PAUL HASTINGS

Dealing with Bulk Data: Key Federal and State Regulation

October 25, 2024

Agenda

- Introductions
- Current State of the Law
  - Key Federal Laws, Regulations and Orders
  - Key State Laws
- Relevant Enforcement Actions and Cases
- Best Practices and Key Considerations

Introductions

Current State of the Law and Regulation

Regulations at Federal and State Level

Key Federal Regulation and Oversight

- Protecting Americans' Data from Foreign Adversaries Act ("PADFA")
- Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern ("Bulk Data EO")
- DOJ Notice of Proposed Rulemaking on Bulk Data EO
- FTC Oversight and Enforcement
- CFPB RFI

Key State Laws

- California: Delete Act (Cal. Civ. Code §§ 1798.99.80-88); CCPA (Cal. Civ. Code § 1798.100 et. seq.)
- Vermont (Vt. Stat. Ann. tit. 9, §§ 2446-2447)
- Texas (Tex. Bus. & Com. Code Ann. Ch. 509)
- Oregon (House Bill 2052)

Protecting Americans Data from Foreign Adversaries Act ("PADFA")

- Effective **June 23, 2024**
- Enforced by the FTC
- Prohibits **data brokers** form selling, licensing renting trading, transferring, releasing, disclosing, providing access to, or otherwise making available **personally identifiable sensitive data** of a U.S. individual to any foreign adversary country or any entity that is controlled by a foreign adversary (e,g, China, Russia, Iran, and North Korea)
- Expansive definition of **"sensitive data"** that includes government-issued identifier (i.e., social security number), genetic information, account or devise log-in credentials, race, color, ethnicity, or religion, etc.
- **"Personally identifiable sensitive data"** refers to any sensitive data that identifies or is linked or reasonably linkable, either alone or combined with other data, to either an individual or a device that identifies that individual or that is linked or reasonably linkable to an individual

PIH

PADFA (Continued)

- **"Data broker"** means entities that, for valuable consideration, sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available data of U.S. individuals, not collected directly from the individuals by that entity, to another entity that is not acting as a service provider
    - Excludes entities that: (i) transmit data of U.S. individuals at their request or direction, including their communications; (ii) provide, maintain or offer a product or service where personally identifiable sensitive data, or access to such data, is not the product or service; (iii) report or publish news or information concerning local, national or international events or matters of public interest; (iv) report, publish or make available news or information to the general public (including information from books, magazines, phone books, movies, internet, radio, news media or internet sites available to the general public) not including obscene visual depictions; or; (v) act as a service provider.
- **"Service provider"** means an entity that collects, processes or transfers data on behalf of, and at the direction of (i) an individual or entity that is not a foreign adversary or controlled by a foreign adversary, or (ii) a government entity, and receives data from or on behalf of either of those entities
- **Restriction also applies to transfers to entities "controlled by a foreign adversary,"** which means an entity that is:
    - A foreign person domiciled in, headquartered in, has its principal place of business in, or is organized under the laws of, a foreign adversary country; or
    - An entity that is at least 20 percent owned by a foreign person or combination of foreign persons from the previous category, either directly or indirectly; or
    - A person under the control of either of the previous two entities

Executive Order 14117 on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern ("Bulk Data EO")

- Signed on February 28, 2024
- Seeks to **restrict access by "countries of concern" to Americans' bulk sensitive personal data and U.S. Government-related data** when such data access would pose "**an unacceptable risk to the national security of the United States**"
- Directs the Department of Justice (DOJ) to promulgate regulations to prevent large-scale transfer of sensitive personal data and U.S. Government-related data to "countries of concern"
  - Also directed other agencies to address data security risks, notably, it encouraged the CFPB to address the role data brokers play in contributing to national security risks
- **DOJ issued an NPRM on October 21, 2024**
  - There will be a 30-day comment period from the data the proposed rule is published in the federal register.

P | H

Bulk Data EO – DOJ NPRM

- **"Countries of Concern"** could include China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela
- Defines **"covered persons"** as:
  - Foreign entities that are 50 percent or more owned by a country of concern, organized under the laws of a country of concern, or has its principal place of business in a country of concern
  - Foreign entities that are 50 percent or more owned by a covered person
  - Foreign employees or contractors of countries of concern or entities that are covered persons
  - Foreign individuals primarily resident in countries of concern
  - Any person, wherever located, determined by the Attorney General: (i) to be, to have been, or to be likely to become owned or controlled by or subject to the jurisdiction or direction of a country of concern or covered person; (ii) to act, to have acted or purported to act, or to be likely to act for or on behalf of a country of concern or covered person; or (iii) to have knowingly caused or directed, or to be likely to knowingly cause or direct a violation of the rule
- **"Sensitive personal data"** defined broadly to include categories like:
  - Certain covered personal identifiers (e.g., names linked to device identifiers, social security numbers, driver's license, or other government identification numbers)
  - Precise geolocation data (e.g., GPS coordinates
  - Biometric identifiers (e.g., facial images, voice prints and patterns, and retina scans)
  - Human genomic data (e.g., DNA within each of the 24 distinct chromosomes in the cell nucleus, including results from genetic testing);
  - Personal health data (e.g., height, weight, vital signs, symptoms, test results, diagnosis, and psychological diagnostics); and
  - Personal financial data (e.g., information related to an individual's credit, debit cards, bank accounts, and financial liabilities, including payment history).

Bulk Data EO – DOJ NPRM (Continued)

- Will regulate specific categories of data transactions if certain bulk thresholds are met.
- Establishes the following **"bulk" thresholds** for regulated transactions*:

Human Genomic Data	***Biometric Identifiers***	***Precise Geolocation Data***	***Personal Health Data***	***Personal Financial Data***	***Certain Covered Personal Identifiers***
Over 100 U.S. persons	Over 1,000 U.S. persons	Over 10,000 U.S. persons	Over 10,000 U.S. persons		Over 100,000 U.S. persons

- Defines two categories of **"prohibited data transactions"** between US persons and countries of concern or covered persons and three categories of **"restricted transfers" based** on risk of access
  - Restricted transactions are permitted if certain security requirements developed by Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) are met
  - CISA concurrently published proposed security requirements for public comment
- Sets **limits on resale or transfer of data through third parties** by requires U.S. persons engaged in data brokerage with any foreign person that is not a covered person to satisfy certain conditions, including contractual requirements that the foreign person refrain from reselling or providing access to that data to a country of concern or covered person through a subsequent covered data transaction

**Also regulates any combination of these data types that meet the lowest threshold for any category in the dataset.*

Bulk Data EO – DOJ NPRM (Continued)

- **Exempts certain transactions** such as those that are:
  - Personal communications that do not transfer anything of value; the import or export of informational materials involving expressive materials; and travel information, including data about personal baggage, living expenses, and travel arrangements.
  - Official U.S. Government activities.
  - Financial services if they involve transactions ordinarily incident to and part of providing financial services, such as banking, capital markets, or financial insurance services; financial activities authorized for national banks; activities defined as financial in nature or complementary to a financial activity under the Bank Holding Company Act; transfer of personal financial data incidental to e-commerce; and the provision of investment management services that provide advice on portfolios or assets for compensation, including related ancillary services.
  - Corporate group transactions between a U.S. person and its foreign subsidiary or affiliate, if they are ordinarily incident to and part of routine administrative or business operations, such as human resources, payroll, taxes, permits, compliance, risk management, travel, and customer support
- **Does not** prescribe due-diligence, recordkeeping, reporting, or other compliance requirements across the U.S. economy or across all data transactions but DOJ noted it expected companies to develop and implement compliance programs based on their risk profiles

Bulk Data EO – DOJ NPRM (Continued)

- **Sets specific compliance obligations** for U.S. persons engaged in a restricted transaction, including:
  - Implementing a comprehensive compliance program with risk-based procedures to verify and log data flows, sensitive personal and government-related data types and volume, transaction parties' identities, data end-use and transfer methods, and vendor identities
  - Establishing written policies on data security and compliance that are certified annually by a responsible officer or employee
  - Conducting and retaining the results of an annual audit by an independent auditor to verify compliance with the security requirements established by CISA
  - Maintaining and certifying the accuracy of records for 10 years documenting data transfer methods, transaction dates, agreements, licenses, advisory opinions, and any relevant documentation received or created in connection with the transaction

- Establishes an **enforcement mechanism**:
  - DOJ can issue findings of violations and civil penalties, including an opportunity for parties to respond before the Department issues a penalty
  - Willful violations can lead to criminal fines up to one million dollars ($1,000,000) and up to 20 years imprisonment

FTC Regulation and Oversight of Data Brokers

FTC has historically sought to regulate data brokers

- 2014 Report: Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission

Increased scrutiny of data brokers since 2022

- 2022 Blog Post stating that the FTC will use the "full scope of its authorities" to stop the "illegal use and sharing" of consumers' location, health, and other sensitive data.
- ANPRM on Commercial Surveillance and Data Security Rulemaking increased scrutiny of data brokers
- Kochava Inc. enforcement action

Wave of enforcement actions in early 2024 against "mass data collectors"

- Settlements with Avast, X-Mode and InMarket

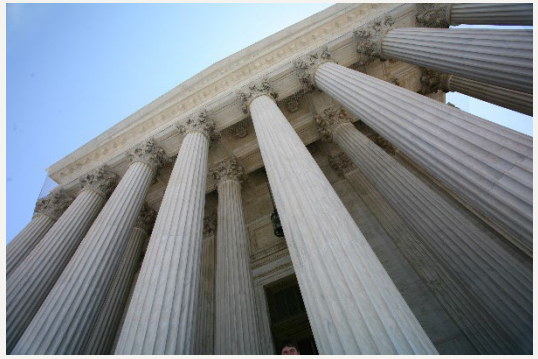
FTC Enforcement Actions

Kochava

- FTC filed suit against Kochava Inc. for selling geolocation data from hundreds of millions of mobile devices to trace movements of individuals to an from sensitive locations
- The FTC alleged that Kochava, in its role as a data broker, collects a wealth of information about consumers and their mobile devices by, among other means, purchasing data from outside entities to sell to its own customers

Avast

- FTC finalized order banning software provider, Avast, from selling, disclosing, or licensing any web browsing data for advertising purposes to settle charges the company sold such information after promising that its products would protect consumers from online tracking
- Avast must pay $16.5M, which will be used to provide redress to consumers



X-Mode

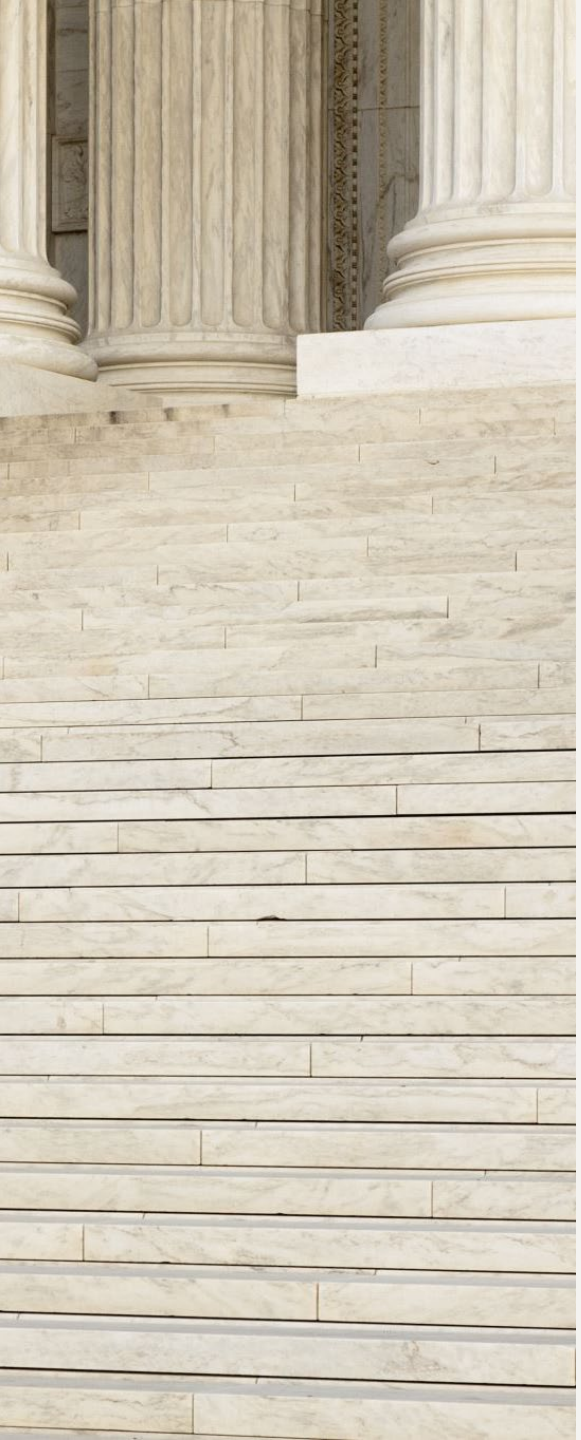
- FTC finalized order prohibiting data broker, X-Mode, and its successor Outlogic, from sharing or selling any sensitive location data to settle allegations that the company sold precise location data that could be used to track people's visits to sensitive locations, such as medical and reproductive health clinics and places of worship
- X-Mode/Outlogic must also create a program to maintain a list of sensitive locations and ensure it is not sharing, selling, or transferring location data about such locations, and it must delete/destroy all location data it previously collected and products developed from that data unless it obtains consumer consent or ensures the data is deidentified/rendered non-sensitive

InMarket

- FTC finalized order with digital marketing and aggregator, InMarket Media, over allegations that the company unlawfully collected and used consumes' location data for advertising and marketing
- InMarket is now prohibited from selling, sharing, or licensing any precise location data and any product/service categorizing/targeting consumers based on sensitive location data, and it must delete/destroy all location data previously collected and any products produced from that data unless it obtains consumer consent or ensures the data has been deidentified

Other Federal Regulatory Action

- In early 2023, the CFPB sought comments from the public in a request for information (RFI) related to data brokers to assist the CFPB and policymakers in understanding the current state of business practices in existing enforcement, supervision, regulatory, and other authorities
- CFPB later announced a decision to launch a rulemaking targeting data brokers with two rulemaking proposals under consideration including:
  - A rule defining a data broker selling certain types of consumer data as a "consumer reporting agency"
  - A rule clarifying key identifiers, such as name, DOB, and SSN, qualify as consumer report data
  - The CFPB intends to release the proposed rules for public comment this year



State Regulation of Data Brokers

California

- **Delete Act** –Grants Californians the right to demand that data brokers erase their personal information from the data brokers' records
- **CCPA** –Data brokers are required to:
  - Register with and report to CPPA on responses to consumer deletion requests
  - Data brokers must provide specific information about data collection as well as undergo audits

Vermont

- **Vt. Stat. Ann. Tit. 9, §§ 2446-2447** –Data brokers:
  - Must register with the Secretary of State
  - Must provide specific information, such as method for requesting opt out and a statement specifying data collection, databases, or sales activities from which consumers may opt out
  - Have a duty to protect personally identifiable information

Texas

- **Tex. Bus. & Com. Code Ann. Ch. 509** –Data brokers:
  - Must register with the Secretary of State
  - Must provide notice they are a data broker on their website/mobile app
  - Must maintain a comprehensive information security program
  - If they have personal information of children under 13, they must state how they comply with laws regarding such information

Oregon

- **House Bill 2052** – Data brokers:
  - Must register with Oregon Department of Consumer and Business Services
  - With registration, must provide a declaration describing whether and how Oregon residents may opt out of all or a portion of the data broker's activities and whether an Oregon resident may authorize an agent to exercise these rights on their behalf

PIH

State Regulatory Action and Cases

California Proposed Rules on Data Broker Registration

- On July 5, the California Privacy Protection Agency (CPPA) published proposed rules on data broker registration under the Delete Act
- The public comment period closed in August

Recent New Jersey Cases

- Series of suits brough by Atlas Data Privacy Corp under Daniel's Law
- Daniel's Law allows for NJ judges and other officials to request that data brokers remove their addresses and phone numbers and are allowed to assign their claims to a third party
- Atlas has filed more than 140 Daniel's Law cases on behalf of thousands of "covered persons," the first of their kind, against different data brokers this year, more than 60 of which have filed a consolidated motion to dismiss
- Many of these suits have transferred to federal court and have turned into a constitutional battle that could impact state and federal privacy efforts as well as hinder efforts to protect vulnerable individuals from violent threats

What's Next?

Questions?

Andy Bagnell

Senior Legal Counsel
Tencent America

700 K St., NW Suite 620
Washington, D.C. 20001

Andybagnell@global.tencent.com

Andy Bagnell is a Senior Legal Counsel in Tencent's Compliance and Transactions Department and is based in Washington, D.C. Andy advises internal stakeholders within Tencent and the Tencent Group regarding international regulatory compliance, focusing on compliance with CFIUS regulations and other international foreign investment programs. Andy also advises on other international regulatory issues, including anti-bribery, anti-trust, cross border investigations, privacy, and other regulatory issues.

Andy is also a member of Tencent Global Research Institute, assisting the Global Public Affairs Department by monitoring and preparing updates regarding policy developments and relevant litigation related to privacy, anti-trust, sanctions, and other matters impacting the gaming and communications industries.

Prior to joining Tencent, Andy worked at Hogan Lovells in Washington D.C. as part of their White Collar practice. Andy also served on active duty with the U.S. Marine Corps as an attorney as a prosecutor and as a command advice attorney, focusing on international law and large-scale investigations.

Andy is admitted in Washington, D.C., Massachusetts, and North Carolina.

Keith Feigenbaum

Of Counsel
Litigation Department

2050 M Street NW, Washington, DC 20036

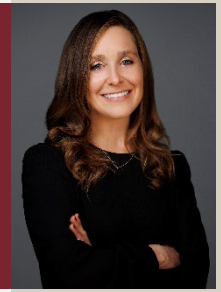
+1.202.551.1929

keithfeigenbaum@paulhastings.com

Keith Feigenbaum is Of Counsel in the Global Trade Controls practice of Paul Hastings and is based in the firm's Washington, D.C. office. Keith advises clients on a broad spectrum of government contracts and national security matters, including compliance counseling, export controls, foreign ownership, control, and influence (FOCI), cybersecurity, mergers and acquisitions, suspension and debarment, bid protests, investigations, claims and disputes, and other issues impacting government contractors and federal grantees.

Prior to private practice, Keith served in several capacities with the U.S. Department of Defense, including the Defense Logistics Agency's Office of General Counsel and the U.S. Army Judge Advocate General's (JAG) Corps. As an Army Reservist, Keith is a lieutenant colonel and adjunct professor of government contract and fiscal law at the Army JAG School in Charlottesville, VA. He holds an active Top Secret/SCI security clearance.

Keith is admitted in Delaware, New Jersey, and Pennsylvania, and is supervised by an Attorney Licensed in the District of Columbia.



Rachel Kurzweil

Of Counsel,
Litigation Department

2050 M Street NW, Washington, DC 20036
P: +1.202.551.1940
F:Fax: +1.202.551.0440

rachelkurzweil@paulhastings.com

Rachel Kurzweil is an Of Counsel in the Data Privacy and Cybersecurity Group and is based in the Firm's Washington D.C. office. Rachel is a leading privacy, cyber and health regulatory attorney with broad ranging experience advising clients in areas of U.S. state, federal and international privacy regulation and compliance, data breach, cyber and privacy incidents, and regulatory compliance. Rachel has extensive experience operationalizing global privacy and cybersecurity laws and regulations including the CCPA, VPPA, CAN-SPAM, GLBA, TCPA, DPPA, COPPA, FISA, and other state privacy laws, state wiretapping laws including CIPA and WESCA, GDPR and other international privacy laws.

Rachel routinely assists a wide variety of multinational clients across industries with compliance with international, state and federal privacy, security and data breach notification laws and regulations, including conducting privacy assessments, drafting privacy policies and procedures, and data privacy impact assessments. She also has deep expertise in advising clients in highly regulated sectors, including financial services and health care. She counsels these companies and coordinates with their technology and advertising partners, to address legacy regulatory issues and the emerging privacy and cyber risks that arise from industry innovations and data sharing. She also regularly represents clients in strategic transactions involving personal data and cybersecurity risk.

Rachel regularly assists clients with complex health and life sciences matters involving the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), Section 5 of the Federal Trade Commission Act and myriad state privacy, security and breach notification laws, as well as adjacent regulatory regimes such as the ONC Information Blocking Rule. She has extensive experience in helping clients navigate the intersection between federal privacy and data protection laws and state regimes such as the California Consumer Privacy Act (CCPA), the Washington My Health My Data Act (MHMDA) and the California Confidentiality of Medical Information Act (CMIA).

Prior to joining the firm, Rachel was a Counsel with an AmLaw50 law firm, specializing in privacy and health. She also worked as a Health Litigation Fellow with AARP Foundation.

Rachel is admitted in Maryland, Pennsylvania and Washington, D.C.

21 OFFICES across the Americas, Asia, and Europe.

Global Presence

The Americas

Atlanta
Century City
Chicago
Houston
Los Angeles
New York
Orange County
Palo Alto
San Diego
San Francisco
São Paulo
Washington, DC

Asia

Beijing
Hong Kong
Seoul
Shanghai
Tokyo

Europe

Brussels
Frankfurt
London
Paris

1 LEGAL TEAM to integrate with the strategic goals of your business.

Our Firm

In today's world of transformative change, our purpose is clear—to help our clients and people navigate new paths to growth.

Founded in 1951, Paul Hastings has grown strategically to anticipate and respond to our clients' needs in markets across the globe. Our innovative approach and unmatched client service has helped guide our journey to becoming one of the world's leading global law firms in such a short time.

We have a strong presence throughout Asia, Europe, Latin America, and the U.S. We offer a complete portfolio of services to support our clients' complex, often mission-critical needs—from structuring first-of-their-kind transactions to resolving complicated disputes to providing the savvy legal counsel that keeps business moving forward.

A Top-Ranked Firm
on *The American Lawyer's* A-List of the Most Successful Law Firms in the U.S. nine years in a row

A Top-Ranked Firm
in the *Financial Times* Innovative Lawyer's Report across Asia, Europe, and North America

Top 10 for "Best Place to Work" in Vault's annual survey eight years in a row

A Top-Ranked Firm
for Best Overall Diversity, according to Vault

50 Serving 50% of the Fortune 100

117 of our clients are on Fortune's Most Admired List

58 We advise clients based in 58 countries around the world