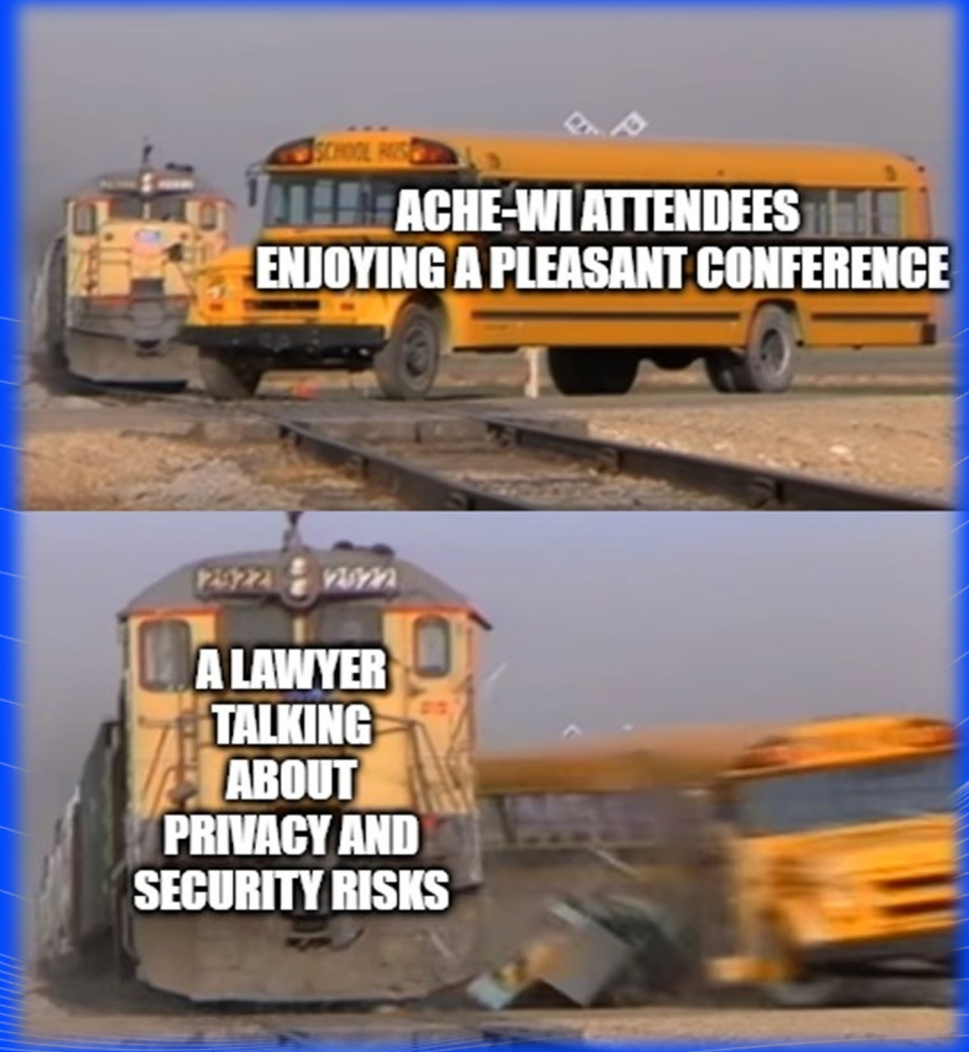


HUSCH BLACKWELL

Current Trends in Privacy and Cybersecurity

Brad Hammer
Husch Blackwell – Minneapolis
brad.hammer@huschblackwell.com



Overview:

Quick “Basics”

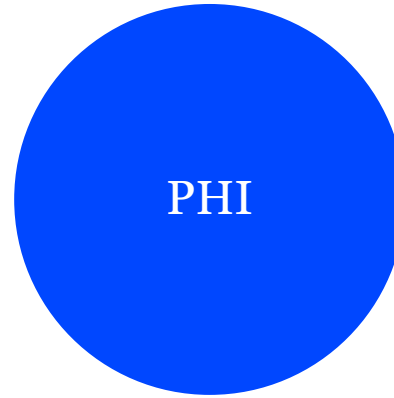
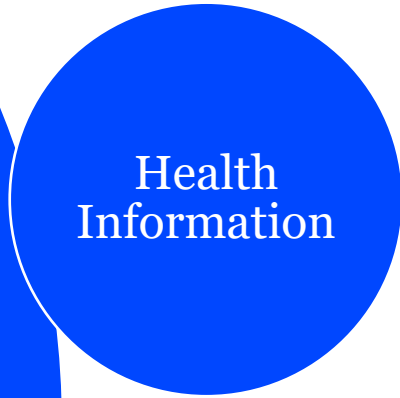
Cyber/Breach Trends

Developments In the Law

Litigation / Enforcement Trends

What’s Next?

The Basics: What is Personal Information?



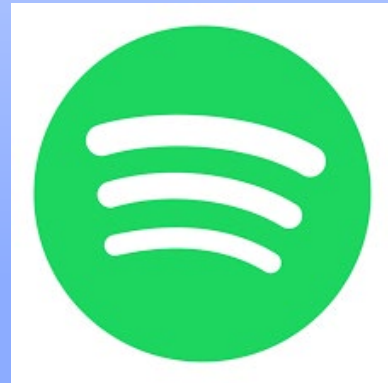
Elements from state data breach laws



What is Personal Information?

Name OR Unique Identifier with any of the following:	contact information, address, phone number, email, fax	account/order information, purchase history, shipping details	billing information, credit card, bank account, billing contact information	professional information, company/employer information, job title, professional affiliations	Geographic or location information
information contained in posts made on the public forums and interactive features of a website or app	information gathered through cookies, pixels, and similar technology	residency, citizenship, visa number, military status, nationality, and passport information	payroll, wage, salary, and benefit information	skills, work experience, education, certificates, registrations, professional licenses, training, and language abilities	performance-related information, reviews, references, disciplinary procedure information, attendance records
physical limitations and special accommodations	results of credit and criminal background checks, drug and alcohol testing, screening, health certifications	photo, video surveillance, other images or photographs, key card use times and locations	voicemails, e-mails, correspondence, documents, and other work products	medical and health information	survey or feedback information

What is Personal Information?



What is Processing?



The Law:

What type of law/standard is regulating the data?

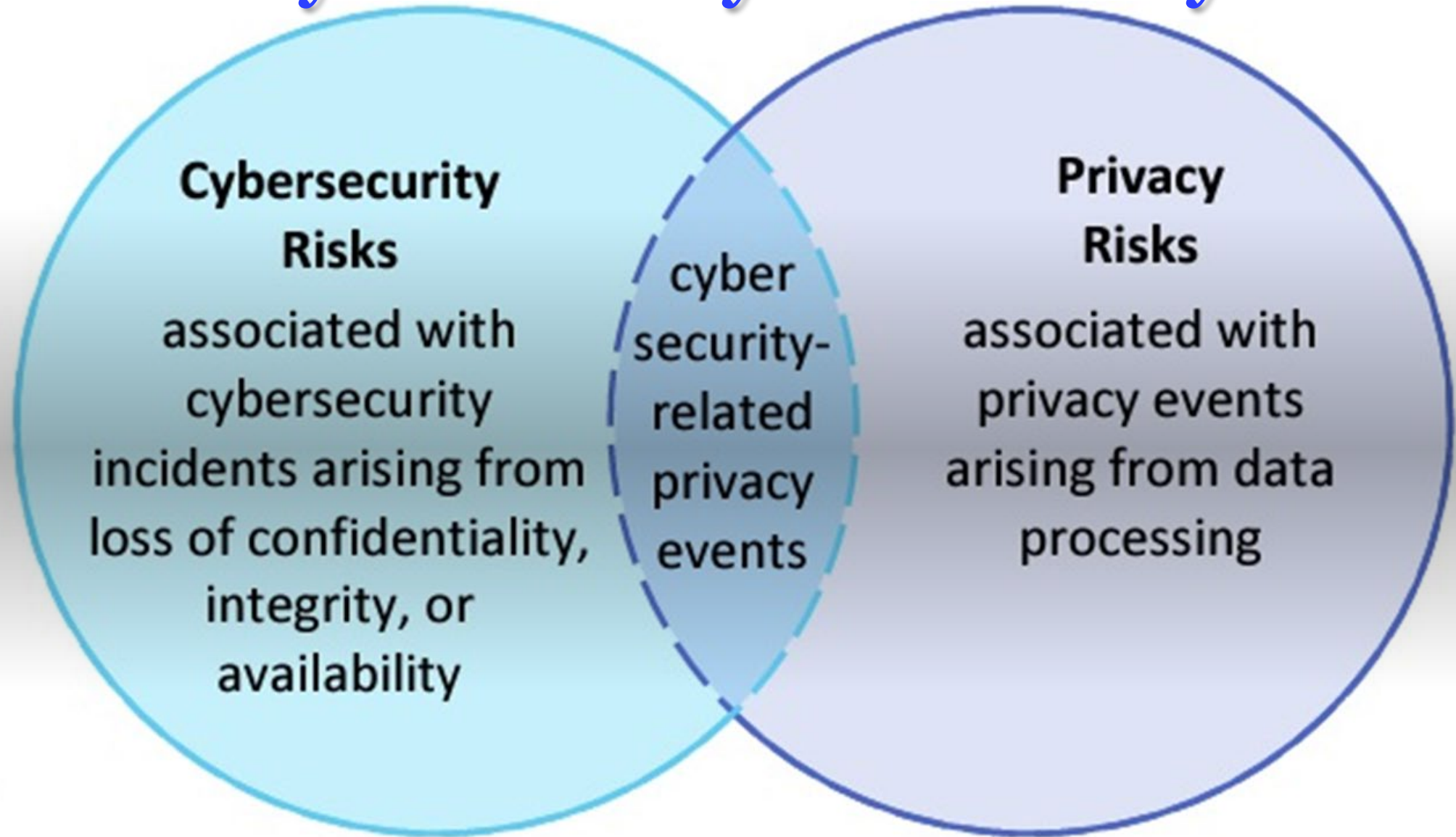
Comprehensive

- Regulating all (or most) data.
- Examples:
 - GDPR (EU)
 - CCPA
 - New State Laws

Sectoral

- Regulating a particular sector or type of data.
- Examples:
 - HIPAA (health)
 - GLBA (finance)
 - FERPA (education)

Cybersecurity and Privacy



BRACE YOURSELVES

SCARE SLIDES ARE COMING

Cybersecurity
and Breach
Trends





SAM DARNOLD MANIA!



Cost of a Data Breach Report 2024



604 Organizations



17 Industries



16 Countries



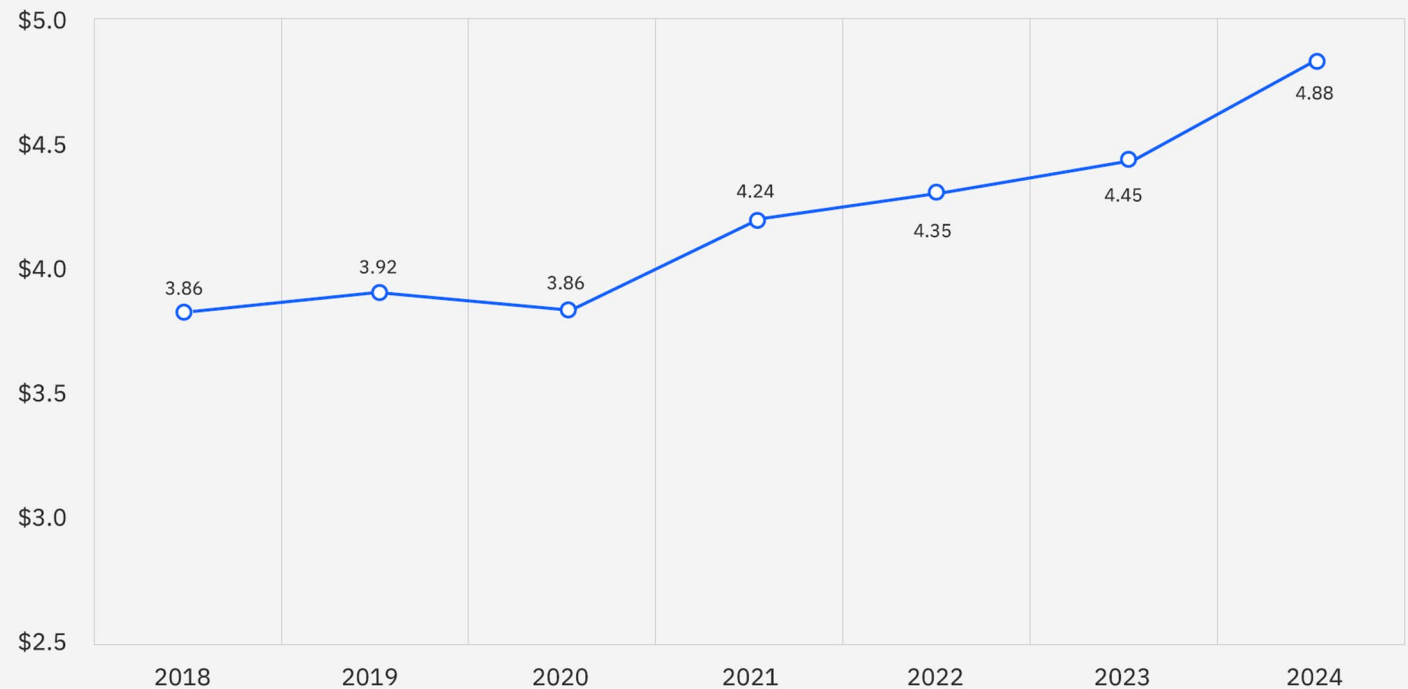
2,100 – 113,000 Compromised Records



3,556 Interviews Conducted



Global average total cost of a data breach



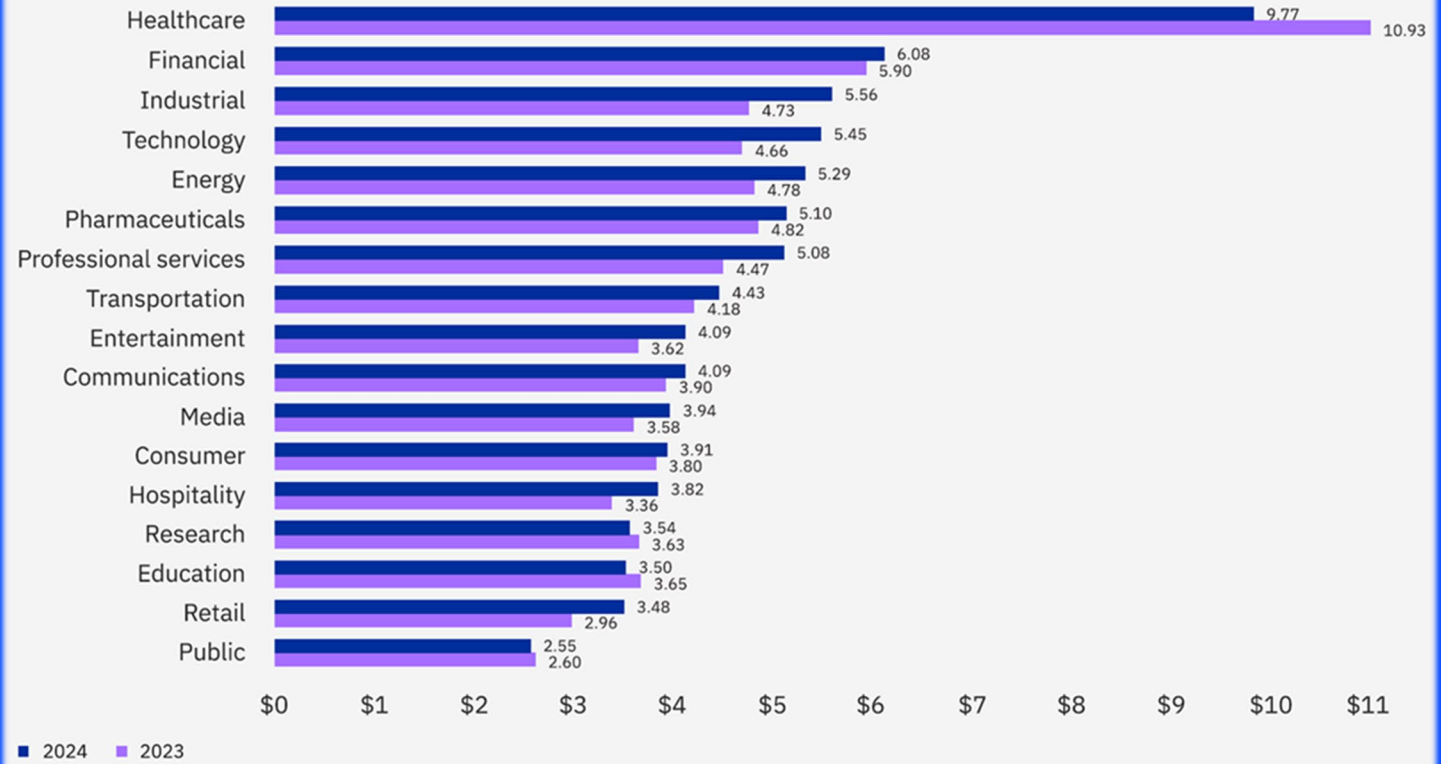
Cost of a Data Breach Report 2024



Cost of a data breach by country or region

#	Country	2024	2023
1	United States	\$9.36	\$9.48
2	Middle East	\$8.75	\$8.07
3	Benelux	\$5.90	—
4	Germany	\$5.31	\$4.67
5	Italy	\$4.73	\$3.86
6	Canada	\$4.66	\$5.13
7	United Kingdom	\$4.53	\$4.21
8	Japan	\$4.19	\$4.52
9	France	\$4.17	\$4.08
10	Latin America	\$4.16	\$3.69
11	South Korea	\$3.62	\$3.48
12	ASEAN	\$3.23	\$3.05
13	Australia	\$2.78	\$2.70
14	South Africa	\$2.78	\$2.79
15	India	\$2.35	\$2.18
16	Brazil	\$1.36	\$1.22

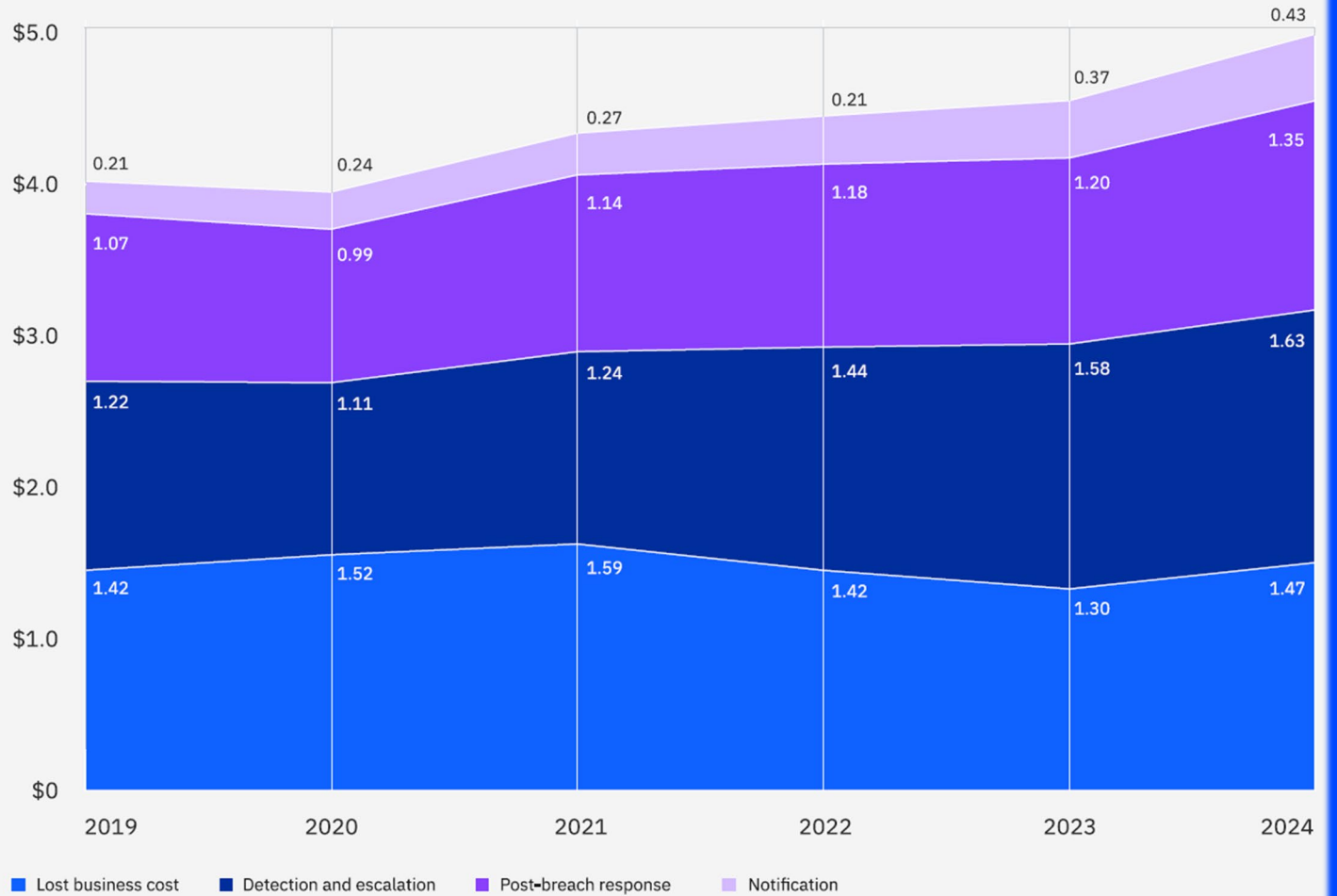
Cost of a data breach by industry



IBM – PONEMON INSTITUTE:
 COST OF DATA BREACH REPORT 2024
 (COSTS IN MILLIONS USD)

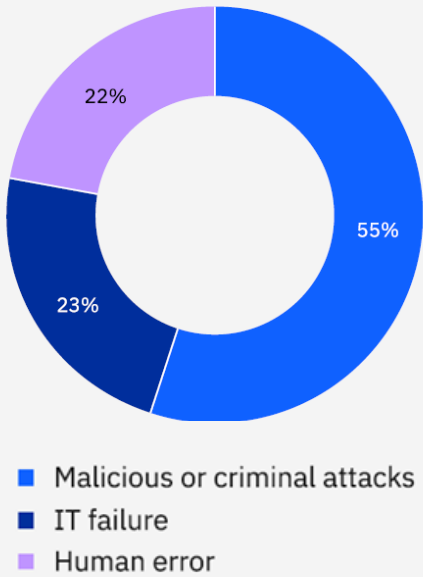


Average cost of a data breach in 4 components

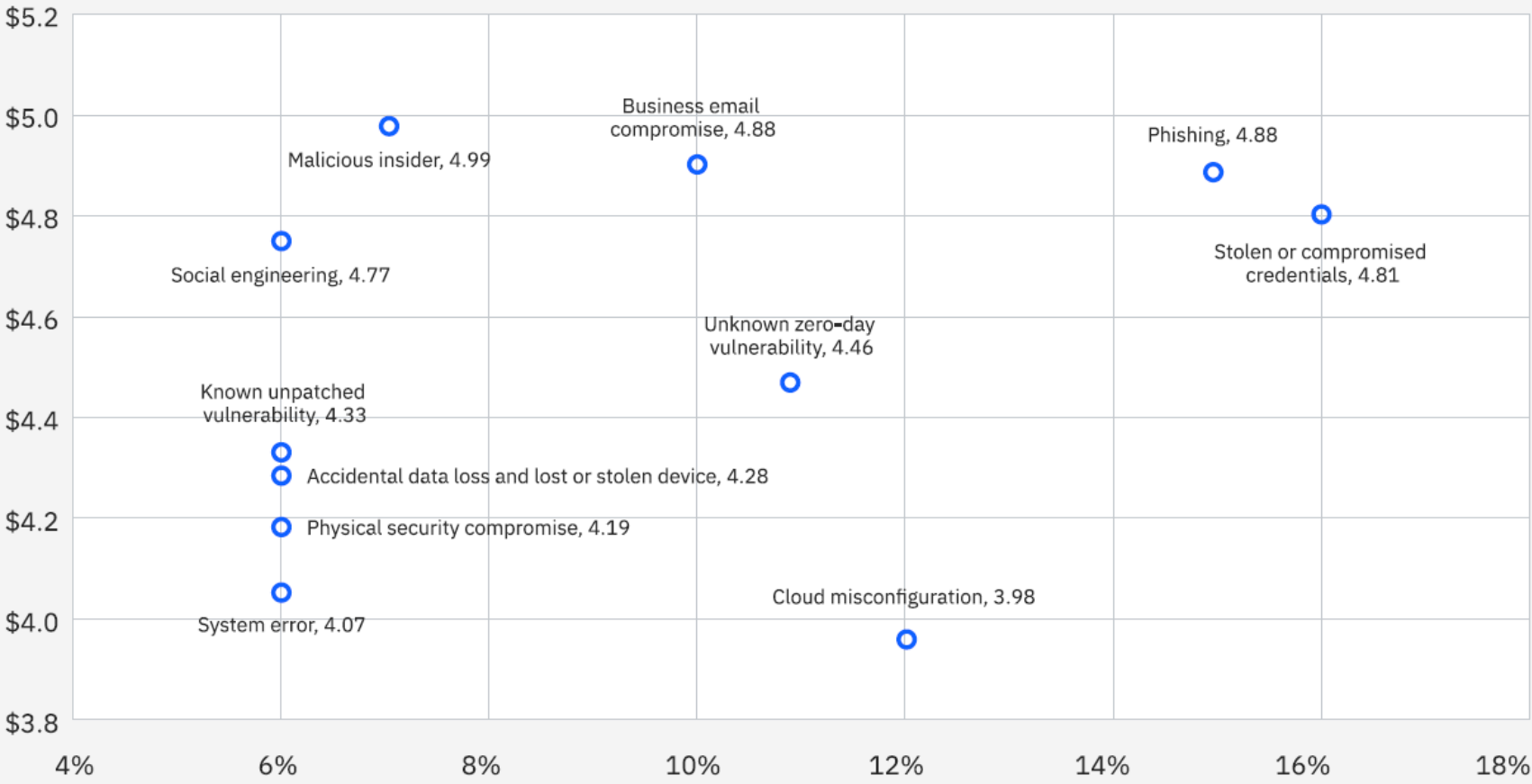


IBM – PONEMON INSTITUTE:
 COST OF DATA BREACH REPORT 2024
 (COSTS IN MILLIONS USD)

Root cause of the data breach between 3 categories



Cost and frequency of a data breach by initial attack vector



HUSCHBLACKWELL

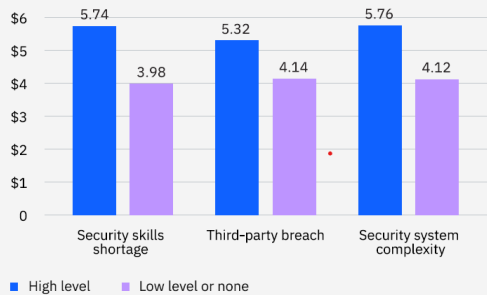
Factors that increased the average breach cost



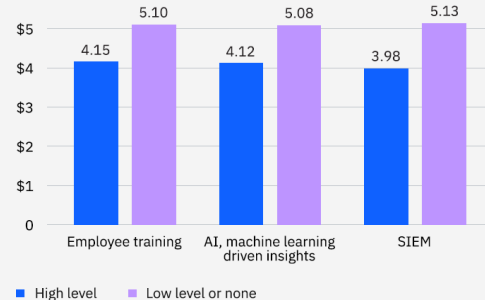
Factors that reduced the average breach cost



Cost of a data breach for organizations with a high level versus low level of 3 cost amplifying factors



Cost of a data breach for organizations with a high level versus low level of 3 cost mitigating factors



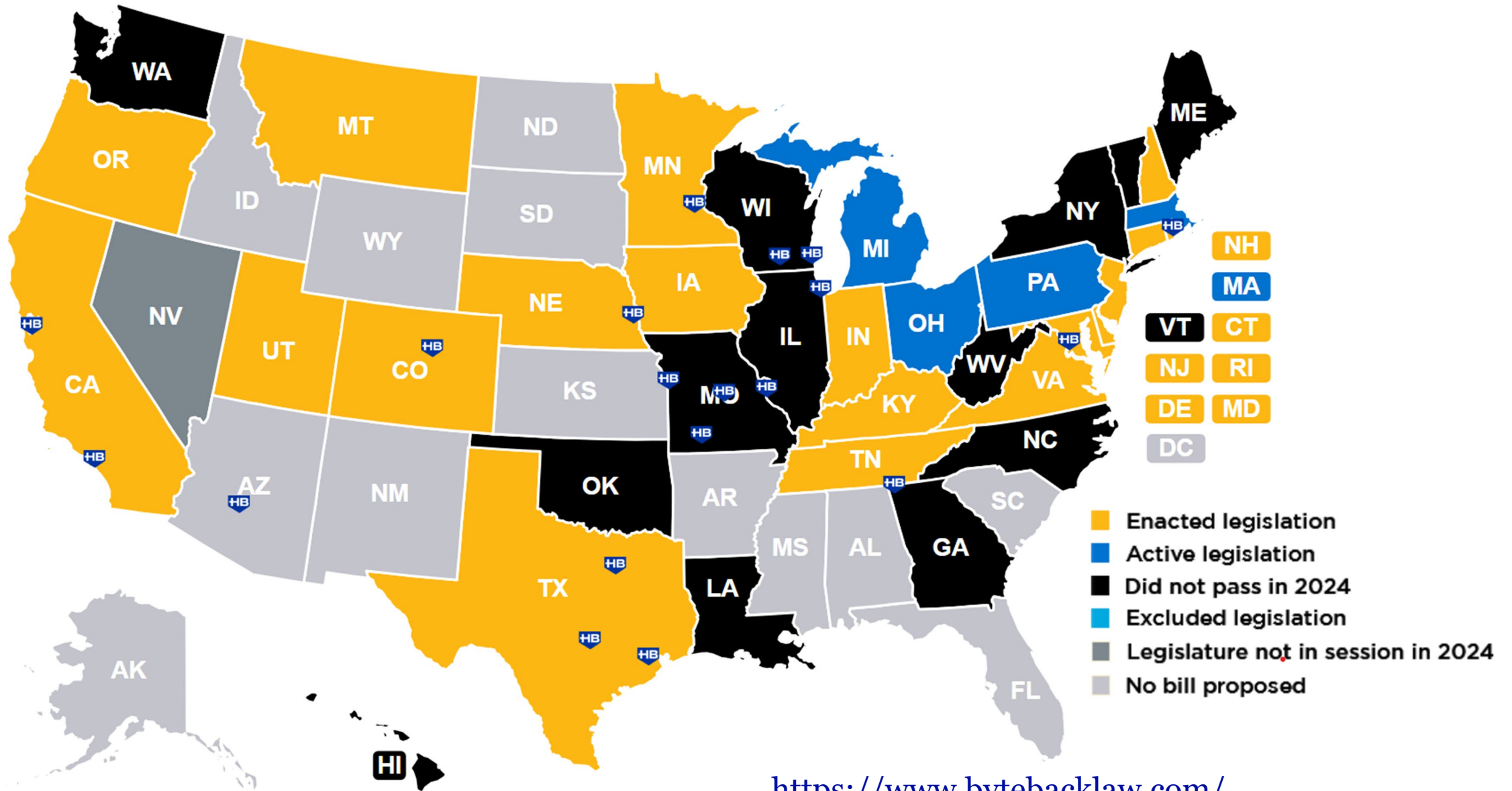
Developments
in State,
Federal, and
International
Law

**YOU GET A NEW PRIVACY LAW,
AND YOU GET A NEW PRIVACY LAW**



EVERYONE GETS NEW PRIVACY LAWS

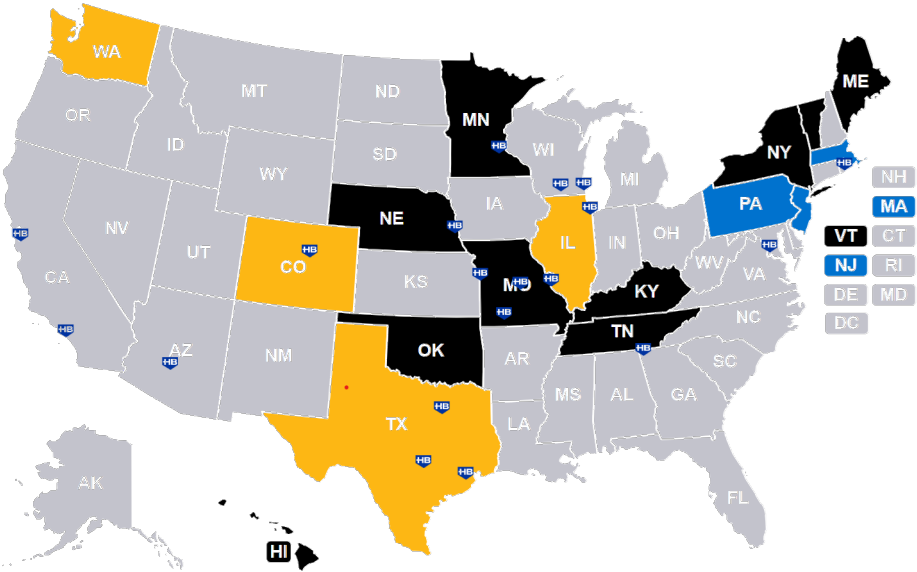
US State Comprehensive Laws 2024



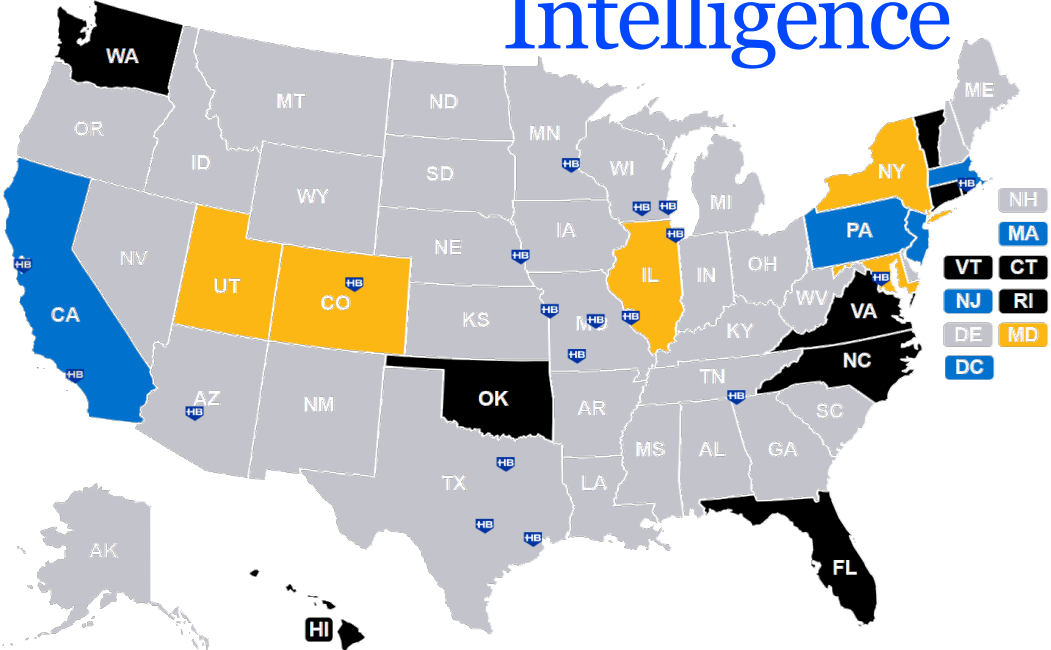
<https://www.bytebacklaw.com/>

2024 State Law Trackers

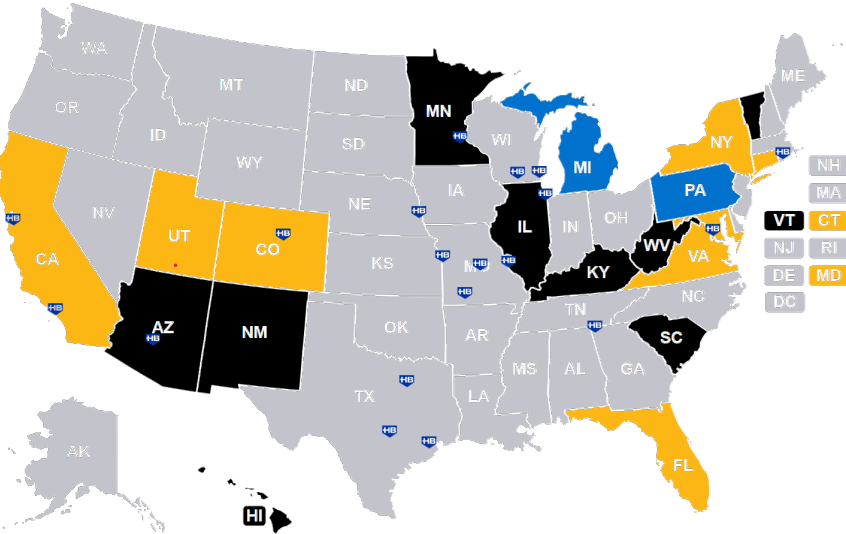
Biometrics



Artificial Intelligence

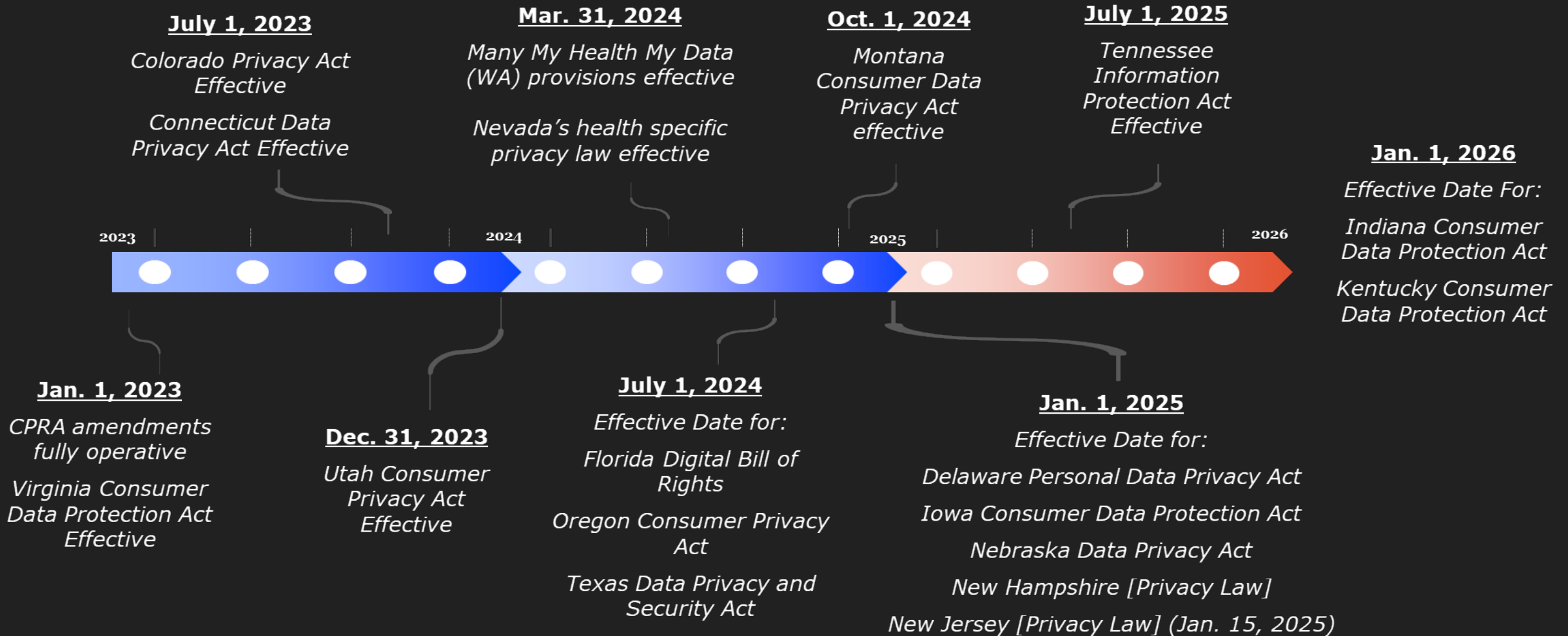


Children's Data



- Enacted legislation
- Active legislation
- Did not pass in 2024
- Excluded legislation
- Legislature not in session in 2024
- No bill proposed

Key Dates for US Privacy Law



Individual Rights (State Law)– Sale/Share of Data

(based on text of statute)

	CA	CO	CT	DE	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Opt-out of Sale	✓	✓	✓	✓	✓	●	✓	✓	✓	✓	✓	✓	✓	✓	●	●	✓	●	✓
Opt-out of targeted advertising/sharing	✓	✓	✓	✓	✓	?	✓	✓	✓	✓	✓	✓	✓	✓	●	●	✓	✓	✓
Opt-out of certain types of profiling	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	●	●	✓	✗	✓
Recognize opt-out signals	✓	✓	✓	✓	✗	✗	✗	●	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗

Federal Law

Post-Dobbs OCR Regulations

- Prohibits disclosing PHI in an investigation surrounding reproductive healthcare.

Health Care Cybersecurity Improvement Act of 2024 (proposed)

- Charges the Secretary of HHS with setting minimum cybersecurity standards for Medicare's Accelerated Payment Program and Advance Payments Program

OCR and Website Tracking

- Relief from enforcement of the OCR bulletin on unauthenticated web pages following the decision in AHA et. Al. v. Becerra et al

Unauthenticated Pages – OCR Examples/Guidance

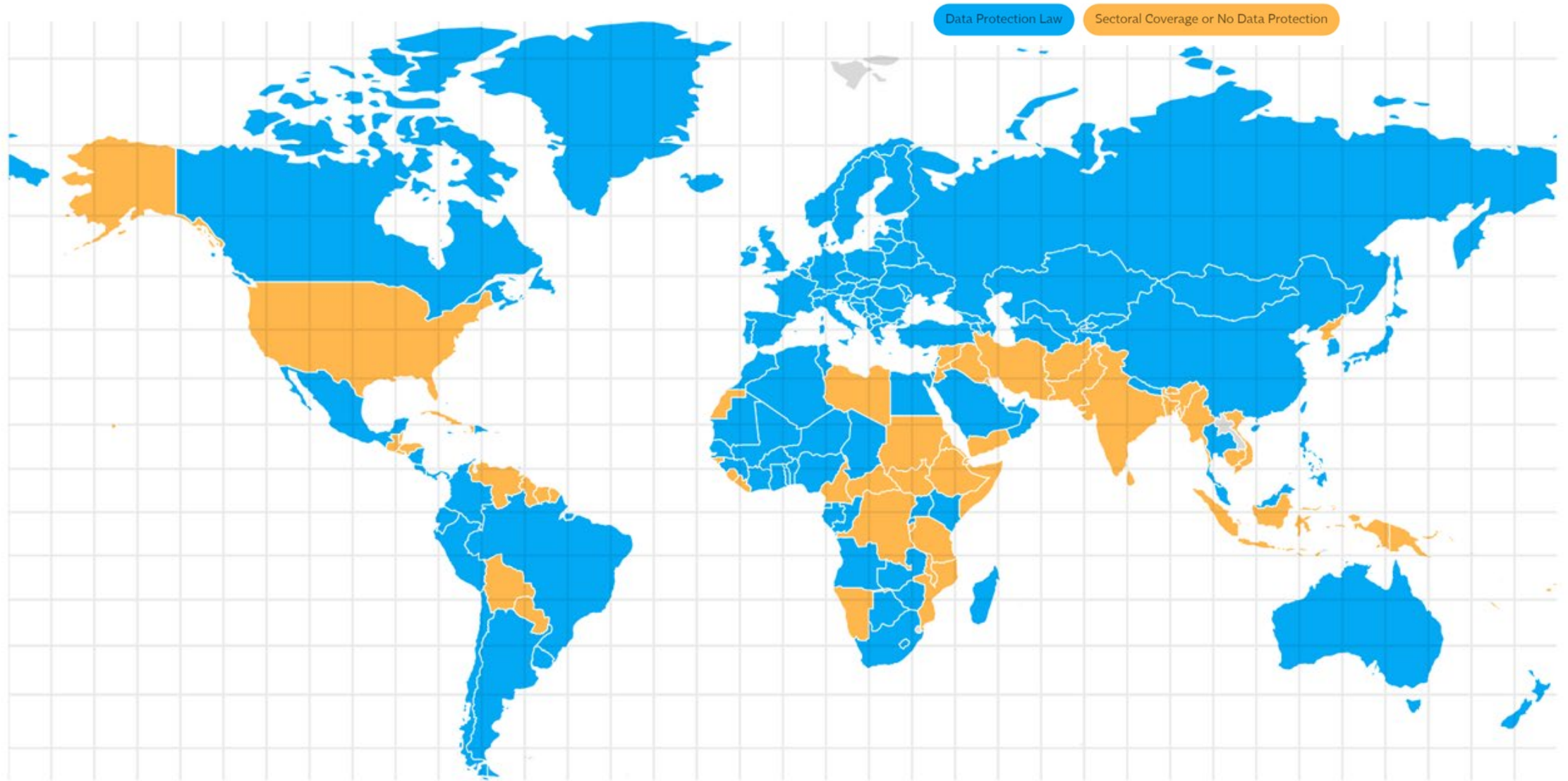
PHI

- If an individual were looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care.
- Tracking technologies might collect an individual's email address, or reason for seeking health care typed or selected by an individual, when the individual visits a regulated entity's webpage and makes an appointment with a health care provider or enters symptoms in an online tool to obtain a health analysis.

Not PHI

- Where a user merely visits a hospital's webpage that provides information about the hospital's job postings or visiting hours, the collection and transmission of information showing such a visit to the webpage, along with the user's IP address, geographic location, or other identifying information showing their visit to that webpage, would not involve a disclosure of an individual's PHI to tracking technology vendor.
- If a student were writing a term paper on the changes in the availability of oncology services before and after the COVID-19 public health emergency.

Global Considerations



[HTTPS://IAPP.ORG/RESOURCES/GLOBAL-PRIVACY-DIRECTORY/](https://iapp.org/resources/global-privacy-directory/)

Global data transfer contracts

By IAPP Director of Research and Insights Joe Jones

Restrictions on International Data Transfer

There are at least 20 draft, template or standardized contractual clauses or undertakings for international data transfers covering transfers from 71 countries.



Regions

Association of Southeast Asian Nations
Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam

Council of Europe - Draft
All European Economic Area states plus Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Moldova, Monaco, Montenegro, North Macedonia, San Marino, Turkey and the U.K.

European Economic Area
Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden

Latin American Data Protection Board (RIPD)
Andorra, Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico, Panama, Peru, Portugal, Spain and Uruguay

Individual jurisdictions

Abu Dhabi Global Market

Argentina

Brazil

China

Dubai International Financial Centre

Guernsey

Hong Kong

Jersey

Moldova

New Zealand

Peru

Serbia

Switzerland

Turkey


United Kingdom

Uruguay

Jurisdictions part of multiple regional contracts

Argentina† **Peru†** **Spain***
Brazil† **Portugal*** **Uruguay†**

† Covered by their own and RIPD contracts.
* Covered by EEA and RIPD contracts.



Enforcement and Litigation Trends

HIPAA Enforcement Actions

Settlements from 2023 and 2024



HHS Office for Civil Rights Settles HIPAA Security Rule Failures for \$950,000

Settlement with Heritage Valley Health System marks OCR's third ransomware settlement as the agency sees 264% increase in large ransomware breaches since 2018

Today, the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) announced a settlement with Heritage Valley Health System (Heritage Valley), which provides care in Pennsylvania, Ohio and

HHS Office for Civil Rights Settles HIPAA Investigation with Arizona Hospital System Following Cybersecurity Hacking

Banner Health pays \$1.25 million to settle cybersecurity breach that affected nearly 3 million people

Today, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) announced a settlement with Banner Health Affiliated Covered Entities ("Banner Health"), a nonprofit health system headquartered in Phoenix, Arizona, to resolve a data breach resulting from a hacking incident by a threat actor in 2016 which

HHS' Office for Civil Rights Settles First Ever Phishing Cyber-Attack Investigation

Louisiana Medical Group settles after investigation reveals large cybersecurity breach affecting nearly 35,000 patients

Today, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), announced a settlement with Lafourche Medical Group, a Louisiana medical group specializing in emergency medicine, occupational medicine, and laboratory testing. The settlement resolves an investigation following a phishing attack that affected the electronic protected health information of approximately 34,862 individuals. Phishing is a type of cybersecurity attack used to trick individuals into disclosing sensitive information via electronic communication, such as email, by impersonating a trustworthy source. This marks the first settlement OCR has resolved involving a phishing attack under the Health Insurance Portability and Accountability Act (HIPAA) Rules. HIPAA is the federal law that protects the privacy and security of health information.

U.S. Enforcement Action

Date ↓	Reference ↑↓	Jurisdiction ↑↓	USD ↑↓	Agency ↑↓
Sep-11-2024	Cybersecurity: FTC Fined Security Camera Company 2.95M and Orders a Sec...	United States	\$2,950,000.00	FTC
Aug-29-2024	Robocalls: FCC Settles with Telecom for \$1M for Discouraging Voter Turnout Us...	United States	\$1,000,000.00	FCC
Aug-16-2024	Data Breach: NY Biochem to Pay \$4.5M in a Multi-state Settlement Due to Sec...	United States	\$4,500,000.00	New York Connecticut ...
Aug-13-2024	Online Profiling: Data Broker Oracle Pays \$115M to Retire Privacy Allegations	United States	\$115,000,000.00	Northern District Court ...
Aug-12-2024	Facial Recognition: Meta's Biometric Processing Leads to Record \$1.4 Billion Se...	United States	\$1,400,000,000.00	State of Texas
Jul-31-2024	Data Breach: FCC Settles with Telecom for \$16M Mandating Improved Security...	United States	\$16,000,000.00	FCC
Jul-19-2024	Children and Minors: FTC Fines Messaging App for Making Deceptive Claims A...	United States	\$5,000,000.00	FTC

Litigation Trends

Illinois Biometric Information Privacy Act (BIPA) Lawsuits

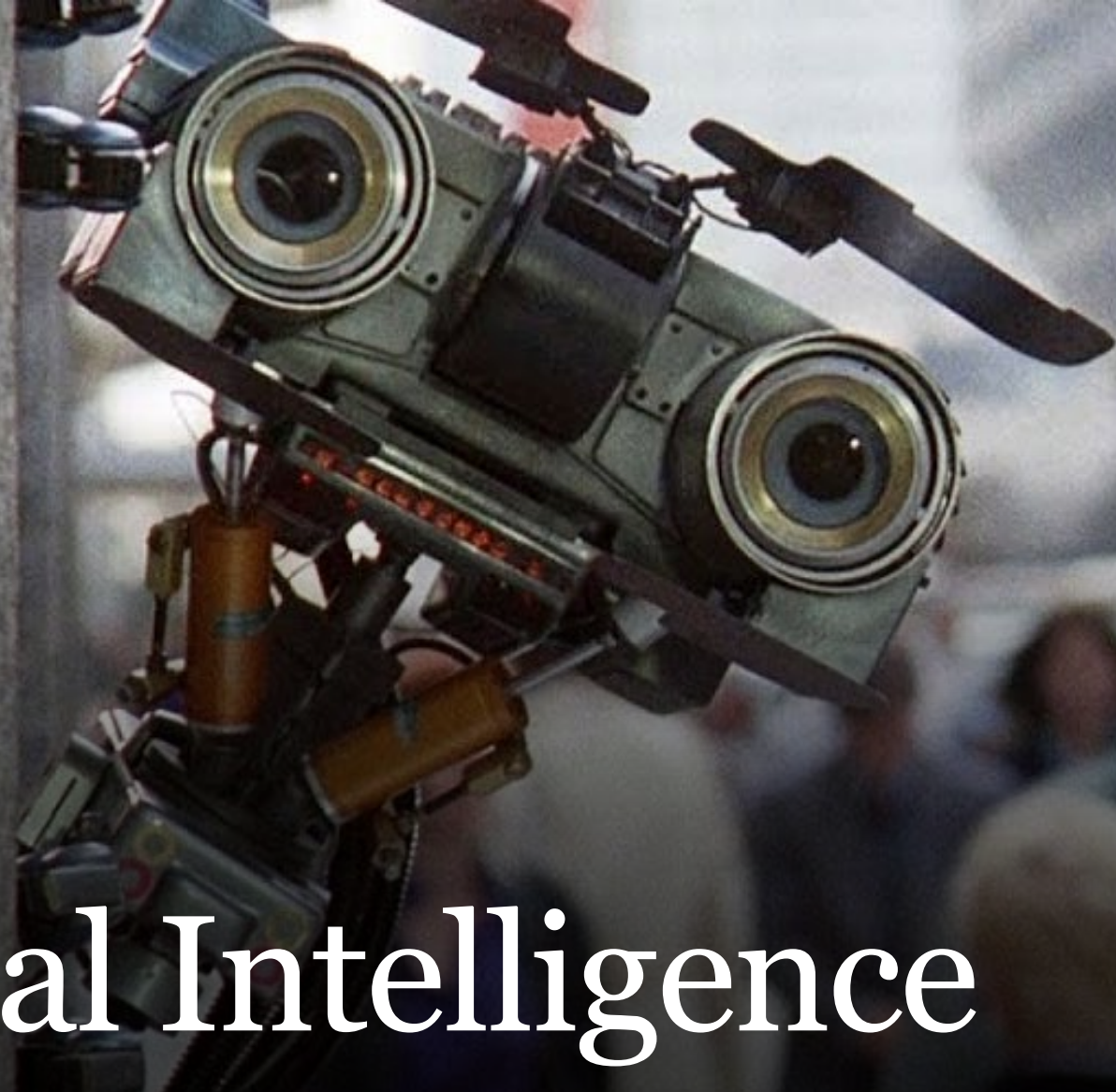
Website Chatbot Wiretapping Lawsuits

Website Session Replay Technology Lawsuits

Video Privacy Protection Act (VPPA) Lawsuits

Artificial Intelligence Lawsuits

Website Cookie Selection Lawsuits



Artificial Intelligence

Defining Generative AI

To understand generative artificial intelligence (GenAI), we first need to understand how the technology builds from each of the AI subcategories listed below.

Expert System AI

Programmers teach AI exactly how to solve specific problems by providing precise instructions and steps.

Artificial Intelligence

The theory and methods to build machines that think and act like humans.

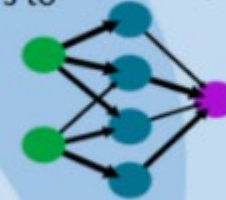


Machine Learning

The ability for computers to learn from experience or data without human programming.

Deep Learning

Mimics the human brain using artificial neural networks such as **transformers** to allow computers to perform complex tasks.



Generative AI

Generates new text, audio, images, video or code based on content it has been **pre-trained** on.



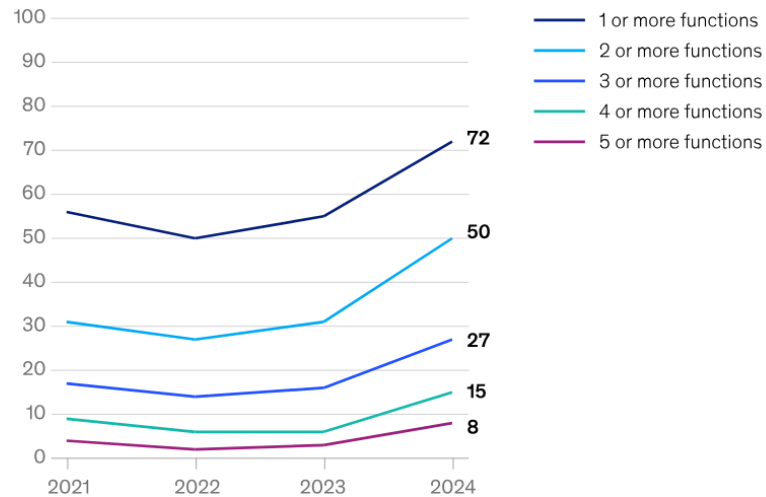
ChatGPT Midjourney Bard

AI for Education

© AI for Education 2023

aiforeducation.io

Business functions at respondents' organizations that have adopted AI,¹% of respondents

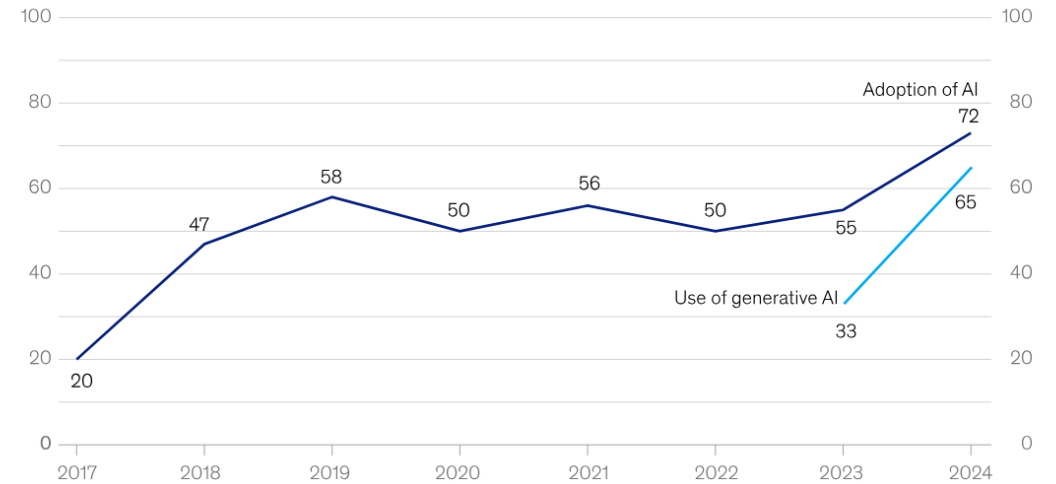


¹In 2021, n = 1,843; in 2022, n = 1,492; in 2023, n = 1,684; in early 2024, n = 1,363.
Source: McKinsey Global Survey on AI, 1,363 participants at all levels of the organization, Feb 22–Mar 5, 2024

McKinsey & Company

AI adoption worldwide has increased dramatically in the past year, after years of little meaningful change.

Organizations that have adopted AI in at least 1 business function,¹% of respondents

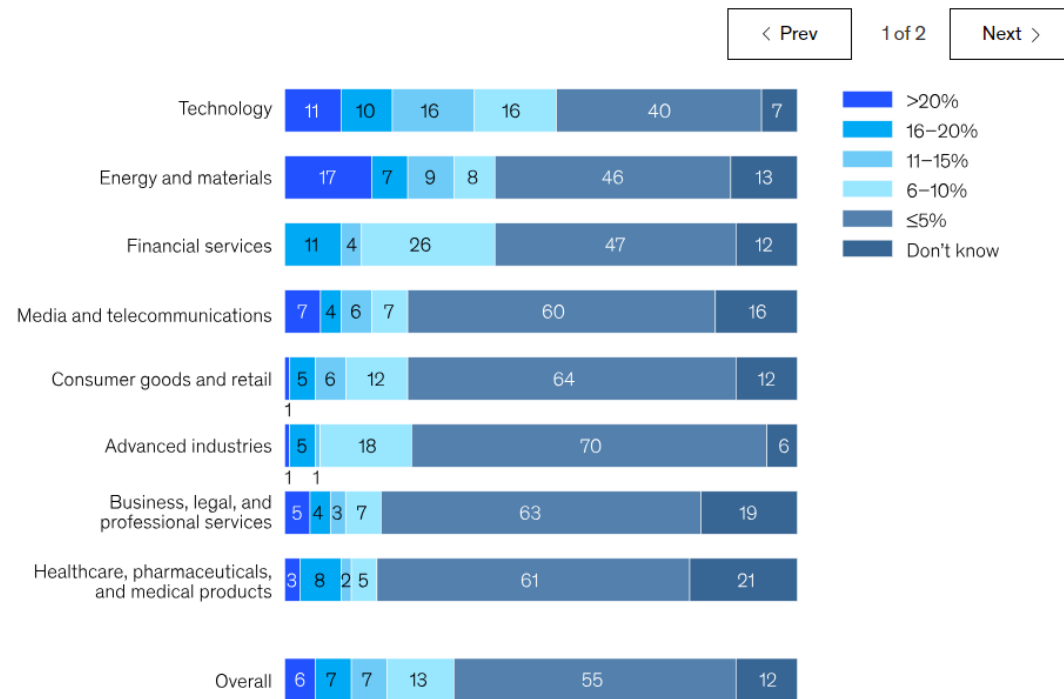


¹In 2017, the definition for AI adoption was using AI in a core part of the organization's business or at scale. In 2018 and 2019, the definition was embedding at least 1 AI capability in business processes or products. Since 2020, the definition has been that the organization has adopted AI in at least 1 function.
Source: McKinsey Global Survey on AI, 1,363 participants at all levels of the organization, Feb 22–Mar 5, 2024

McKinsey & Company

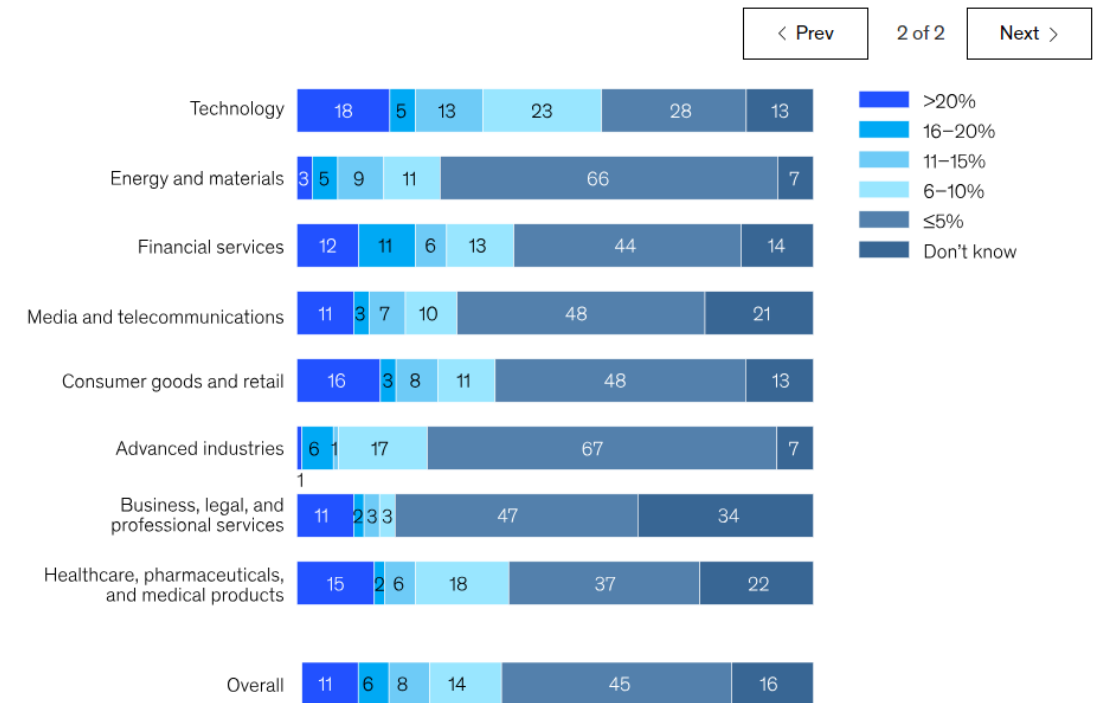
In most industries, organizations are about equally likely to invest more than 5 percent of their digital budgets in generative AI and analytical AI.

Share of organization's digital budget spent on generative AI,¹ % of respondents



In most industries, organizations are about equally likely to invest more than 5 percent of their digital budgets in generative AI and analytical AI.

Share of organization's digital budget spent on analytical AI technology,¹ % of respondents



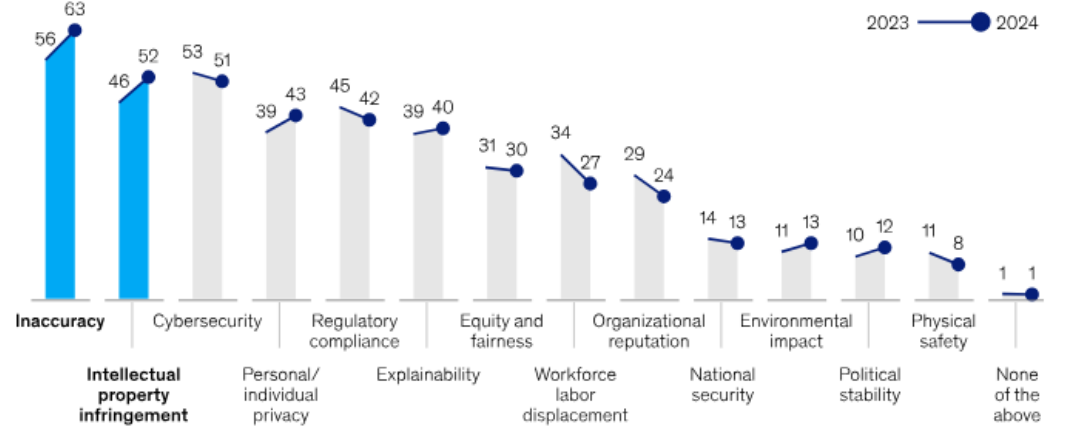
Nearly one-quarter of respondents say their organizations have experienced negative consequences from generative AI's inaccuracy.

Generative-AI-related risks that caused negative consequences for organizations,¹% of respondents



Inaccuracy and intellectual property infringement are increasingly considered relevant risks to organizations' generative AI use.

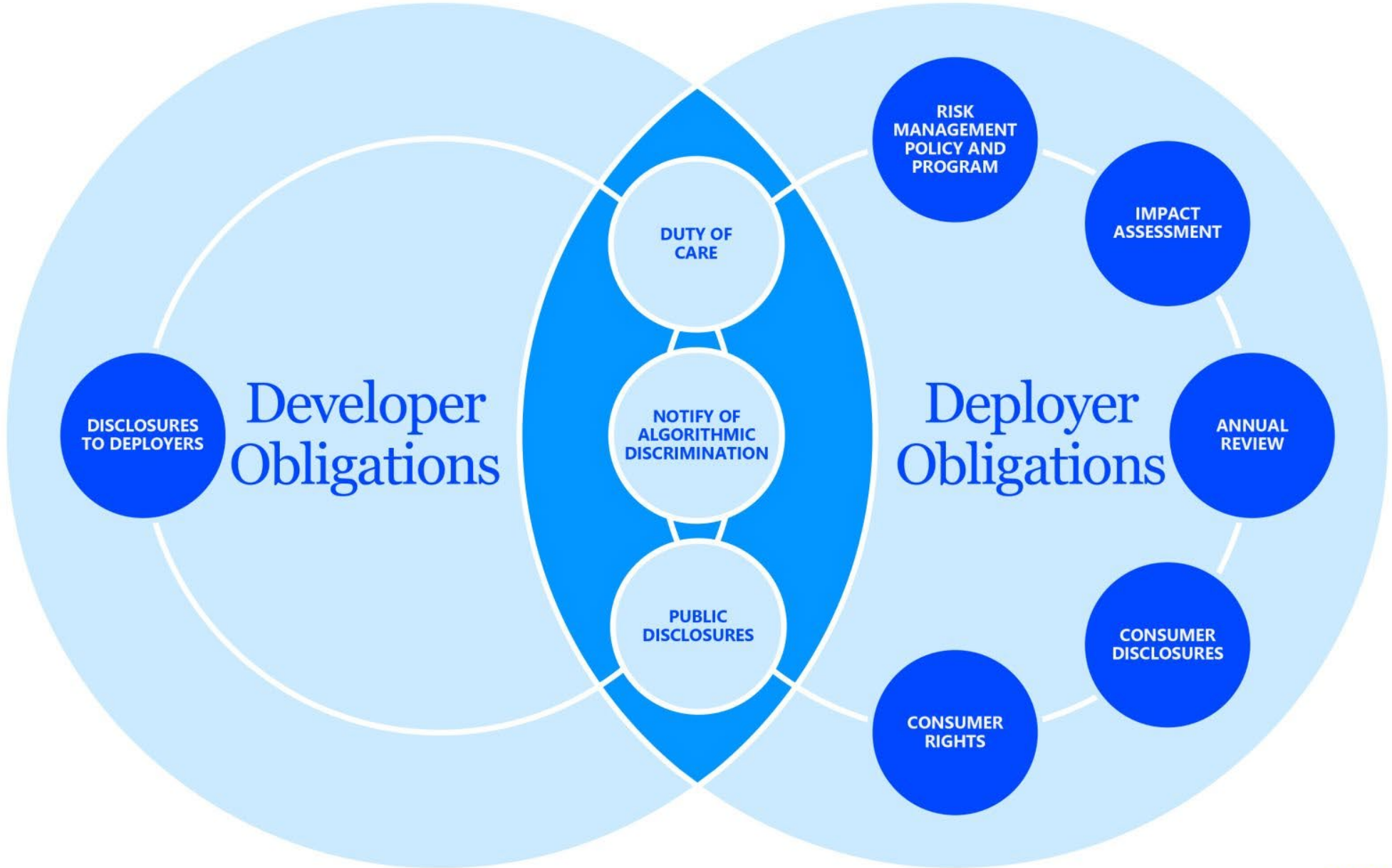
Gen AI risks that organizations consider relevant,¹% of respondents



Gen AI risks that organizations are working to mitigate,¹% respondents



Colorado AI Act: Developer v. Deployer Obligations



Grading Foundation Model Providers' Compliance with the Draft EU AI Act

Source: Stanford Center for Research on Foundation Models (CRFM), Institute for Human-Centered Artificial Intelligence (HAI)

	OpenAI	cohere	stability.ai	ANTHROPIC	Google	BigScience	Meta	AI21labs	ALEPH ALPHA	EleutherAI	Totals
Draft AI Act Requirements	GPT-4	Cohere Command	Stable Diffusion v2	Claude 1	PaLM 2	BLOOM	LLaMA	Jurassic-2	Luminous	GPT-NeoX	
Data sources	● ○ ○ ○	● ● ● ○	● ● ● ●	○ ○ ○ ○	● ● ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	22
Data governance	● ● ○ ○	● ● ● ○	● ● ○ ○	○ ○ ○ ○	● ● ● ○	● ● ● ●	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	19
Copyrighted data	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	7
Compute	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	● ○ ○ ○	● ● ● ●	17
Energy	○ ○ ○ ○	● ○ ○ ○	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	16
Capabilities & limitations	● ● ● ●	● ● ● ●	● ● ● ●	● ○ ○ ○	● ● ● ●	● ● ● ○	● ● ○ ○	● ● ○ ○	● ○ ○ ○	● ● ● ○	27
Risks & mitigations	● ● ● ○	● ● ○ ○	● ○ ○ ○	● ○ ○ ○	● ● ● ○	● ● ○ ○	● ○ ○ ○	● ● ○ ○	○ ○ ○ ○	● ○ ○ ○	16
Evaluations	● ● ● ●	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ○ ○	● ● ● ○	● ● ○ ○	○ ○ ○ ○	● ○ ○ ○	● ○ ○ ○	15
Testing	● ● ● ○	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ○ ○	● ● ○ ○	○ ○ ○ ○	● ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	10
Machine-generated content	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	● ○ ○ ○	● ● ● ○	21
Member states	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ○ ○	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ○ ○ ○	● ● ○ ○	9
Downstream documentation	● ● ● ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	● ● ● ●	● ● ● ●	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	24
Totals	25 / 48	23 / 48	22 / 48	7 / 48	27 / 48	36 / 48	21 / 48	8 / 48	5 / 48	29 / 48	

STANFORD UNIVERSITY: DO FOUNDATION MODEL PROVIDERS COMPLY WITH THE DRAFT EU AI ACT?

National Institute of Standards and Technology (NIST) AI Risk Management Framework

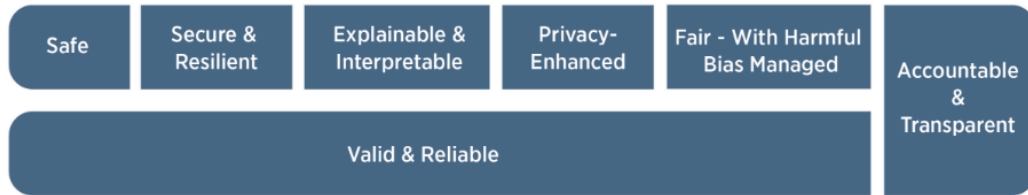


FIGURE 4: CHARACTERISTICS OF TRUSTWORTHY AI SYSTEMS. VALID & RELIABLE IS A NECESSARY CONDITION OF TRUSTWORTHINESS AND IS SHOWN AS THE BASE FOR OTHER TRUSTWORTHINESS CHARACTERISTICS. ACCOUNTABLE & TRANSPARENT IS SHOWN AS A VERTICAL BOX BECAUSE IT RELATES TO ALL OTHER CHARACTERISTICS.

Examples of Potential Harms

Harm to People

- Individual: Harm to a person's civil liberties, rights, physical or psychological safety, or economic opportunity.
- Group/Community: Harm to a group such as discrimination against a population sub-group.
- Societal: Harm to democratic participation or educational access.

Harm to an Organization

- Harm to an organization's business operations.
- Harm to an organization from security breaches or monetary loss.
- Harm to an organization's reputation.

Harm to an Ecosystem

- Harm to interconnected and interdependent elements and resources.
- Harm to the global financial system, supply chain, or interrelated systems.
- Harm to natural resources, the environment, and planet.

AI Risk Management Framework



Map

Context is recognized and risks related to context are identified

Measure

Identified risks are assessed, analyzed, or tracked

Govern

A culture of risk management is cultivated and present

Manage

Risks are prioritized and acted upon based on a projected impact

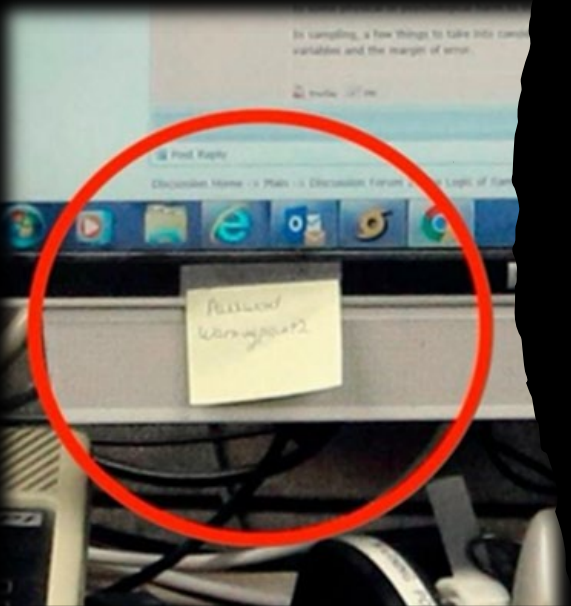


What Now?



The Basics of Evaluating Data Risk

- WHAT data does an organization have?
- WHERE is the data coming from? Going to?
- WHO has access to the data?
- WHEN is the data collected and deleted?
- WHY does the organization have the data?
- HOW is the organization protecting the data?



Consider both
the Technology
Factor and the
People Factor

Practically Speaking...

Carry out due diligence and assessments, as well as keeping up to date with legal developments.




Identify as many similarities to approaches across jurisdictions as possible.



Where there are inconsistencies/differences, either:

Choose the strictest law/regulation, or

Evaluate the risk associated with non-compliance or partial in certain areas



Get comfortable being uncomfortable.



DO SOMETHING

- Analysis paralysis is real
- Establish achievable tasks/steps
- Don't overcomplicate those tasks/steps
- Take it one step at a time

HUSCHBLACKWELL

Questions?



Brad Hammer

PARTNER

MINNEAPOLIS

PHONE: 612.852.2710

FAX: 612.852.2701

EMAIL: BRAD.HAMMER@HUSCHBLACKWELL.COM

