

# Privacy Law Update 2023

Alexander (Sandy) R. Bilus

Partner, Chair of Cybersecurity & Privacy  
Saul EwingLLP  
Alexander.Bilus@saul.com

Kenneth J. Liddle

Chief Compliance Officer and Assistant General Counsel  
Northeastern University  
Ke.Liddle@northeastern.edu



**Northeastern  
University**

# Topics for Today's Discussion

## General Discussion on Privacy Programs

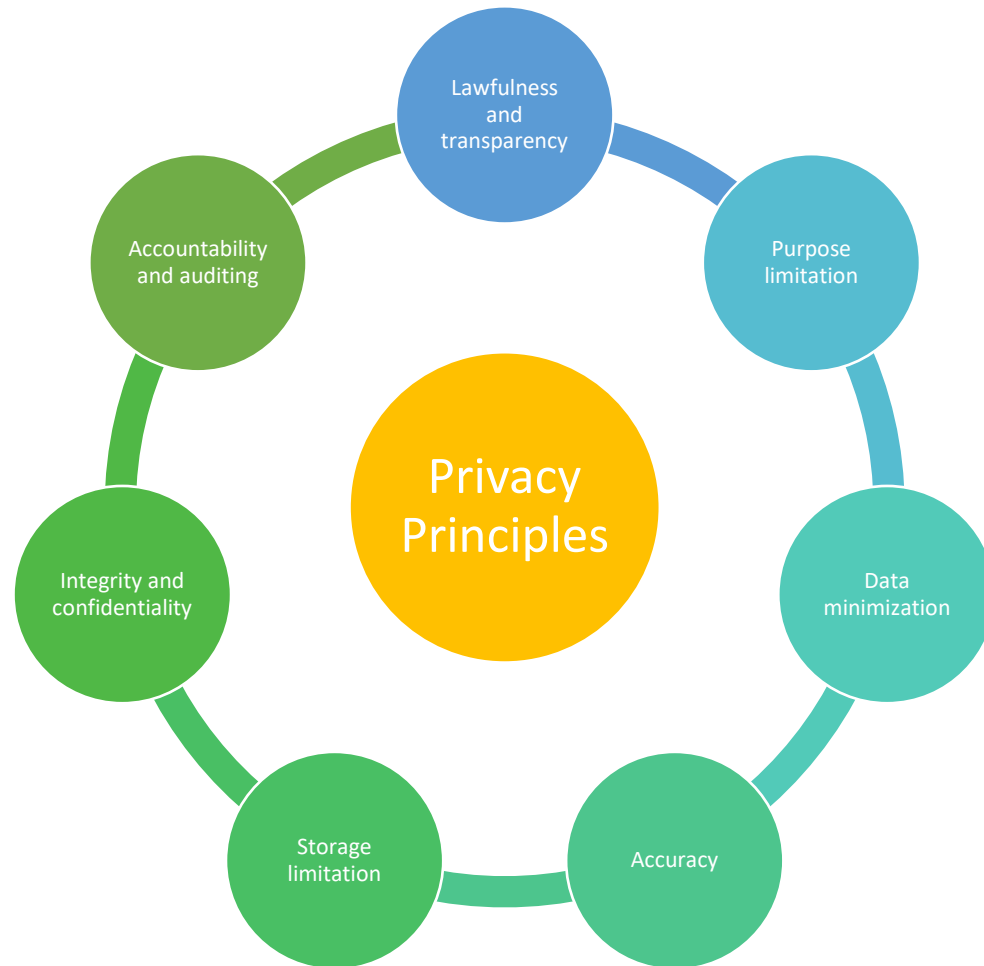
## Privacy Law Roundup

- GLBA
- HIPAA
- State Privacy law
- Biometrics
- International Privacy Law
  - Trends
  - EEA/EU/UK GDPR
  - China PIPL

## Artificial Intelligence

# The Privacy Principles

---



# Privacy Compliance Steps

Initial and ongoing assess-ments

Privacy notices

Consent forms

Policies/  
processes

Contracts

Training

# The Chief Privacy Officer



Do you have one?



What are the responsibilities and duties of a CPO?


- Governance
- Policies
- Assessment
- Training
- Incident Response
- Monitoring/Auditing

# Gramm- Leach-Bliley Act (GLBA)

## Security Rule

- Requires Written Information Security Program (WISP), effective June 9, 2023
- “Encouraged” to use [NIST 800-171 \(Rev 3\)](#) (Updated May 10, 2023)
- [Guidance from the Dept of Ed](#) (February 9, 2023), defines the scope of GLBA data
  - Broadly defined to cover most loan activities, and data used to “administer or aid in the administration of the Title IV programs”

## Privacy Rule

- Remember - Compliance with FERPA is considered compliance with GLBA’s privacy rule, but not security rule
- 

# GLBA Written Information Security Plan (WISP)

## **Requires WISP with nine elements:**

1. Designate a “qualified individual” for information security
2. Information security risk assessments
3. Inclusion of safeguards (based on those risks)
4. Regular testing/monitoring of safeguards
5. Appropriate policies and procedures
6. Some structure of governance/oversight
7. Continuous improvement

If maintaining the information of over 5,000 students, additionally:

8. Established incident response plan
9. Qualified Individual must report at least annually to the controlling body (ie. Board).

See 16 C.F.R. 314.4

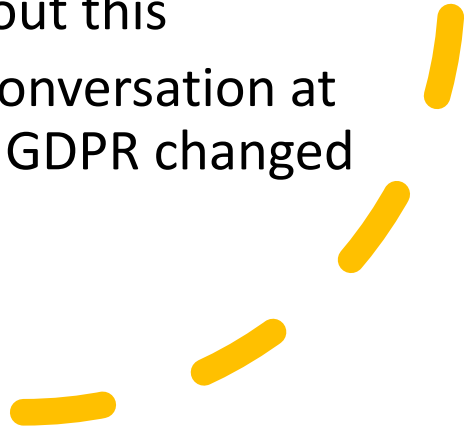
# Federal Privacy Laws

## HIPAA

- Notice of Proposed Rulemaking, December 2020, expected implementation Summer 2023
  - Focus on patient access to records, reducing time to responded from 30 days to 15 days
  - Reduces and caps fees patients can be charged for records
- COVID Flexibilities ending
  - Return to normal enforcement
- What to expect
  - more records requests,
  - those requests to cover more data (including billing records),
  - reduced ability to offset the cost, and
  - more enforcement
- Start planning!
- Remember – if data is FERPA, then by definition it is not HIPAA



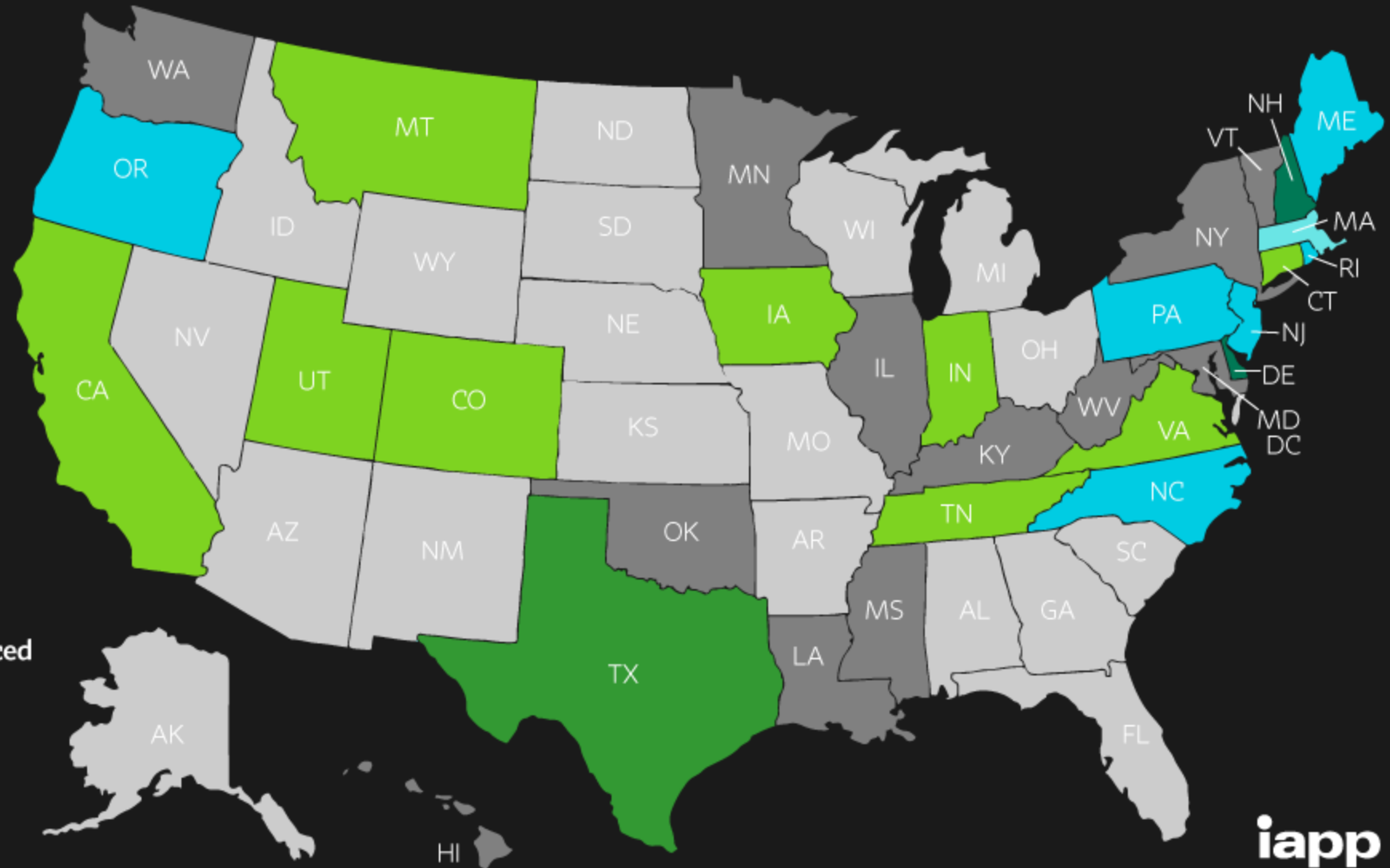
# Federal Privacy Laws

- SEC Cybersecurity Rules
    - Expected to take effect Summer 2023
    - Requirements for regulated companies
      - Defined cybersecurity risk policies and procedures;
      - The Board must annually assess the design and effectiveness of these policies and procedures; and
      - SEC and public notification of any “significant cybersecurity incident”
  - Interesting, but why are we talking about the SEC?
    - Possible direct application (depending on bond or funding activities), but likely limited for most schools
    - More importantly, anticipate that your board members will be hearing about this and asking about this
    - Potential to fundamentally change the conversation at the national level (much in the way that GDPR changed the global privacy conversation)
- 

# US State Privacy Legislation Tracker 2023

## STATUTE/BILL IN LEGISLATIVE PROCESS

- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced



🔄 Last updated: 6/9/2023

# State Privacy Laws

STATE	LEGISLATIVE PROCESS	STATUTE/BILL (HYPERLINKS)	COMMON NAME	CONSUMER RIGHTS								BUSINESS OBLIGATIONS					
				Right to access	Right to correct	Right to delete	Right to opt out of certain processing	Right to portability	Right to opt out of sales	Right to opt in for sensitive data processing	Right against automated decision making	Private right of action	Opt-in default (requirement age)	Notice/transparency requirement	Risk assessments	Prohibition on discrimination (exercising rights)	Purpose/processing limitation
<b>LAWS SIGNED (TO DATE)</b>																	
California		<a href="#">CCPA</a>	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	X		X		X	X			L	16	X			X
		<a href="#">Proposition 24</a>	California Privacy Rights Act (2020; fully operative Jan. 1, 2023)	X	X	X	S	X	X		X	L	16	X	X	X	X
Colorado		<a href="#">SB 190</a>	Colorado Privacy Act (2021; effective July 1, 2023)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Connecticut		<a href="#">SB 6</a>	Connecticut Data Privacy Act (2022; effective July 1, 2023)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Indiana		<a href="#">SB 0005</a>	Indiana Consumer Data Protection Act (2023; effective Jan. 1, 2026)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Iowa		<a href="#">SF 262</a>	Iowa Consumer Data Protection Act (2023; effective Jan. 1, 2025)	X		X		X	X		X-		S/13	X		X	X
Montana		<a href="#">SB 384</a>	Montana Consumer Data Privacy Act (2023, effective Oct. 1, 2024)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Tennessee		<a href="#">HB 1181</a>	Tennessee Information Protection Act (2023; effective July 1, 2024)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Utah		<a href="#">SB 227</a>	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)	X		X	P	X	X				13	X		X	
Virginia		<a href="#">SB 1392</a>	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X

A - risk assessments for limited purposes only  
 IN - opt-in consent requirement  
 L - private right of action limited to certain violations only  
 P - right to opt-out of processing for profiling/targeted advertising purposes  
 S - sensitive data  
 X - right or obligation exists  
 ~ - right to opt out of certain automated decision making

# US State Law Privacy Compliance Checklist

Are you in scope?

If so:

- Privacy Policies & Notices
- Consent Forms
- Contracts
- Responding to Rights Requests
- Privacy Impact Assessments
- Security – risk assessment and administrative, technical, and physical measures

# New Privacy Litigation Trend: Website Data Collection Lawsuits

---

Wave of class action  
lawsuits

Targeting  
companies that  
collect  
information  
about their  
website users

Do you use:

- Cookies?
- Web beacons?
- The Facebook/Meta Pixel?
- Google Analytics?
- Chat Bots?
- Session Replay Software?

# New Privacy Litigation Trend: Website Data Collection Lawsuits

---

## Privacy Policy

- Disclose use of data collection tools
- Disclose what is collected and why
- Disclose what is shared with third parties and why

## Terms of Use

- Consider arbitration provision
- Consider venue provision

## Cookie Banner

- Ask for affirmative agreement



# Biometric Update

# Biometric Background

---

What is biometric data?

---

Why is biometric data important?

---

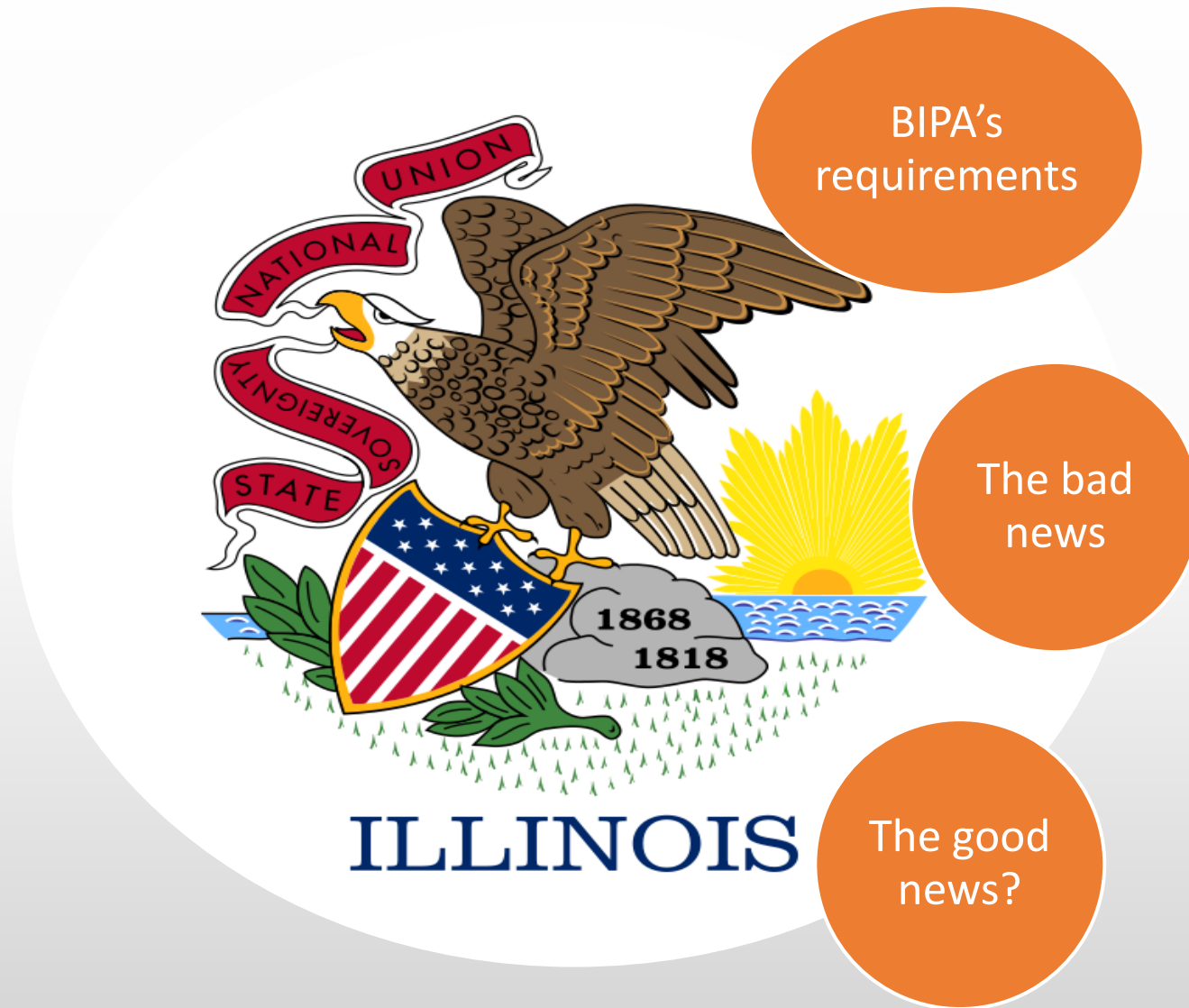
Key Biometric Privacy Laws

---





# Focus on: BIPA





# International Privacy Laws

# Trends in International Privacy

- Continued adoption of personal privacy laws styled on GDPR principles
  - Australia, Brazil, Canada, Chile, China, Egypt, India, Israel, Japan, New Zealand, Nigeria, South Africa, South Korea, Switzerland, Thailand, Turkey, EU, and UK
- Over 130 countries have some type of national data privacy law
- EU/EEA/UK still the “gold” standard

# EU/EEA/UK Update

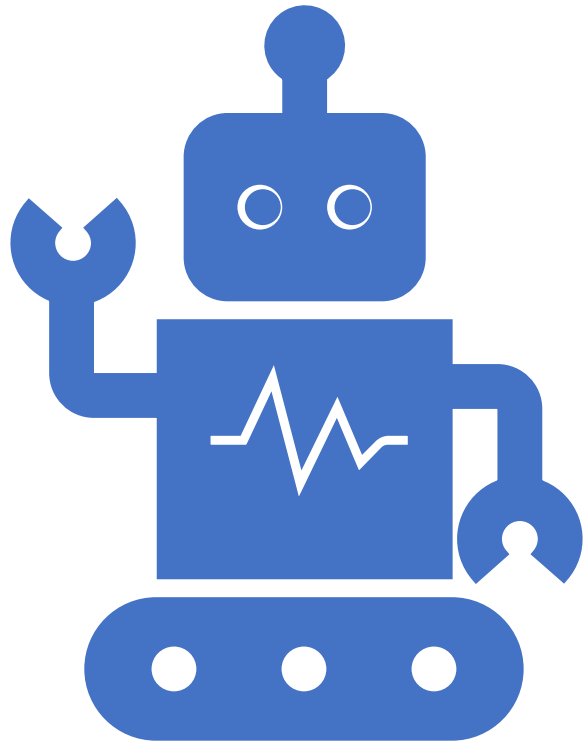
---

- **The most common way to legally transfer personal information to the US is the use of the NEW standard contractual clauses (SCC)**
  - Review your contracts, starting with the enterprise level contracts with the most personal data (such as those used for email, student records, and HR).
  - UK contracts using the old SCC must be updated to new SCC by March 21, 2024 (and all EU/EEA contracts should already be updated)
  - Clauses referencing the “Privacy Shield” self certification program are no longer valid
- **Negotiations on the EU-US Data Privacy Framework**
  - Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, October 22, 2022
  - Both the European Parliament and European Data Protection Board issued non-binding resolutions calling on the European Commission to reject the EU-U.S. Data Privacy Framework
  - The adequacy of the Framework is still under review by the European Commission
- **Review your privacy policy. We all updated them in 2018, but that was a long, long time ago!**
- **Also, think about record retention – what is a minimum, and what is a maximum?**

# China

---

- Personal data is covered by a trio of laws - Cybersecurity Law ("CSL"), the Personal Information Protection Law ("PIPL") and the Data Security Law ("DSL").
- Similar to GDPR in many respects, but with increased direct oversight by the government (Cybersecurity Administration of China (the "CAC"))
- PIPL Article 38 outlines three adequate cross-border transfer mechanisms for sending personal information of Chinese individuals outside of China:
  - (1) passing a security assessment organized by the CAC,
  - (2) obtaining a certificate from a CAC-recognized professional organization, or
  - (3) entering into standard contractual clauses

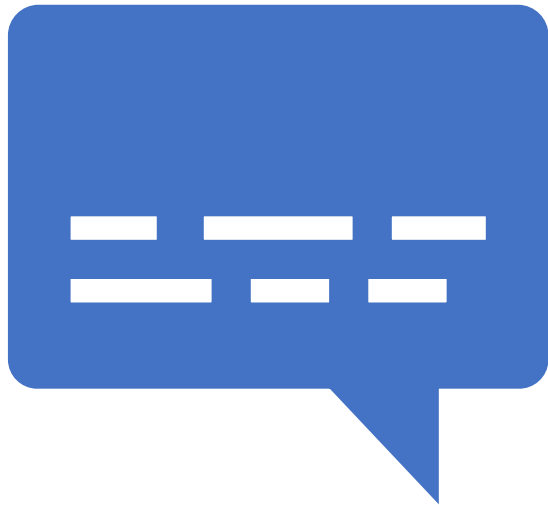


Artificial Intelligence



# Common Concerns with AI

- Notice/Transparency
- Data Minimization
- Use Limitations
- Data Subject Rights
- Automated Decision Making / Discrimination
- The unknowable future!



## Prompt: Write a short bullet point list about the privacy and data security concerns raised by the use of generative AI.

- **Unauthorized data synthesis:** Generative AI models can potentially synthesize realistic data, including text, images, and videos. This raises concerns about the creation and dissemination of misleading or fabricated content, leading to potential misuse and harm.
- **Identifiable information leakage:** Generative AI models trained on large datasets might inadvertently include personal or sensitive information in the generated outputs. This could result in unintended exposure of private data and pose risks to individuals' privacy.
- **Deepfake proliferation:** Generative AI techniques can be used to create highly convincing deepfake videos and audio recordings, making it difficult to distinguish between real and fake content. This raises concerns about the misuse of deepfakes for defamation, fraud, or other malicious purposes.
- **Lack of accountability:** As generative AI models become more sophisticated, it becomes increasingly challenging to trace the origin and authenticity of generated content. This lack of accountability can enable malicious actors to evade responsibility for their actions, leading to legal and ethical challenges.
- **Biased and unfair outcomes:** Generative AI models learn from the data they are trained on, which can inadvertently include biases present in the training data. This can lead to the generation of biased content, perpetuating and amplifying existing societal biases and discrimination.
- **Data security vulnerabilities:** Generative AI models often require large amounts of data for training, leading to potential vulnerabilities in data storage and processing. If these models are not adequately secured, they can become targets for attacks, resulting in the exposure or theft of sensitive information.
- **Consent and ownership issues:** The use of generative AI raises questions about consent and ownership of the generated content. In cases where personal data or copyrighted material is involved, it becomes essential to address these concerns and establish clear guidelines for ownership and usage rights.
- **Regulatory and legal challenges:** The rapid advancement of generative AI has outpaced the development of comprehensive regulations and legal frameworks. This creates challenges in ensuring the responsible and ethical use of these technologies while protecting individuals' privacy and data security.



# Emerging Guidance and Framework

- 
- United States
    - White House OSTP: AI Bill of Rights
    - Joint Senate Commerce & Judiciary sub-cmte
    - NIST AI Risk Management Framework
  - Europe
    - EU AI Act
      - Established Four levels of AI risk
      - Registration requirement demonstrating compliance evaluation
      - Brings AI under the product liability framework
    - Italian DPA temporary ban on ChatGPT
    - French & UKA DPAs issue AI guidance

