ACC Association of Corporate Counsel
SAN FRANCISCO BAY AREA

MAY 21, 2025

Collecting and Transferring Personal Data Around The World: U.S. and Global Developments In Privacy Laws

ATHERIA LAW

SHOOK HARDY & BACON

Presented By:

Katherine Heaton

Claims Focus Group Leader Cyber and Technology, Cyber Services & InfoSec, Beazley Insurance Services | Denver
Katherine.heaton@beazley.com

Tammy Webb

Partner, Shook | San Francisco
tbwebb@shb.com

Christina Terplan

Partner, Atheria Law| San Francisco
christina.terplan@atherialaw.com

Charlotte Worlock

Partner, Atheria Law| London
charlotte.worlock@atherialaw.com

Camila Tobón

Partner, Shook | Denver
ctobon@shb.com

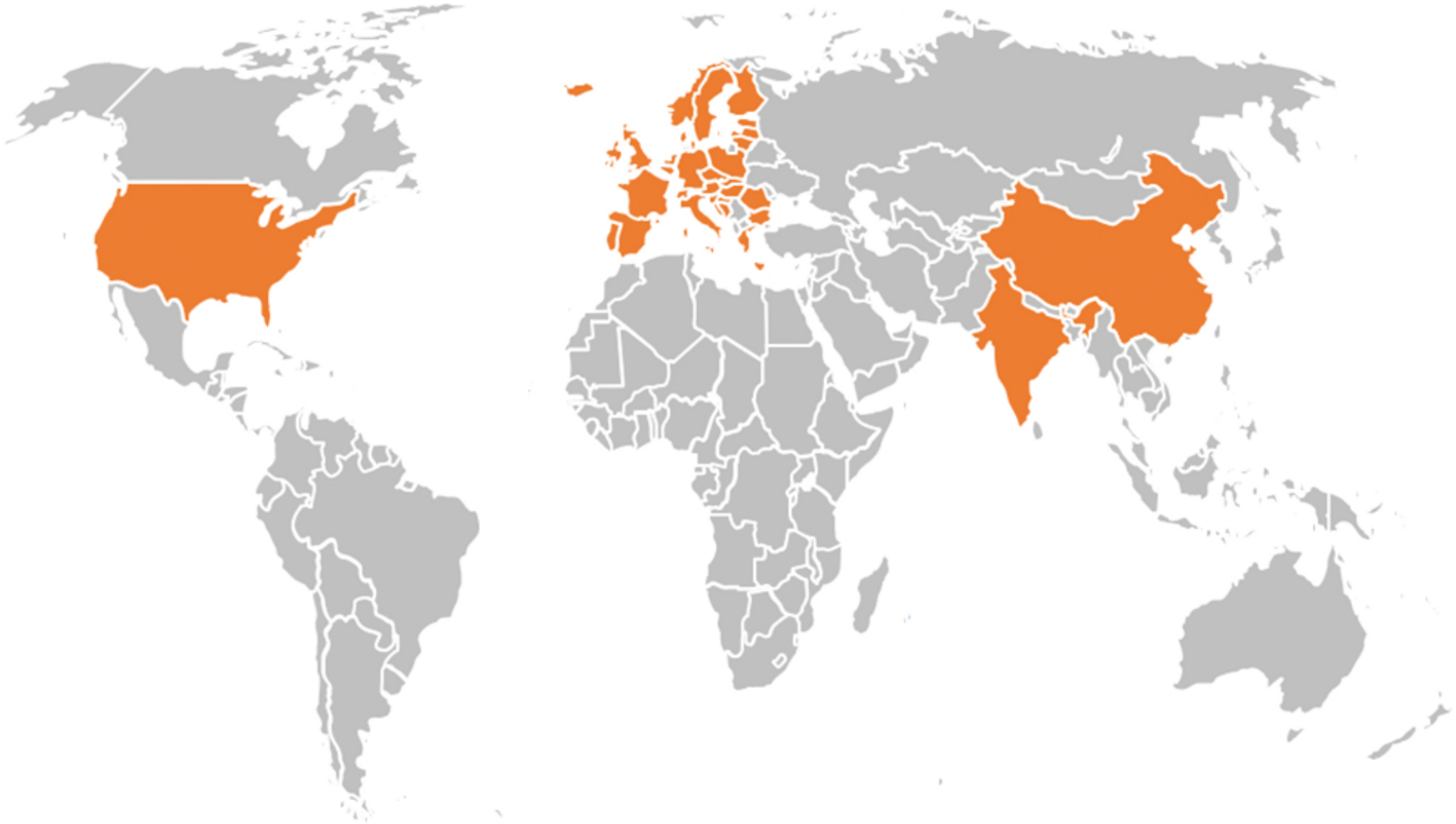
Agenda

- Evolving Global Data Localization Requirements
- Expansion of Collective Redress in the EU and UK
- Conflicting Data Protection Obligations Under US Laws

COLLECTING AND TRANSFERRING PERSONAL DATA AROUND THE WORLD: U.S. AND GLOBAL DEVELOPMENTS IN PRIVACY LAWS

Evolving Global Data Localization Requirements

Areas of Focus



U.S. introduces data localization

- DoJ Data Security Program
  - Rule Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons
- Final Rule published January 8, 2025
- Effective April 8, 2025, but 90-day limited enforcement period in effect until July 8, 2025
- National security rule (not a privacy rule)
  - Imposes prohibitions and restrictions on U.S Persons transferring or granting access to certain types of data to Countries of Concern or Covered Persons

Key Terms

- Countries of Concern
  - China (including Hong Kong and Macau)
  - Cuba
  - Iran
  - North Korea
  - Russia
  - Venezuela
- Covered Persons
  - Foreign entity headquartered in or organized under the laws of a Country of Concern
  - Foreign person residing in a Country of Concern or employee/contractor of a Covered Person Entity of Country of Concern
  - Any person the U.S. designates
  - Foreign entity 50% owned, directly or indirectly, by any of the above or Country of Concern

Key Terms

- Covered Transaction
  - Any transaction that involves any access by a CoC or Covered Person to any government-related data or bulk U.S. sensitive personal data and that involves:
    - Data brokerage;
    - A vendor agreement;
    - An employment agreement; or
    - An investment agreement
- Data Brokerage
  - The sale of data, licensing of access to data, or similar commercial transaction, where the recipient did not collect or process the data directly from the individual

Key Terms

- "Bulk" sensitive data
  - 100
    - Human genomic data
  - 1,000
    - Human 'omic data, Biometric identifiers, Precise geolocation
  - 10,000
    - Personal health or financial data
  - 100,000
    - Covered personal identifiers
  - Any combination of these where the lowest applicable threshold is met

- Covered Personal Identifiers
  - Government ID or account numbers (full or truncated)
  - Financial account numbers or PINs (full)
  - Device-based or hardware-based identifiers (e.g., IMEI, MAC, SIM)
  - Demographic or contact data (e.g., name, address, email, phone, etc.)
  - Advertising identifiers (MAID, Google ad ID, Apple ID, etc.)
  - Account-authentication data (e.g., username and password)
  - Network-based identifier (e.g., IP address or cookie data)
  - Call-detail data (e.g, CPNI)

Requirements

- Prohibited
  - Covered data transaction involving data brokerage with a CoC or a Covered Person (§ 202.301)
  - Any transaction with a foreign person unless the U.S. person:
    - Contractually requires the foreign person to refrain from subsequent covered data transactions involving data brokerage of the same data with a CoC or covered person; and
    - Reports any known or suspected violations of the contractual requirement (§ 202.302)
- Restricted
  - Covered data transaction involving a vendor, employment, or investment agreement with a CoC or a Covered Person
  - U.S. Person must comply with certain specified security requirements (§ 202.401)

Examples

- Prohibited
  - A U.S. subsidiary of a company headquartered in a CoC licenses subscription-based access to a chatbot developed by the U.S. sub, in the U.S., using bulk U.S. sensitive personal data
  - This involves data brokerage because it involves the transfer of data from the U.S. company to the parent licensee, which did not collect or process the data directly from the individuals whose data was used to train the chatbot
- Restricted
  - A U.S. company engages in an employment agreement with a covered person to provide information technology support. As part of their employment, the covered person has access to personal financial data.
  - The U.S. company would be required to implement and comply with the security requirements for the employment agreement to be authorized.

Exemptions

The categories of transactions exempted include:

1. Personal communications
2. Information or informational materials
3. Travel
4. Official business of the U.S. Government
5. Financial services
6. Corporate group transactions
6. Transactions required or authorized by U.S. federal law or international agreements, or necessary for compliance with federal law
7. Investment agreements subject to CFIUS action
8. Telecommunications services
9. Drug, biological product and medical authorizations
10. Other clinical investigations and post-marketing surveillance data

EU Requirements

- The General Data Protection Regulation (GDPR) requires organizations to store and process personal data within the European Union (EU) or in third countries with "adequate" data protection.
- In determining adequacy, Art.45 GDPR indicates European Commission shall take into account:
  - The rule of law and access of public authorities to data in that third country/or to which an organization is subject;
  - Existence of an independent supervisory authority with responsibility for enforcing compliance with data protection rules; and,
  - International commitments the third country/organization has entered into re: protection of personal data.
- Personal data can flow freely from the EU to companies in the United States that participate in the Data Privacy Framework (DPF).

EU - Web Analytics

- Use of tracking pixels and/or Google Analytics requires explicit prior consent from website visitors.
- Consent must be freely given, specific, informed, and unambiguous. If visitor withdraws consent, pixel must be disabled.
- Austrian DPA has banned Meta Pixel. Danish DPA has announced Meta Pixel use is "illegal".
- Swedish DPA has issued several fines for GDPR violations related to companies' use of Meta Pixel, for unlawful transfer of personal data:
  - Apoteket AB - SEK 37 million
  - Apohem AB - SEK 8 million
  - Avanza Bank - SEK 15 million
- French, Austrian, Danish, and Italian DPAs found that Google Analytics' processing of European user data could result in illegally transferring data outside of Europe.

UK Approach

- Since Brexit, UK data protection has evolved:
  - UK General Data Protection Regulation (UK GDPR)
  - Data Protection Act 2018 (DPA)
- EU has deemed UK to have adequate data protection, allowing relatively free flow of data between UK and EU.
- UK focus on data privacy and processing, rather than requiring data to be stored within UK borders.
- Relatively liberal approach to international data transfers (including use of web analytics).

China loosens data transfer restrictions

- New rules aim to reduce the compliance burden on businesses exporting data out of China
- Patchwork of rules
  - Personal Information Protection Law (PIPL)
  - Cybersecurity Law (CSL)
  - Data Security Law (DSL)
  - Cyberspace Administration of China (CAC) regulations

Data Export Requirements

	Data Export Security Assessment (CAC)	Standard Contract or Certification
Critical Information Infrastructure Operators (CIIO)*	X	
Non-CIIO transferring PI	≥ 1M PI records since Jan 1 of the current year (up from ≥ 100k PI since Jan 1 of the previous year)	≥ 100k but < 1M PI since Jan 1 of the current year (up from < 100k PI since Jan 1 of the previous year)
	≥ 10k SPI records since Jan 1 of the current year (same except previously calculated from Jan 1 of the previous year)	< 10k SPI since Jan 1 of the current year (same except previously calculated from Jan 1 of the previous year)
Important Data#	X	

*CIIO: an entity that operates important network facilities and information systems (e.g., communications, energy, transport, finance) or other system that could seriously harm China's national security, economy, or public interest

#Important data: data that may endanger national security, economic operation, social stability, or public health and safety once tampered with, destroyed, leaked, or illegally obtained or used

Data Export Exceptions

- PI of less than 100,000 individuals since January 1 of the current year by a non-CIIO
- Necessity for the performance of a contract to which individual is a party
  - E.g., e-commerce, payments, ticket and hotel bookings
- Employee PI for purposes of implementing HR management according to employment policies and collective labor contracts
- For the protection of an individuals' life, health, or property security in emergency situations
- PI collected or generated outside China and then transmitted to China for processing

India strikes a balance

- The Digital Personal Data Protection Act was enacted in 2023
  - The DPDPA is yet to take effect
- Consultation on the DPDPA rules recently closed
  - Once the final rules are published, expect a transition period between 18-24 months
- The consultation process was extensive, demonstrating that the government does not want to rush regulation without understanding how it will impact the digitization of India

Placeholder for Data Transfer Restrictions

- The DPDPA provides that the government can restrict the transfer of personal data to certain countries (data localization)
- The draft Rules
  - specify that data fiduciaries in India may transfer personal data abroad only in compliance with conditions set by the government
  - Impose data localization requirements on "significant data fiduciaries" — those deemed "significant" based on the volume and nature of personal data processed —to, under certain conditions, store personal data, as well as traffic data relating to its flow, only within India
    - SDFs may include social media, e-commerce, and online gaming companies

GLOBAL DEVELOPMENTS

Expansion of Collective Redress in the EU and UK

Collective Redress Directive (RAD)

- Directive (EU) 2020/1828 on Representative Actions for the Protection of the Collective Interests of Consumers (RAD).
- Requires all EU member states to have in place at least one procedural mechanism for consumers to seek collective redress for alleged harm caused by a business through breaches of EU consumer laws (including GDPR).
- Actions to be brought by "qualified entities" (QEs), not individual consumers.
- Allows injunctive measures as well as compensation, but discourages punitive damages.
- "Loser pays" rule on costs and courts may dismiss "manifestly unfounded cases" at the earliest stage of proceedings.
- Will materially alter existing EU collective redress landscape.

RAD Implementation Status

- EU member states were required to transpose RAD into their national legal systems by 25 December 2022.
- Majority of jurisdictions have now implemented RAD, although some still have transition steps underway (eg France and Bulgaria).
- Spain has not implemented the RAD.

UK

- RAD not applicable to UK
- No overarching mass actions regime:
  - GLO – Group Litigation Order
  - CPR 19.8 - Representative Action
  - CPO – Collective Proceedings Order in the Competition Appeals Tribunal (CAT)
- Claimant lawyers are forming alliance to promote group litigation in EU and UK

U.S. DEVELOPMENTS

Conflicting Data Protection Obligations Under U.S. Law

Is Adtech – the Latest Data Transfer Concern?

PIXELS

- Piece of code on website
- When user visits website, data about the visit may be shared with third party technology providers
- Information transmitted is typically anonymous, but will include IP address, URL, browser type, and device type

SESSION REPLAY

- Pieces of code that replay a user's website visits
- Reproduces mouse movements, clicks, page visits, scrolling, tapping, data entry
- Used to:
  - Improve user experience
  - Identify and address technical issues
  - Identify ways to improve conversion

CHATBOTS

- Programs built to automatically engage with consumer messages
- Simulates human conversation with user through text or voice
- Often uses AI tools like natural language processing to understand a user's input and automate responses

BENEFITS

- Understand website traffic
- Find new customers
- Retarget website visitors
- Identify and fix website issues
- Exclude certain users from advertising campaigns
- Measure message reach
- Determine return on investment

RISKS

- Setting and configuration issues
- Litigation
  - Notice
  - User Consent
  - Transparency
- Data Breach
- Contract Formation
- Storage costs
- Retention Periods

What are the trends?

- Video Privacy Protection Act ("VPPA"): 2021 – 69 cases; 2022 – 150 cases; 2023 – 137 cases; 2024 – 250 cases.
- Pixels: 2022 – 160 cases; 2023 – 265 cases; 2024 over 200 cases.
- Companies are receiving significant amounts of demand letters that threaten direct action or class action lawsuits.
- In 2024, settlements reached up to $115 million.
- Fines from State Agencies and the FTC.

Private Enforcement of Privacy Rights

Statutory Claims

- Wiretap Laws (State and Federal)
  - $1,000 to $10,000/violation
  - California Invasion of Privacy Act - $2,500 to $10,000/violation
- Video Privacy Protection Act (VPPA)
  - $2,500/violation
- Computer Tampering Act and Identity Theft Statutes
- Consumer Protection Laws
- Confidentially of Medical Information Act (CMIA)
  - $1,000 to $2,500/violation
- State Privacy Laws
  - 19 comprehensive state privacy laws
  - California Consumer Privacy Act (CCPA and CPRA)

Common Law Claims

- Negligence
- Breach of Fiduciary Duty
- Breach of Implied/Express Contract
- Invasion of Privacy/Intrusion Upon Seclusion
- Unjust Enrichment

Specific Statutory Defenses

Wiretap Act

- **Consent**
- Elements
  - Website doesn't collect "contents" of the communications;
  - No "recording" and not "contemporaneous"
  - No reasonable expectation of privacy
  - Intent
- Statute of limitations
- Standing/lack of harm

VPPA

- Not a Video Tape Service Provider
  - A VTSP is engaged in the business of renting, selling, or delivering prerecorded materials.
- Disclosure is not knowing
- Plaintiff is not a Consumer
- **Consent**
- The information is not personally identifiable information

Strategic Considerations

- Change business practices to seek **consent**
- Settle or litigate?
- Arbitration provisions in TOU
  - Increasingly being adopted
  - Enforcement considerations

Regulatory Enforcement

Increased Regulatory Enforcement

- In 2022, Texas Attorney General Paxton sued Google for unlawfully tracking and collecting users' private data regarding geolocation, incognito searches, and biometric data. In 2025, Google settled for $1.375 billion.
- CCPA Settlements:
  - California Privacy Protection Agency (CPPA) Board required American Honda Motor Co. to change its business practices and pay a $632,500 fine.
  - California Privacy Protection Agency (CPPA) Board required national clothing retailer Todd Snyder, Inc., to change its business practices and pay a $345,178 fine.
- FTC enforcement fines have ranged from $100,000 to $7.8 million.
  - GoodRX
  - BetterHelp
  - Pre-Mom

Things To Watch For

CCPA in Adtech Litigation

- In two recent rulings, judges in the U.S. Northern District of California have allowed proposed class actions under the California Consumer Privacy Act (CCPA) to proceed without an allegation of a data breach.
- The two California judges have allowed class actions to continue where websites have installed cookies and similar tracking technologies to collect information about users. *Shah v. Capital One Financial Corp.* & *M.G. v. Therapymatch*.

Mitigating Risks

- Understand the Technology
- Take Advantage of Privacy Controls
- Get Consent & Update Disclosures
- Terms of Use Considerations
- Other Contractual Options


SHOOK
HARDY & BACON