KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Navigating the New Data Privacy Landscape

Presented April 11, 2023

Speakers

Devi Mehta
Associate General Counsel for Privacy
Blue Cross Blue Shield Association
Devi.Mehta@bcbsa.com

Meghan Farmer
Partner
Kilpatrick Townsend
MFarmer@kilpatricktownsend.com

Alex Borovsky
Associate
Kilpatrick Townsend
ABorovsky@kilpatricktownsend.com

Jennie Cunningham
Associate
Kilpatrick Townsend
JLCunningham@kilpatricktownsend.com

Zain Haq
Associate
Kilpatrick Townsend
ZHaq@kilpatricktownsend.com

Welcome

Agenda

U.S. Comprehensive Data Privacy Laws

An overview of recently enacted and upcoming comprehensive state privacy laws including applicability, requirements, exemptions, and a case study.

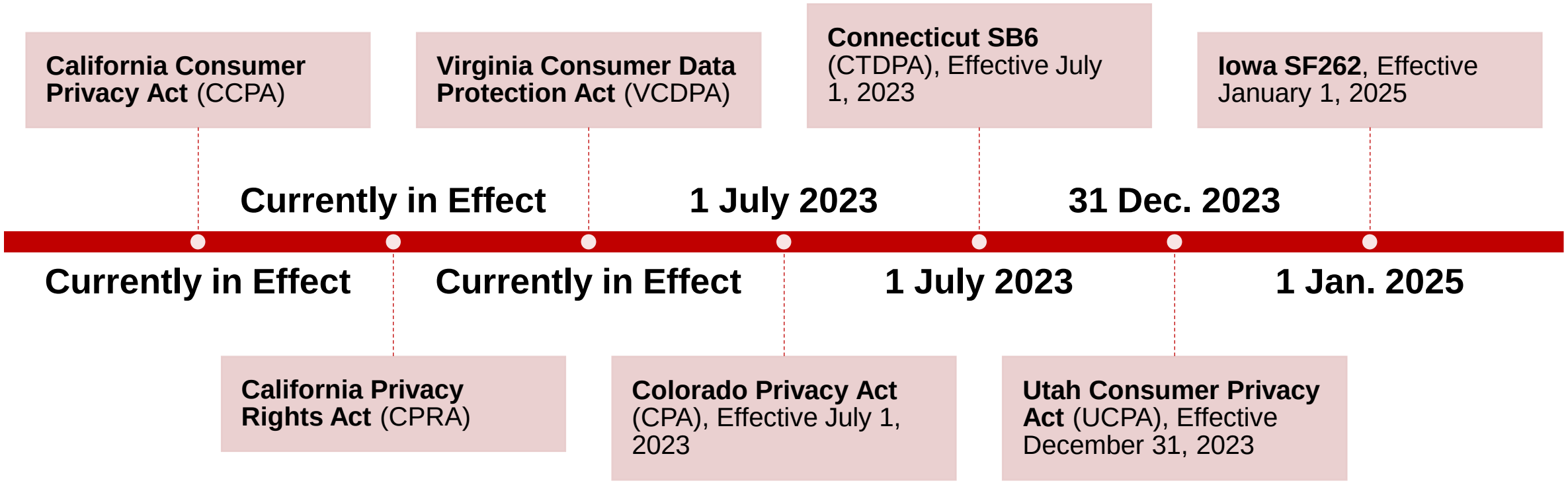
Case Studies

Join us as we examine practical applications of the U.S. state privacy laws to the types of scenarios in-house counsel might face.

U.S. Data Privacy Litigation and Enforcement

A discussion of recent litigation/enforcement trends, what activities can get you in trouble, and some practical considerations to avoid or mitigate risk.

U.S. State Privacy Landscape



Where to Start: What Laws Apply?

- Many organizations skip this step (but should not) – organizations **may not be subject** to all (or any of) the comprehensive U.S. state privacy laws.
- Factors for determining applicability include (among others): (i) an organization's annual revenue; (ii) the number of state residents' the organization controls/processes personal data; and (iii) if the organization is a data broker.
- **Example:** Virginia's Consumer Data Protection Act applies to anyone that conducts business in Virginia or produces products/services targeted to Virginia residents and either:
  - Controls or processes the personal data of at least 100,000 consumers, or
  - Derives more than 50% of its gross revenue from the sale or processing data belonging to at least 25,000 consumers.

General Applicability

CA	VA	CO	CT	UT	IA
Do business in California **AND** 1) annual gross revenue in excess of **$25 million** in the preceding calendar year, 2) annually buys sells, or shares, personal information of **100,000** or more consumers or households, **OR** 3) derives **50% or more annual revenue** from selling/sharing consumers' personal information	Conduct business in Virginia or produces products or services that are targeted to residents of Virginia **AND** 1) during a calendar year, control or process personal data of at least **100,000** consumers, **OR** 2) control or process personal data of at least **25,000** consumers **AND** derive over **50% of gross revenue** from the sale of personal data	Conduct business in Colorado or produces products or services that are intentionally targeted to residents of Colorado **AND** 1) during a calendar year, control or process personal data of at least **100,000** consumers, **OR** 2) control or process personal data of at least **25,000** consumers **AND derives revenue or receives a discount** on the prices of goods or services from the sale of personal data	Conduct business in Connecticut or produces products or services that are targeted to residents of Connecticut **AND** during a calendar year 1) control or process personal data of at least **100,000** consumers **(excluding solely for payment transactions) OR** 2) control or process personal data of at least **25,000** consumers **AND** derive over **50% of gross revenue** from the sale of personal data	Conduct business in Utah or produces products or services that are targeted to residents of Utah **AND** has annual revenue of $25 million or more **AND** 1) during a calendar year, control or process personal data of at least **100,000** consumers, **OR** 2) control or process personal data of at least **25,000** consumers **AND** derive over **50% of gross revenue** from the sale of personal data	Conduct business in Iowa or produces products or services that are targeted to residents of Iowa **AND** during a calendar year 1) control or process personal data of at least **100,000** consumers, **OR** 2) control or process personal data of at least **25,000** consumers **AND** derive over **50% of gross revenue** from the sale of personal data

Potential Exemptions

- Nonprofit Organizations
- HIPAA
- Fair Credit Reporting Act
- Gramm-Leach-Bliley Act
- Children's Online Privacy Protection Act
- Family Educational Rights and Privacy Act
- National Securities Association Under Securities Exchange Act
- Consumer Reporting Agencies
- Air Carriers
- State Versions of These Laws

Data Exemptions: Employee and B2B Data

- Virginia, Colorado, Utah, Connecticut, and Iowa's laws specifically state that a "consumer" does not include an individual acting in an **employment** or **commercial** context.
- The CCPA previously exempted employee data from its scope, but the **CPRA** now applies to employee and B2B data as of January 1, 2023.

Key Considerations for Employee and B2B Data

Employee Data

- Consider providing a separate privacy policy to your California employees
- Re-evaluate how your current DSR process applies to California employees
- Determine whether any of your employment-related contracts need required language under CPRA

B2B Data

- Could the inclusion of B2B data make your organization subject to the CPRA?
- Don’t leap into making this conclusion because of the CPRA’s applicability thresholds (e.g., revenue)

How to Not Mess Up HR with the CPRA

- **Employee Data:** Certain rights under the CPRA may impose a large burden on HR departments in California given that organizations may collect much more data on employees than consumers. In addition, although the CPRA was drafted in a manner intended for consumers, it now applies to employees.
- **Right to Know:** What personal data an organization has for its employees, its sources, and how an organization may use that data is much different than for consumers. This is a reason why a California employee privacy notice may be so important.
- **Right to Delete:** HR records have specific retention periods by law, so requests to delete employee data often cannot be honored. Organizations should be prepared to cite conflicting laws when responding to a request.
- **Right to Correct:** To the extent a process is not already in place, organizations will have to consider how to allow California employees the right to correct inaccurate personal information about them.
- **"Disproportionate Effort":** One way to help address these rights (or at least the obligation to notify third parties to respond to these rights) is developing standards for "disproportionate effort" under CPRA regulations.
- **Minimization:** Data minimization, keeping only necessary records, is also important to reduce the burden of these rights, e-discovery, and the risks of breach of employee information.
- **Preventing Abuse:** Finally, employers will need to carefully consider how to handle requests given that employees are often litigious and certain rights may be exercised for e-discovery purposes.

Key Common Features of U.S. State Privacy Laws

- **Exclude** employee and B2B personal data (not true for California)
- Privacy **notice** requirements
- Consumers **rights** (e.g., right to access, correct, delete, data portability, opt-out of targeted advertising, sale, or profiling)
- **Contract** requirements for processors/service providers
- **Data protection impact assessments** for certain activities (not true for California)
- Rules on the use of **sensitive** data
- Implement reasonable administrative, technical, and physical **data security practices** for personal data
- **No private right of action** (not true for California)
- Enforcement **cure periods** (not true for California)

Enforcement Overview

	CA	VA	CO	CT	UT	IA
Private Right of Action	Failure to implement and maintain reasonable security procedures and practices	None	None	None	None	None
Enforcing Entity	Attorney General, California Privacy Protection Agency	Attorney General	Attorney General, District Attorneys	Attorney General	Attorney General	Attorney General
Cure Period	None	30 days	60 days – expires in 2025	60-days – expires in 2025	30 days	90 days
Penalties	Up to $7,500 per violation	Up to $7,500 per violation	Up to $20,000 per violation	Up to $5,00 per violation	Up to $7,500 per violation	Up to $7,500 per violation

Data Mapping

What is it?

- Determine the source of personal data and the type of personal data your organization processes
- Describe what you are using personal data for
- Determine your processing role (i.e., controller/business or processor/service provider)
- Figure out which third parties have access

Why is it important?

- Not an explicit legal requirement, but the U.S. state privacy laws may limit collection of personal data to what is reasonably necessary or impose other data minimization rules
- Determine your obligations under the U.S. comprehensive data privacy laws
  - E.g., sensitive personal data, entering into data processing agreements

How to do it?

Privacy Policy – Requirements

California (CCPA/CPRA)	Other State Laws (Generally)
• Categories of personal information **described according to the CCPA** • Categories of sources of personal information • Business or commercial purpose for collection • Categories of personal information sold/shared • Categories of third parties to whom sold/shared • Business or commercial purpose for selling/sharing • Whether you have actual knowledge that you sell or share to consumers under 16 • Categories of personal information disclosed to third parties • Categories of third parties' personal information is disclosed to • Business or commercial purpose for disclosure • Whether the business uses or discloses sensitive personal information outside of certain purposes • Explanation of CCPA rights • How consumers can exercise CCPA rights • Notice at collection requirements, including retention periods or retention criteria and a link to take the consumer directly to the CCPA section	• Categories of personal data • Purpose for processing personal data • "Selling" or "Targeted Advertising" and the way a consumer may opt-out • Categories of third parties' personal data is disclosed to • Explanation of consumer rights • How consumers can exercise their rights • How to appeal a controller's actions regarding a consumer rights request • Contact information

Privacy Policy – Practical Considerations

- Organizations are generally moving towards one consumer privacy policy (and one employee privacy policy)
- Accurately reflect what privacy laws are applicable to your organization
- Consider jurisdiction-specific sections (namely CCPA)
- Consider whether to extend consumer rights universally or to specific jurisdictions
- Determine whether to offer “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links
- How do you make sure your privacy policy reflects your organization’s actual practices?

What's a "Sale" Anyways?

According to Law

- "Sale" generally means the exchange of a consumer's personal data to a third party for monetary or **other valuable consideration**
- Virginia, Utah, and Iowa don't include "other valuable consideration" in the definition

According to the California AG

- "Sale" includes online tracking

The SEPHORA Settlement

- **What is it?**
  - First CCPA settlement by the Office of the Attorney General
- **What did Sephora do?**
  - Sephora installed third-party company tracking software on its website and app
  - It stated in its online privacy policy that “we do not sell personal information”
- **What did Sephora not do?**
  - Disclose to consumers it was “selling” their personal information
  - Process user requests to opt-out of “sale” via user-enabled global privacy controls
  - Provide a “Do Not Sell My Personal Information” link
  - Provide two or more designated methods for submitting requests to opt-out of “sale”
- **Why should my organization care?**
  - Pay $1.2 million
  - Various injunctive measures

Online Tracking as a “Sale” – Practical Considerations

Step 1 – Figure Out What You Are Doing

- Learn what tracking technologies our utilized on your websites and applications and which third parties offer them

Step 2 – How to Potentially Avoid a “Sale”

- Obtain consent prior to tracking

Step 3 – How to Comply if You “Sell”

- Make appropriate disclosures surrounding a “sale” in your privacy policy
- Offer “Do Not Sell or Share My Personal Information” link
- Or process opt-out signals in a “frictionless manner”

Privacy Contracting – Requirements

Contract Requirements	CA	VA	CO	CT	UT	IA
Contracts with processing instructions and the nature and purpose of processing	X	X	X	X	X	X
Agreements with sub-processors must impose the same obligations	X	X	X	X	X	X
Types of personal data subject to processing		X	X	X	X	X
Duration of processing		X	X	X	X	X
Rights and obligations of the parties				X	X	X
Ensure each person processing the personal data is subject to a duty of confidentiality		X	X	X	X	X
Upon reasonable request, make available information necessary to demonstrate compliance with applicable data privacy law		X	X	X		X
Allow for, and contribute to, reasonable assessments and audits	X	X	X	X		
Require the deletion or return of all personal information to the controller at the end of the services, unless otherwise required by law		X	X	X		X
Implement appropriate technical and organizational measures			X			
Engage a sub-processor only after providing the opportunity to object			X	X		

Privacy Contracting – Requirements

Contract Requirements	CA	VA	CO	CT	UT	IA
Prohibit selling or sharing personal information	X					
Identify the specific Business Purpose for processing personal information	X					
Prohibit the service provider from retaining, using, or disclosing the personal information: (1) for any purpose other than the Business Purpose; (2) for any commercial purpose other than the Business Purpose; and (3) outside of the direct relationship between service provider and the business.	X					
Comply with all applicable sections of the CCPA, including providing the same level of privacy protection as required of businesses by the CCPA	X					
Grant the business the right to take reasonable and appropriate steps to ensure that service provider uses the personal information in a manner consistent with the business's obligations under the CCPA	X					
Require the service provider to notify the business after it decides that it can no longer meet its obligations under the CCPA	X					
Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider's unauthorized use of personal information	X					
Require the service provider to enable the business to comply with consumer requests or require the business to inform the service provider of the consumer request and comply with the request	X					

Privacy Contracting – Practical Considerations

Practical Implementation

- Consider whether your organization might need a U.S. DPA for your customers or vendors
- Update global DPAs to cover U.S. state data privacy laws, particularly the CCPA
- Identify contracts that implicate personal data and assess if any amendments are required

Most Negotiated Provisions

- Indemnity for breach of the DPA/personal data breach and limitation of liability
- Audit rights
- Costs of personal data breach
- Timing for notices

Sensitive Personal Data – Compliance Strategies

- **Definitions:** There are some differences among the U.S. comprehensive state privacy laws, but "sensitive personal data" may include health data, genetic or biometric data, precise geolocation, certain demographic information (e.g., race, ethnicity, immigration status, and sexual orientation), SSN, and financial account data.
- **Prepare:** Review data maps or conduct data mapping to determine if your organization processes sensitive personal data and for what purposes.
- **Consent:** Some state laws (CA, UT, and IA) are "opt-out" whereas others (VA, CO, and CT) are "opt-in."
- **CPRA:** Potentially implement "Limit the Use of My Sensitive Personal Information" link.
- **Strategize:** Organizations may minimize obligations by masking or changing data to make it not sensitive. Consider whether collection is necessary at all.

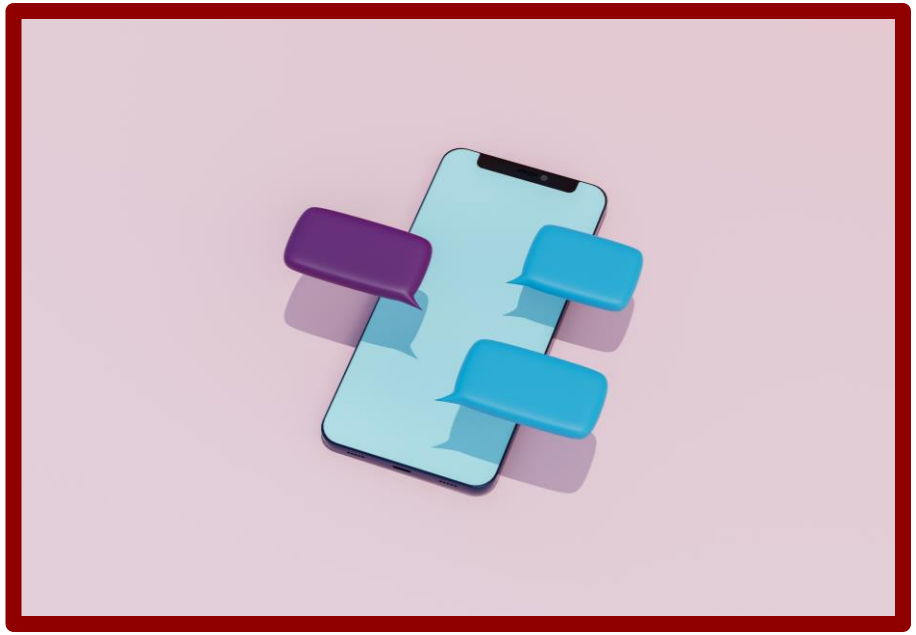
CA	VA	CO	CT	UT	IA
Opt-out	Opt-in	Opt-in	Opt-in	Opt-out	Opt-out

Children's Personal Data

- **Federal** laws related to children's data (i.e., COPPA)
- **FTC enforcement priority:** issue at state and federal level; consider **international** obligations
- VA, CO, CT, and IA include personal data from a known child in the definition of **sensitive** personal data
- **Consent** (parent/guardian):
  - Required to process data of children <13 (VA, CO, UT, CT)
  - Required to sell, share, or process data for targeted advertising purposes of children <16 (CA and CT)
- **Children's Design Code** (CA)
- **Prepare:** work with website, product, marketing, and other relevant teams to understand what is being collected
- **Strategize:** consider data minimization, assess disclosures/consents

Case Study

A Mobile App



The Scenario:

- You are privacy counsel for a highly profitable D.C.-based tech startup that has employees in CO, UT, CA, VA, and CT. This D.C.-based company only operates and has employees in the U.S. The company has a significant number of employees in California.
- A product manager comes to you with a new idea for a mobile app that it designed for the company's own employees (rather than customers) solely for the company's internal use.
- Using health data submitted by employees (like vaccination status) and data collected from other sources (like sick days collected from workday, the app can recommend health-related benefits that the employee may want to take advantage of.
- Additionally, it can provide leadership insights into the most productive members of the workforce.
- How would you analyze this proposal from your product manager? What questions would you ask and what should you consider?

Case Study Part 2

A New Mobile App

The Scenario:

- You are still privacy counsel for a highly profitable D.C.-based tech startup operating in CO, UT, CA, VA and CT. This D.C.-based company only operates and has employees in the U.S.
- Your previous app was so successful internally that now the business would like to make it available to the public, with just a few tweaks to make it relevant to a wider audience.
- The app will be available to anyone who wants to use it via the App Store and Google Play.
- It will still rely on health data submitted by the user (like vaccination status and self-reported health metrics like height, weight, blood pressure, temperature, etc.).
- Using this information, the app will profile the user to create wellness recommendations about how the individual can improve their overall health and wellness.
- How would you analyze this proposal from your product manager? What questions would you ask and what should you consider?

KILPATRICK TOWNSEND

Questions?

KILPATRICK TOWNSEND

U.S. Data Privacy Litigation and Enforcement Updates

Roadmap

- CCPA Enforcement (other than Sephora)
- State Wiretap Laws
- Illinois Biometric Information Privacy Act (BIPA)
- Video Privacy Protection Act (VPPA)
- FTC Enforcement

CCPA Enforcement

- View enforcement examples here: https://oag.ca.gov/privacy/ccpa/enforcement
- Investigations have focused on:
  - Privacy policies not disclosing whether information was sold/shared
  - Failure to post or properly implement the “Do Not Sell or Share My Personal Information” link
  - Opt-out requests for “sale,” including responding to GPC signals
  - Not posting a “Notice of Financial Incentive” in connection with loyalty programs
- **Key Takeaway:** California’s Office of the Attorney General has focused on your organization’s outward privacy disclosures (i.e., your privacy policy). In particular, they have focused on “selling” and “sharing” and related opt-outs.

State Wiretap Litigation: What Gets You in Trouble

- Class action litigation under state wiretap laws with a private right of action is on the rise in **"two-party consent states"** (CA, FL, and PA are most active)
- The two-party consent state statutes require **all parties to consent** to communication being recorded
- **Litigation risk:** any technology that captures a website user's communication/ interaction with the website without their consent
  - E.g., session replay tools → record a user's interactions with the website (e.g., keystrokes, text input, mouse movements)
  - Recent cases have extended to chat bots
- Two case examples:
  - *Javier v. Assurance IQ* → Captured plaintiff answering demographic and medical questions to obtain insurance quote
  - *Yoon v. Lululemon* → Captured plaintiff's mouse movements, keystrokes, pageviews

State Wiretap Litigation: How to Avoid Trouble

- **How to Avoid Risk:**
  - Obtain consent prior to deploying tracking software
  - Practical option – use your cookie banner to obtain opt-in consent
  - Update your privacy policy/cookie policy to include disclosures surrounding your tracking software
  - Record the consent
- **How to Potentially Mitigate Risk:**
  - Include a class action waiver and mandatory arbitration provision in your website terms of use

BIPA: What Gets You in Trouble

- Applies to **Illinois** residents only
- **Litigation risk:** applies to a "**biometric identifier**" or "**biometric information**"
  - "Biometric identifier" includes a: 1) retina or iris scan; 2) fingerprint; 3) voiceprint; 4) scan of hand geometry; or 5) scan of face geometry
  - "Biometric identifier" does not include written signatures, photographs, physical descriptions, such as height, weight, hair color, or eye color, or most information captured from a patient in a healthcare setting
  - "Biometric information" means any information based on an individual's biometric identifier used to identify an individual
- **Substantive exposure for non-compliance:**
  - Private right of action
  - Fines are per violation (*Cothron v. White Castle Sys. Inc.*)
  - Average recovery of $440 per class member (class sizes vary from 724 members to 15.37 million members)

BIPA: How to Avoid Trouble

- Is your organization collecting biometrics (e.g., hand scanner, face verification)?
- Are those biometrics being collected from Illinois residents?
- If so, implement six key BIPA compliance measures:
  1. Provide notice: notice must explain collection, storage, and use of biometrics and the purpose and retention period for such collection, storage, and use
  2. Obtain consent: obtain consent prior to collection
  3. Create a written retention and destruction policy: policy must specify retention period and procedures for permanently erasing biometrics when purpose limitation or 3-year retention period has been met
  4. Ensure your organization does not sell, lease, trade, or profit from biometrics
  5. Do not share biometrics except under limited exceptions: i.e., consent, completion of financial transaction, state/fed law disclosure, warrant/ subpoena
  6. Safeguard your biometric information: under a reasonable standard of care in your organization's industry and in a manner that is the same or more protective than what is applied to confidential/ sensitive information

VPPA: What Gets You in Trouble

- VPPA prohibits a video tape service provider from knowingly disclosing personally identifiable information ("PII") concerning any consumer absent informed consent
- **Litigation Risk:** recent lawsuits focused on organizations sharing PII and viewing practices with social media companies through use of a tracking pixel on a website with an embedded video or audio-video file
- Definition of "PII" may vary depending on the court:
  - Broad approach → transmission of viewing records + GPS coordinates + device unique identification number = PII
  - Narrow approach → must identify a particular person

VPPA: How to Avoid Trouble

- **How to Avoid Risk:** obtain consent, but this is not always practical in this context
- **How to Mitigate Risk:**
  - Include a class action waiver and mandatory arbitration provision in your website terms of use
  - Limit the data being shared with third parties
- **Numerous VPPA Defenses:**
  - Defendant is not a “video tape service provider”
  - Information is not “personally identifiable information”
  - Defendant did not make a “knowing disclosure”
  - Plaintiff is not a “consumer”

Some of you will never know how lit this place would be on a Friday night.

Recent FTC Enforcement

GoodRx (February 1, 2023)

- **Facts:**
  - Stated in its privacy policy it would never disclose personal health information with advertisers or other third parties
  - Used data it shared with social media company to target its users with personalized advertisements
  - Failed to report unauthorized disclosures to such advertisers and other third parties
- **Result:**
  - Required to pay $1.5 million penalty
  - Permanently prohibited from sharing user health information with third parties for advertising
  - Required to obtain user's express consent before disclosing user health information with applicable third parties for other purposes

BetterHelp (March 2, 2023)

- **Facts:**
  - During sign-up process, promised consumers it would not use or disclose their personal health data except for limited purposes, such as to provide counseling services
  - Used and revealed consumers' email addresses, IP addresses, and health questionnaire information to third parties for advertising purposes
- **Result:**
  - Required to pay $7.8 million penalty
  - Permanently prohibited from sharing user health information with third parties for advertising
  - Required to obtain user's express consent before disclosing user health information with applicable third parties for other purposes

KILPATRICK TOWNSEND

Questions?

Locations

Counsel to innovative companies and brands around the world

We help leaders create, expand, and protect the value of their companies and most prized assets by bringing an equal balance of business acumen, technical skill, and creative thinking to the opportunities and challenges they face.

Anchorage
Atlanta
Augusta
Beijing
Charlotte
Chicago
Dallas
Denver
Houston
Los Angeles
New York
Phoenix
Raleigh
San Diego
San Francisco
Seattle
Shanghai
Silicon Valley
Stockholm
Tokyo
Walnut Creek
Washington DC
Winston-Salem