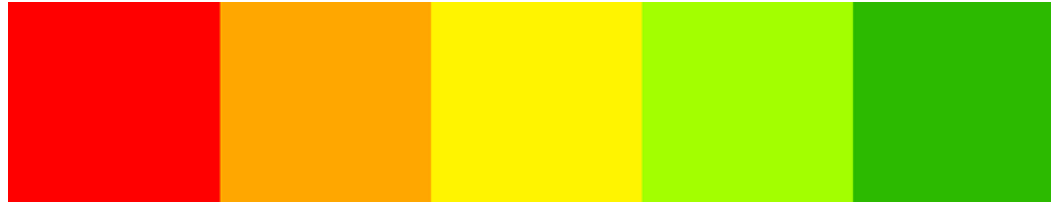
- Class action waiver:
 - *Keller v. Chegg, Inc.*, 2023 WL 5279649 (N.D. Cal. Aug. 15, 2023) (enforcing class action waiver and requiring individual arbitration).
 - Enforceability of class action waiver must be resolved prior to class certification. See *In re Marriott Inter., Inc.*, 2023 WL 5313006 (4th Cir. Aug. 18, 2023).
- Issues of arbitrability can be delegated to arbitrator:
 - *Torres v. Veros Credit LLC*, 2023 WL 5505887 (N.D. Cal. July 13, 2023).
- Denial of arbitration motion provides for immediate right of appeal under FAA and stay of proceedings:
 - *Coinbase, Inc. v. Bielski*, 143 S. Ct. 1915 (2023).

YES – parties must manifest their mutual assent to the terms of the agreement:

1. Does the online service provide reasonably **conspicuous notice** of the terms?
2. Does the user take some action that **unambiguously manifests** assent to those terms?

The Clickwrap-Browsewrap Spectrum

Browsewrap



Clickwrap

Clickwrap: “[A] website presents users with specified contractual terms on a pop-up screen and users must check a box explicitly stating ‘I agree’ in order to proceed.” *Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849, 856 (9th Cir. 2022).

Browsewrap: “[A] website offers terms that are disclosed only through a hyperlink and the user supposedly manifests assent to those terms simply by continuing to use the website.” *Id.*

- Font size
- Color of text compared to background
- Proximity
- Hyperlink readily apparent
- Other elements on the screen which may distract the user or obscure the textual notice

Is the user required to take action to manifest assent to be bound by the terms and conditions?

- Check a box?
- Notice of legal significance of taking action?
- Proximity of notice and checkbox?

- No judicial relief. See, e.g., *Abernathy v. DoorDash, Inc.*, 438 F. Supp. 3d 1062 (N.D. Cal. 2020).
- Can a company mitigate the risks?
 - Informal dispute resolution provisions.
 - Small claims court options.
 - Remove certain threshold issues from delegation clause.
 - Alternative arbitration provider.
 - Individual filing requirements to deter unmeritorious claims.
 - Do not agree to pay all arbitration filing fees.
 - Assess likelihood of mass arbitration claims.

- *Bohnak v. Marsh & McLennan Co., Inc.*, 2023 WL 5437558 (2d Cir. Aug. 24, 2023):
 - Plaintiff's alleged injuries arising from the risk of future harm are concrete.
 - Plaintiff's injuries were actual and imminent under three-factor test from *McMorris v. Carlos Lopez & Assocs.*, 995 F.3d 295 (2d Cir. 2021):
 - Was breach the result of targeted attack intended to get PII?
 - Has any data been misused?
 - Was the data high-risk?
- *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365 (1st Cir. 2023):
 - Post-*TransUnion* case finding standing based on risk of future harm.
- *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022):
 - Post-*TransUnion* data breach case finding standing.

- “Every class member must have Article III standing in order to recover individual damages.” *Transunion LLC v. Ramirez*, 141 S. Ct. 2190, 2208 (2021).
- *Green-Cooper v. Brinker Int’l, Inc.*, 73 F.4th 883 (11th Cir. 2023):
 - Two named plaintiffs lacked standing because injury not fairly traceable to defendant.
 - Vacated class certification and remanded back to district court to clarify predominance analysis because class definitions may include uninjured individuals.
- *Van v. LLR, Inc.*, 61 F.4th 1053, 1069 (9th Cir. 2023):
 - Vacated class certification and remanded back to district court to determine whether individual issues surrounding absent class member injury predominate and preclude class certification.



Privacy Litigation Trends

Katy Spicer

- Section 5 of FTC Act:
 - “offering” or “making available”
 - “incorporating”, “using”, or “relying on”
 - unfair or deceptive “privacy or data security practices”
 - unfair or deceptive practices relating to risks of harms to consumers, including reputational harm

FEDERAL TRADE COMMISSION (“FTC”)
CIVIL INVESTIGATIVE DEMAND (“CID”) SCHEDULE
FTC File No. 232-3044

Meet and Confer: You must contact **FTC counsel**, [REDACTED] as soon as possible to schedule a telephonic meeting to be held within fourteen (14) days after You receive this CID. At the meeting, You must discuss with FTC counsel any questions You have regarding this CID or any possible CID modifications that could reduce Your cost, burden, or response time yet still provide the FTC with the information it needs to pursue its investigation. The meeting also will address how to assert any claims of protected status (e.g., privilege, work-product, etc.) and the production of electronically stored

I. SUBJECT OF INVESTIGATION

Whether “the “Company,” as defined herein, in connection with offering or making available products and services incorporating, using, or relying on Large Language Models has (1) engaged in unfair or deceptive privacy or data security practices or (2) engaged in unfair or deceptive practices relating to risks of harm to consumers, including reputational harm, in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, and whether Commission action to obtain monetary relief would be in the public interest. See also attached resolution.

information under the Freedom of Information Act, 5 U.S.C. § 552. We also will not disclose such information, except as allowed under the FTC Act (15 U.S.C. § 57b-2), the Commission’s Rules of Practice (16 C.F.R. §§ 4.10 & 4.11), or if required by a legal obligation. Under the FTC Act, we may provide Your information in response to a request from Congress or a proper request from another law enforcement agency. However, we will not publicly disclose such information without giving You prior notice.

Manner of Production: Contact [REDACTED] by email or telephone at least five days before the return date for instructions on how to produce information responsive to this CID.

Certification of Compliance: You or any person with knowledge of the facts and circumstances relating to the responses to this CID must certify that such responses are complete by signing the “Certification of Compliance” attached to this CID.

1. Transparency first

- Detail the related Security Incident identified in public notice
- Disseminated advertisements – proof of clear and conspicuous notice to consumers

2. Governance Program

- All types of Personal Information collected, used, and stored
- Corporate Governance Model
 - Policies and procedures to assess risk and *safety*
 - Complaint process
- Human review and supervision of data
- Steps taken to prevent Personal Information from being included
- Consumer understanding before implementation

3. Know your data

- *Each* LLM provided, offered, or made available
- All third parties with “use” or “access” to LLM, paid or *unpaid*
- Data used to train (scraping, third parties, public, vetting)
- API Integrations

Top Privacy Litigation Trends 2023

1. Where's the action right now —————> systems that record and share:

- Session Replay
- Chat/video programs
- Pixels

2. What are theories of liability?

3. Horizon:

- B2B disputes
- AI litigation
- Shareholder disputes – MGM – time to target and impact on share price
- Competitor claims

1. **Best Practice 1:** Ensure that outside counsel engages a third-party forensic firm with whom Company does not have a pre-existing relationship. *See In re Capital One Consumer Data Sec. Breach Litig.*, 2020 U.S. Dist. LEXIS 112177 (D. Va. June 25, 2020).
2. **Best Practice 2:** Do not share the forensic report with a wide audience (especially not with external parties such as the FBI), and do not include remediation recommendations in the forensic report. *See Wengui v. Clark Hill*, 2021 U.S. Dist. LEXIS 5395 (D.D.C. Jan. 12, 2021).
3. **Best Practice 3:** To obtain work product protection, the forensic report must have been prepared “in anticipation of litigation.” To preserve privilege provide the forensic report directly to outside counsel, not to Company. *See In re Rutter’s Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 U.S. Dist. LEXIS 136220 (E.D. Pa. July 22, 2021).

Global Coverage

Abu Dhabi

Atlanta

Beijing

Berlin

Birmingham

Böblingen

Bratislava

Brussels

Cincinnati

Cleveland

Columbus

Dallas

Darwin

Denver

Dubai

Dublin

Frankfurt

Hong Kong

Houston

Leeds

London

Los Angeles

Madrid

Manchester

Miami

Milan

New Jersey

New York

Palo Alto

Paris

Perth

Phoenix

Prague

San Francisco

Santo Domingo

Shanghai

Singapore

Sydney

Tampa

Tokyo

Warsaw

Washington DC

Africa

Brazil

Caribbean/Central America

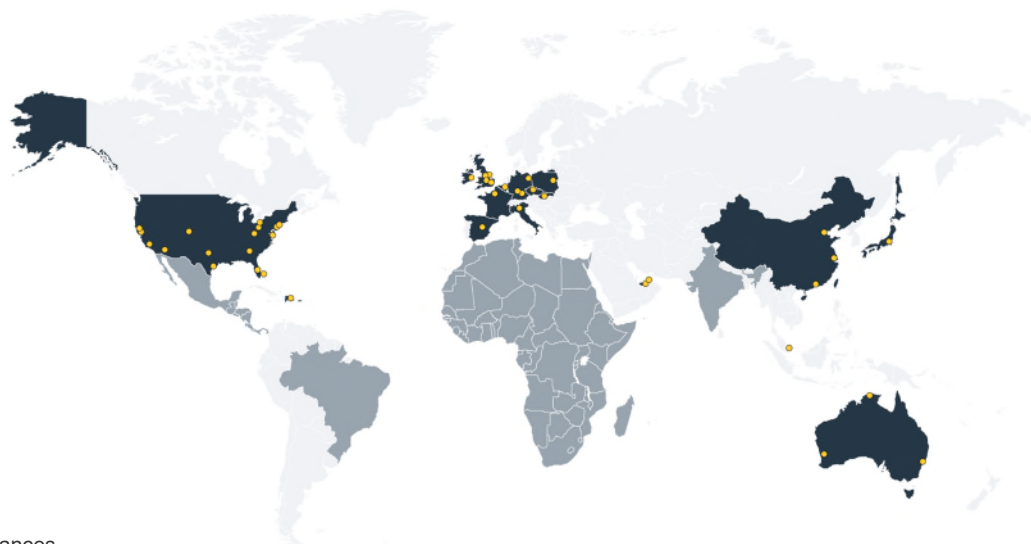
India

Israel

Mexico

Office locations

Regional desks and strategic alliances



AI Policy Perspectives

September 19, 2023



Presenters



Rodney Emery
Principal, Washington DC
T +1 202 457 6179
rodney.emery@squirepb.com




Stacy Swanson
Policy Advisor, Washington DC
T +1 202 457 5627
stacy.swanson@squirepb.com



Julia Jacobson (*Moderator*)
Partner, New York
T +1 212 872 9832
julia.jacobson@squirepb.com

What is AI?

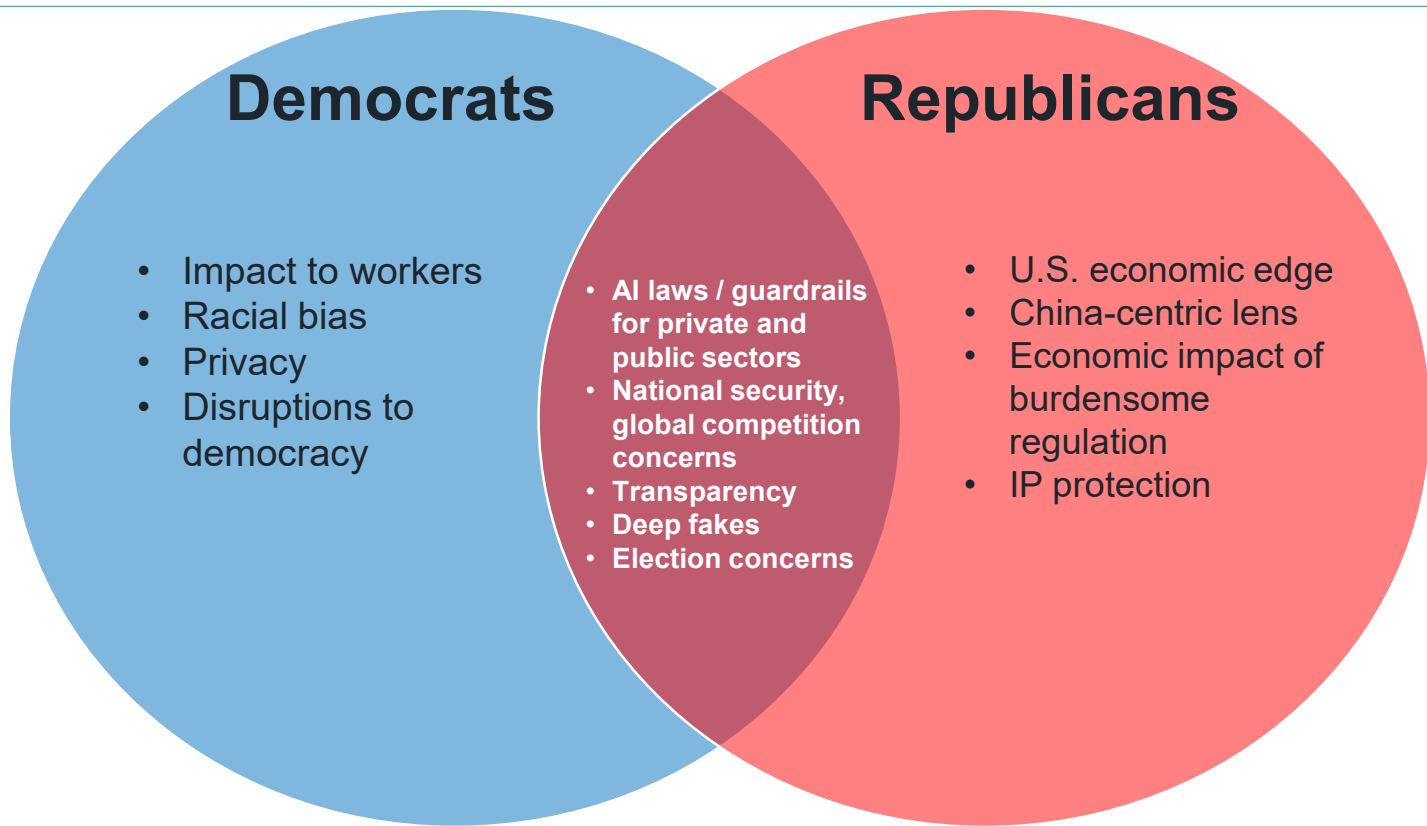
A central graphic of a human head profile in blue outline, facing right. Inside the head are two interlocking blue gears. Surrounding the head are several other blue gears of different sizes, some partially visible, creating a mechanical theme.

An AI system is a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives.

- *NIST AI Risk Management Framework*

AI is defined in many ways and often in broad terms ... it may depend on who is defining it for whom, and who has the power to do so ... what matters more is output and impact.

- *U.S. Federal Trade Commission*



- On October 4, 2022, the Biden White House (through the Office of Science and Technology Policy (**OSTP**)) released a “[Blueprint for an AI Bill of Rights](#).” The Blueprint was designed to “help guide the design, development and deployment of artificial intelligence (AI).”
 - “ ... this framework uses a two-part test to determine what systems are in scope. This framework applies to (1) automated systems that (2) have the potential to meaningfully impact the American public’s rights, opportunities, or access to critical resources or services.
 - Key principles:
 - Safe and Effective Systems
 - Algorithmic Discrimination Protections
 - Data Privacy
 - Notice and Explanation
 - Human Alternatives, Consideration, and Fallback
- Earlier this year, the White House released a series of new efforts to respond to the rise of AI.
- The Biden Administration aims to gather information on how the Federal Government can best oversee and harness the production of AI to further U.S. prosperity.

- The Biden Administration has committed \$140 million in new research to promote innovation and protect people's rights and mitigate potential risks.
 - Additional commitments from the Biden Administration include long-term investments in fundamental and responsible AI research.
- Congressional Democrats have introduced a variety of bills.
 - Propose the establishment of 20-member national commission that will focus on creating guardrails that are set up to prevent harm to American citizens.
- Congressional Democrats:
 - support efforts to promote and protect U.S. AI companies in order to maintain existing advantages over the Chinese tech industry.
 - Care about AI's potential disruption for workers, democracy and national security.

- Republicans are seeking to balance the need to provide AI guardrails, while not quashing American innovation – a U.S. competitive edge in the global economy.
- Similar to Democrats, Republicans raise national security and foreign competitor concerns – namely centered on China – which colors lawmakers' approach to any legislation.
- Other themes include increased transparency if AI is used; whether there is a human decisionmaker component; safeguarding against the exploitation of children; and licensing/ensuring copyright protections.
- In June, Senator Josh Hawley (R-MO) announced his guiding principles for AI legislation – create private rights of action; protect personal data; enforce age limits on use; block technology to and from China; and establish a licensing system. He has since teamed up with Senator Richard Blumenthal (D-CT).
- In August, Senator Todd Young (R-IN) suggested Congress could establish a new office in the White House to tackle AI or perhaps expand the authority of the Office of Science and Technology Policy.

- Several bills have been introduced; Senators are introducing or have indicated they are drafting additional legislation to address deepfakes, government procurement of automated systems, and other approaches to AI.
- A bipartisan effort has also emerged in the Senate.
 - In April, Senate Majority Leader Chuck Schumer (D-NY) outlined a set of principles for addressing AI concerns.
 - In June, he unveiled a broad AI framework for the Senate to push forward with comprehensive legislation to provide guardrails for AI on issues such as protecting workers, national security concerns, copyright protections, and defending against “doomsday scenarios.”
 - Leader Schumer tapped Senators Martin Heinrich (D-NM), Mike Rounds (R-SD), and Todd Young (R-IN) to work with him and to serve as sherpas.
- Leader Schumer indicated his preference for a committee-by-committee approach to AI regulation as a way to move the Senate toward a more comprehensive plan.
- As part of the “listen-and learn” effort, Leader Schumer has organized briefings for Senators.
 - September 13th: closed-door gathering of tech CEOs for an all-day listening session on how the fast-moving technology should be regulated. 60 Senators attended.

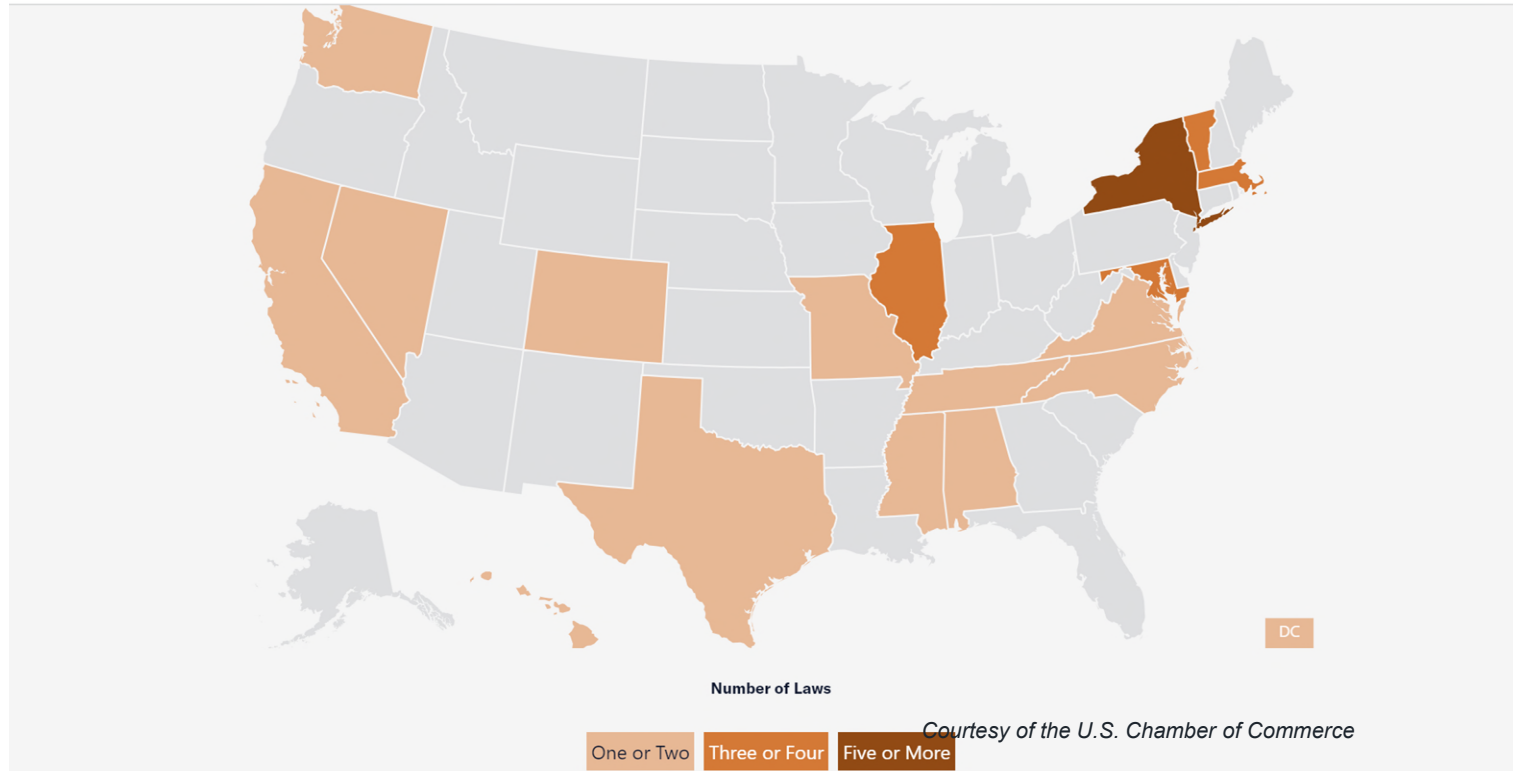
- **Some lawmakers are ready to move forward with AI legislation; other lawmakers seek to listen-and-learn before legislating.**
- Senators Richard Blumenthal (D-CT) and Josh Hawley (R-MO) – leaders of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law – held a hearing to refine their own set of comprehensive AI rules, which they [announced on September 8, 2023](#).
- This “[Bipartisan Framework for U.S. Act](#)” would:
 - Establish a Licensing Regime Administered by an Independent Oversight Body
 - Ensure Legal Accountability for Harms
 - Defend National Security and International Competition
 - Promote Transparency
 - “Protect Consumers and Kids”

- While Senator Blumenthal endorsed Majority Leader Schumer's ongoing briefings or listening sessions for lawmakers on AI, he cautioned, *"You can't know everything before you do something. You need to do the legislation and learn at the same time."*
- Senator Todd Young (R-IN) – one of Leader Schumer's sherpas – said last week: *"My concern as a legislator would be that they get locked into particular provisions as we're still gathering information, and potentially outflanked by somebody who has had the benefit of more counsel from more sources."*
- Senator Maria Cantwell (D-WA), Chair of the Senate Commerce Committee, believes Congress should already have a decent idea of what it would like to accomplish on AI.
 - She reminded reporters last week: *"I set up the [National AI Advisory Committee] years ago for this very thing: what should the government role be?"* She argued that Congress has already had "three years" to discuss what AI legislation should "really look like."

- Congress has considered – but not passed – comprehensive federal privacy legislation (e.g., [American Data Privacy and Protection Act](#)) to align the patchwork of state and sectoral privacy laws.
 - Personal information use in AI systems is a relatively new concern that states are starting to address, e.g., California's [proposed AI risk assessment regulations](#).
 - States have concerns about federal pre-emption of state AI laws and regulations – same for state privacy laws.
 - Patchwork of state AI laws mirroring the state privacy laws?
- Section 230 (of the **Communications Decency Act**) reform may materialize as Congress considers whether to apply the same protections to AI-generated content.
 - In June, Senators Josh Hawley and Richard Blumenthal introduced the [No Section 230 Immunity for AI Act](#) which would exclude generative AI from Section 230. Senator Blumenthal called the bill a "first step" in establishing safeguards around AI.

- Consensus in Congress on regulating AI rules seems unlikely in the near term.
- Meanwhile, the Biden Administration launched a voluntary risk-management framework and a nonbinding AI bill of rights.
 - The White House struck a [voluntary agreement](#) in July with eight major AI companies.
- The Biden Administration also is using existing civil rights laws to help prevent AI bias.
 - In an April [joint announcement](#), the Consumer Financial Protection Bureau, the Department of Justice, the Equal Employment Opportunity Commission, and the Federal Trade Commission laid out some of the ways existing laws would allow them to take action against companies for their use of AI.
- Notably, the White House is reportedly readying new executive actions on AI.
- The White House's OSTP is formulating a new National AI Strategy that it has said will take a "whole-of-society" approach.
- States are advancing AI laws.

States with AI Laws



- Policymaking runs the gamut from implementation of existing laws and regulations to new rulemaking (Executive Branch) and legislation (U.S. Congress).
- Navigating the evolving Executive vs. Legislative Branch approaches to AI, along with state laws, requires due diligence.
- This presents a unique opportunity for AI technology organizations to shape AI policy, such as advocacy to congressional delegation through educational outreach and awareness of the benefits.

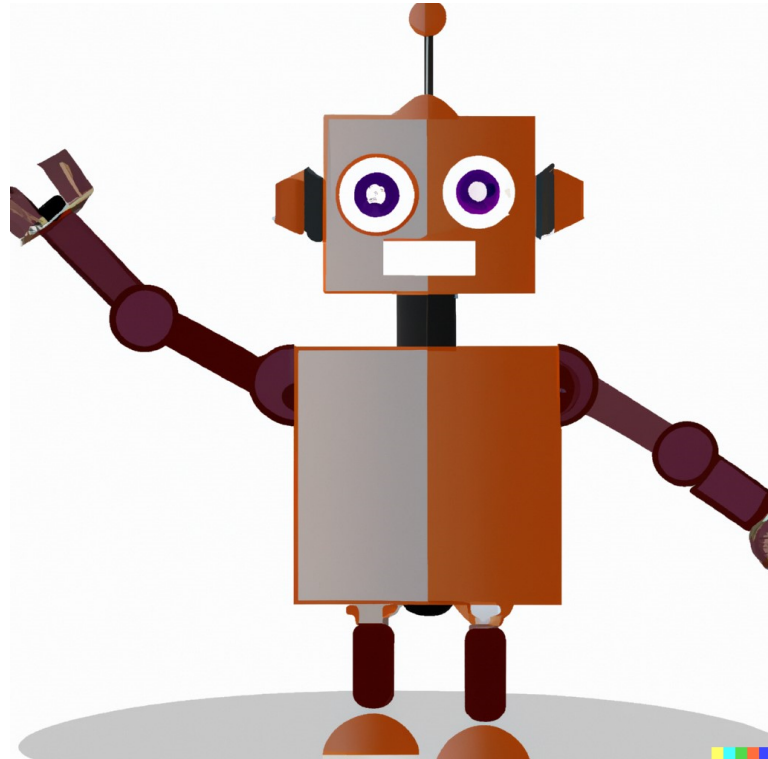
We recommend that businesses engage early in shaping AI policy, rather than wait for a final rule or law or litigation.

- **Global Leadership** – Democrats and Republicans have a shared interest in ensuring the United States remains a leader in the AI international dialogue.
- **Innovative Edge** – The Federal Government will make every effort to protect American companies against foreign competitors; this includes ensuring international laws do not discriminate and place American companies at a commercial disadvantage.
- **Timing** – The politics of an election year in 2024 will present a major challenge for both Democrats and Republicans to pass comprehensive AI legislation. A more measured incremental response from Congress may emerge for achieving successful AI legislative outcomes.
- **To Advocate or Not?** Companies can help influence and shape AI policy by engaging now. Those that do not engage will have to adapt their due diligence structures to the federal and/or policies that eventually emerge.

Questions



Thank you!



Created Using DALL-E