Privacy Law Update

Alexander (Sandy) R. Bilus

Partner, Co-Chair of Cybersecurity & Privacy

Saul Ewing Arnstein & Lehr LLP

Alexander.Bilus@saul.com

Kenneth J. Liddle

Chief Compliance Officer and Assistant General Counsel

Northeastern University

Ke.Liddle@northeastern.edu

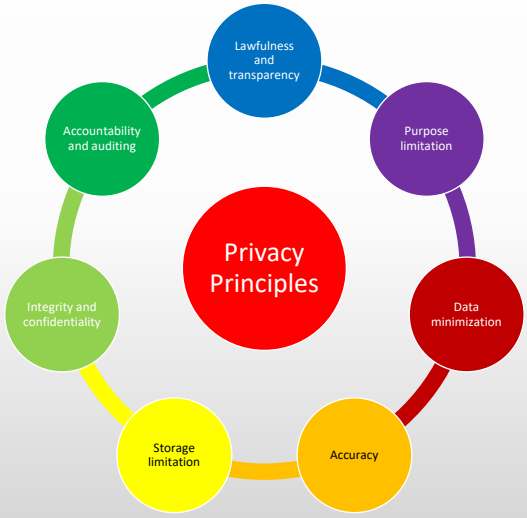
1

Topics for Today's Discussion

- Privacy Principles
- Privacy Law in the United States
  - With a focus on state law and biometrics
- International Privacy Law
- Compliance Strategies and Best Practices

2

The Privacy Principles



3

Federal Privacy Laws

- Sector based protections:
  - FERPA - Educational records
    - CUI or not?
  - GLBA - Consumer financial products and services
    - New regulations effective end of 2022
    - Don't forget the FTC Red Flags Rule
  - HIPAA - Patient health information
    - If it's FERPA, it's NOT HIPAA!
    - See Joint Guidance, updated December 2019
- Currently 15 bills pending in the US House and Senate

4

State Privacy Laws

5

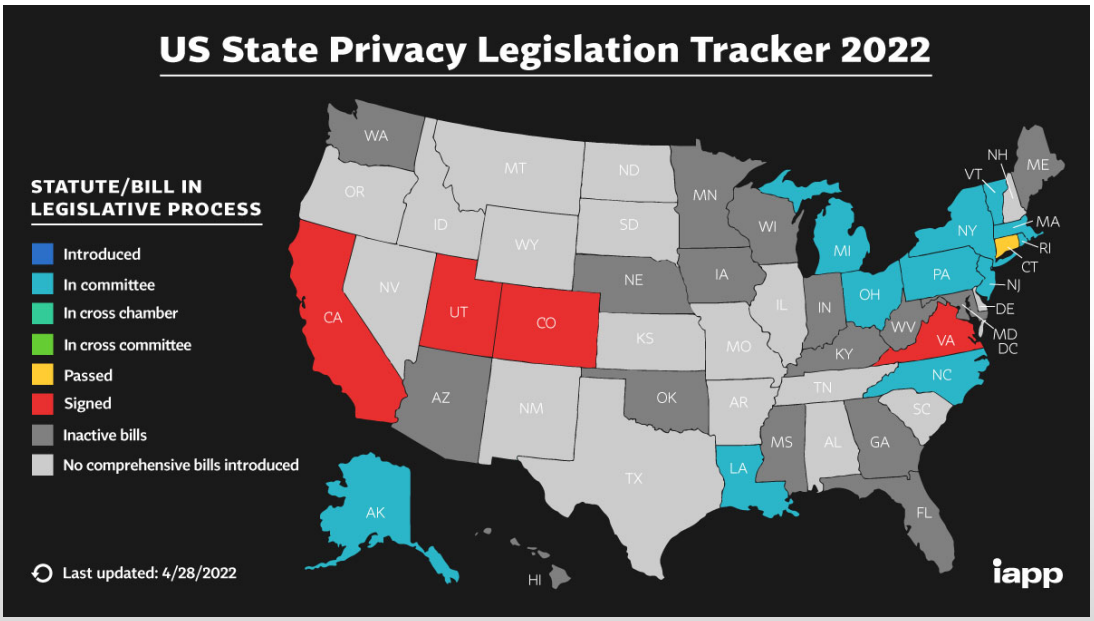
The State Privacy Legislation Landscape

Passed and signed:
- California (x 2)
- Virginia
- Colorado
- Utah
- Connecticut

Active bills:
- AK, LA, MA, MI, NJ, NY, NC, OH, PA, RI, VT

Inactive bills:
- AZ, FL x 2, GA, HI x 4, IN, IA, KY, ME, MA x 3, MN, MI, NE, OK x3, WA x4, WV, WI x4

6



Source: "US State Privacy Legislation Tracker," produced by the International Association of Privacy Professionals originally appeared in the IAPP Resource Center. It is reprinted with permission.

7

Scope of State Law Privacy Laws

US State Privacy Legislation Tracker 2022

Comprehensive Consumer Privacy Bills

STATE	LEGISLATIVE PROCESS	STATUTE/BILL (HYPERLINKS)	COMMON NAME	CONSUMER RIGHTS: Right of access	Right of rectification	Right of deletion	Right of restriction	Right of portability	Right to opt out of sales	Right against automated decision making	Private right of action	BUSINESS OBLIGATIONS: Opt-in default (requirement age)	Notice/transparency requirement	Risk assessments	Prohibition on discrimination (exercising rights)	Purpose/processing limitation
LAWS SIGNED (TO DATE)																
California		CCPA	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	X		X		X	X		L	16	X			X
		Proposition 24	California Privacy Rights Act (2020; effective Jan. 1, 2023)	X	X	X	S	X	X	X	L	16	X	X	X	X
Colorado		SB 190	Colorado Privacy Act (2021; effective July 1, 2023)	X	X	X	P	X	X	X~		S/13	X	X	X	X
Virginia		SB 1392	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)	X	X	X	P	X	X	X~		S/13	X	X	X	X
Utah		SB 227	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)	X		X	P	X	X			13	X		X	
Connecticut		SB 6		X	X	X	P	X	X	X~		S/16	X	X	X	X

A - risk assesments 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

Source: "US State Privacy Legislation Tracker," produced by the International Association of Privacy Professionals originally appeared in the IAPP Resource Center. It is reprinted with permission.

8

Scope of State Law Privacy Laws

- All states have one or more tests for when the law applies, including to entities outside the state
- At this time, only Colorado applies directly to non-profits
- In all states with a privacy law, the law will still apply to any for-profit entities that are contracting with a non-profit
- Carefully consider privacy related terms in contacts that involve large datasets (e.g. software applications)

9

Biometric Privacy Laws

10

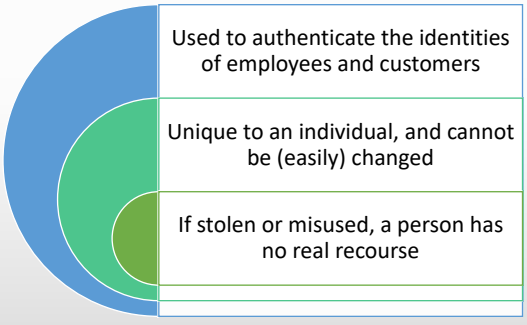
What are biometrics and biometric data?

Biometrics is a way to measure a person's physical characteristics to verify their identify, including physiological traits or behavioral characteristics.

- Fingerprints
- Hand geometry
- Facial geometry (not photographs)
- Retina/iris scans
- Voiceprints
- Behavioral characteristics

11

Why is biometric information important?



12

Key biometric privacy laws

- Illinois Biometric Information Privacy Act (BIPA)
- Texas Capture or Use of Biometric Identifier Act (CUBI)
- Washington HB 1493
- Municipalities: New York City, Portland
- Other privacy laws that sweep in biometric information:
  - State laws: California's CCPA/CPRA, Virginia's CDPA, some state breach notification laws
  - Federal laws: HIPAA, FERPA, COPPA
  - International laws: GDPR, Brazil's LGPD

13

International Privacy Laws

14

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 120 countries have some type of national data privacy law

15

EU/EEA and UK Update

- Any contract that includes the transfer of personal data to the USA must include the NEW standard contractual clauses (SCC)
  - EU/EEA contracts using the old SCC must be updated to new SCC by December 27, 2022
  - New UK Addendum to new EU SCC, intended to harmonize the two
  - UK contracts using the old SCC must be updated to new SCC by March 21, 2024
- Many companies/contracts state that they follow the Department of Commerce "Privacy Shield" but that was invalidated by the Court of Justice of the EU and is no longer valid (*Schrems II*)
  - The new reality is SCC and Transfer Impact Assessments

16

China's Personal Information Protection Act (PIPL)

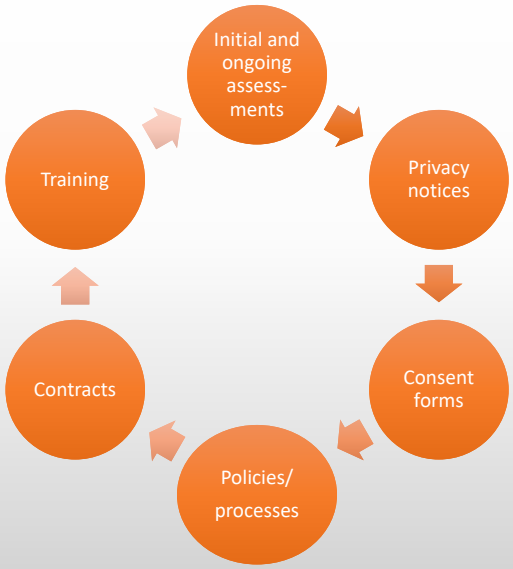
- Effective November 21, 2021, same basic personal rights as GDPR
- Applies to organizations in China, and those outside China that collect or process personal data for the purpose of providing products or services to individuals in China (or analyzing individuals in China)
- International data transfers will need some type of contract (but that template has not been provided yet)
- Must have legal basis for processing (but legitimate interests is not a legal basis!)
- At a certain threshold (undefined), data must be stored in China, and there must a representative in China

17

Compliance Strategies and Best Practices

18

Privacy Compliance Steps

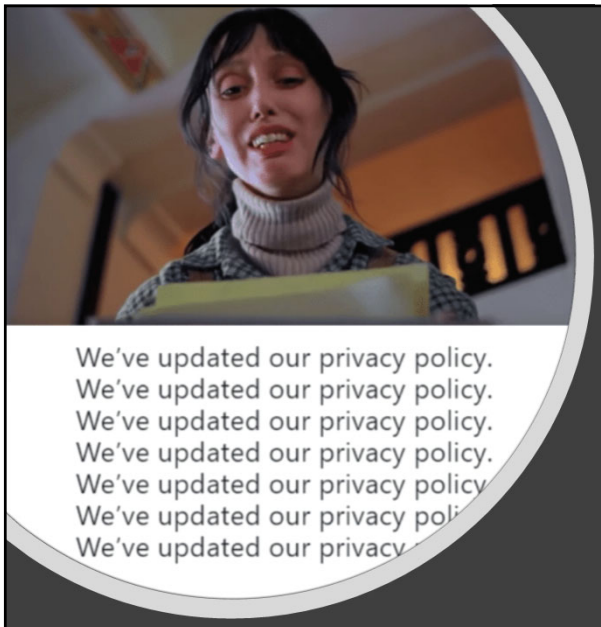


19

Privacy Notices

- Privacy notices
  - Required when personal data obtained from data subject and when personal data is obtained from third party
  - Provide identity and contact info for controller, purpose of the processing, legal basis for the processing (for GDPR), recipients of the data, data retention info, info on transfers outside the EU (for GDPR), jurisdiction-specific descriptions of privacy rights
  - For HIPAA, specific requirements relating to use and disclosure of PHI
- Consent forms
  - Must be written, using "clear and plain" language
  - Don't default to consent as the legal basis for processing

20



Data Inventory and Privacy Notices: Key Provisions

- Scope
- What do you collect?
- How do you collect it?
- For what purpose do you collect it? (Lawful basis?)
- With whom do you share it, and why?
- How do you protect it?
- For how long do you collect it?
- How do individuals exercise their rights and ask questions?
- Do you transfer it across country borders?

21

Privacy Notices: Purpose

- Public-facing document that tells people about your privacy practices
- What do you do with their information?
- How can they exercise control over their information?

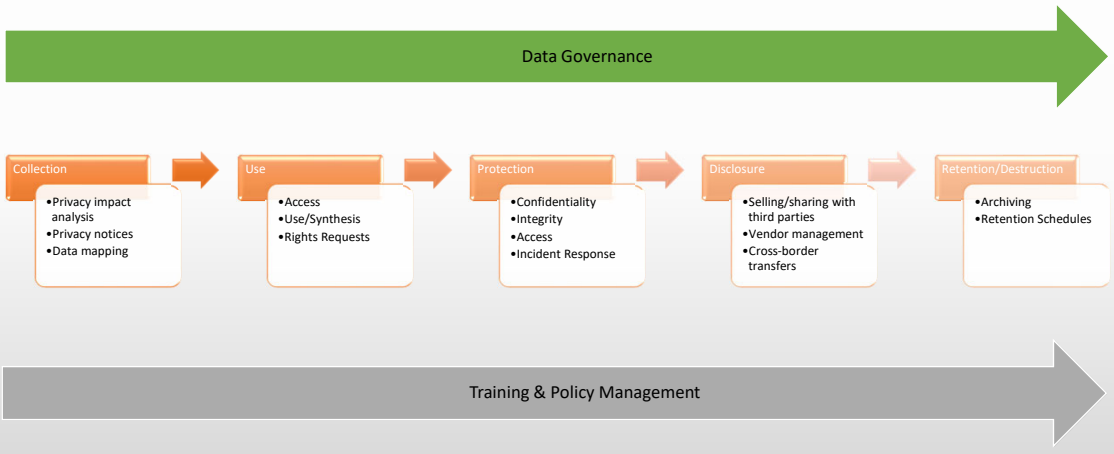
22

Privacy Notices: Dangers for the Unwary

- Copy-pasting someone else's policy
- Inaccuracies
- Outdated statements
- Promises you cannot keep
- Overlapping notices
- Failure to deliver to the right people

23

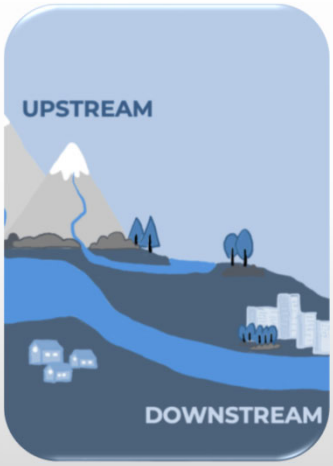
Policies and Procedures



24

Vendor Contracts: Goals

- Your obligations/representations flow to individuals and also flow to vendors you use
- Control use/disclosure of personal information
- Require cooperation
- Reduce and transfer risk
- Avoid system overload



25

Vendor Contracts: Hot Button Issues for Negotiation

- Definitions : E.g., incident, breach, etc.
- Use of data
- Incident response
  - Timing of notification
  - Control over investigation
  - Who pays, and for what?
- Indemnification/limitation on liability issues
- Deletion/retention of data
- Audits and security reviews
- Insurance
- International transfers of personal information

26

Training

Audits

- Training employees
- Maintaining and updating the data inventory
- Evaluate/audit compliance and conduct gap analyses

27

Some more best practices

Privacy Impact Analysis

Working with local outside counsel

How to get resources/attention

Follow the privacy principles

28