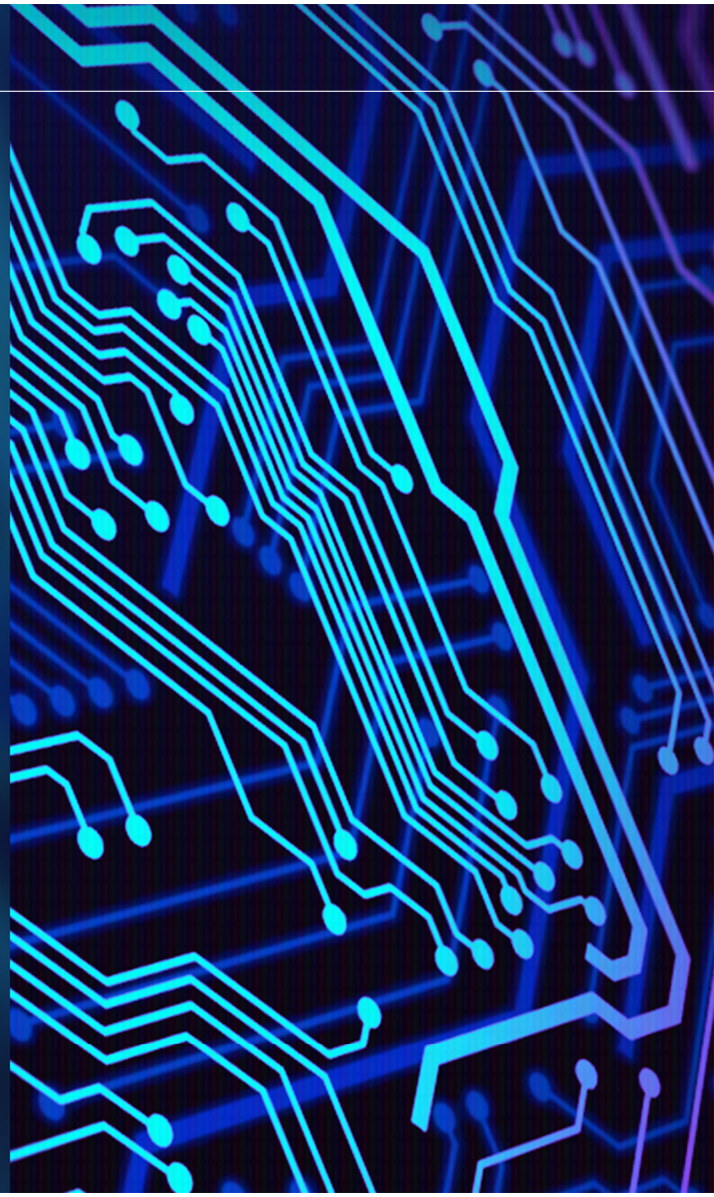
November 2025

Minding the (US-European) Privacy Gap

Cross-Border Data Transfers



LathamTECH

LATHAM & WATKINS LLP

LathamTECH
LATHAM&WATKINS LLP

Speakers

Jennifer Archie

Partner

Washington, D.C.

Connectivity, Privacy & Information

E jennifer.archie@lw.com
T +1.202.637.2205

Calum Docherty

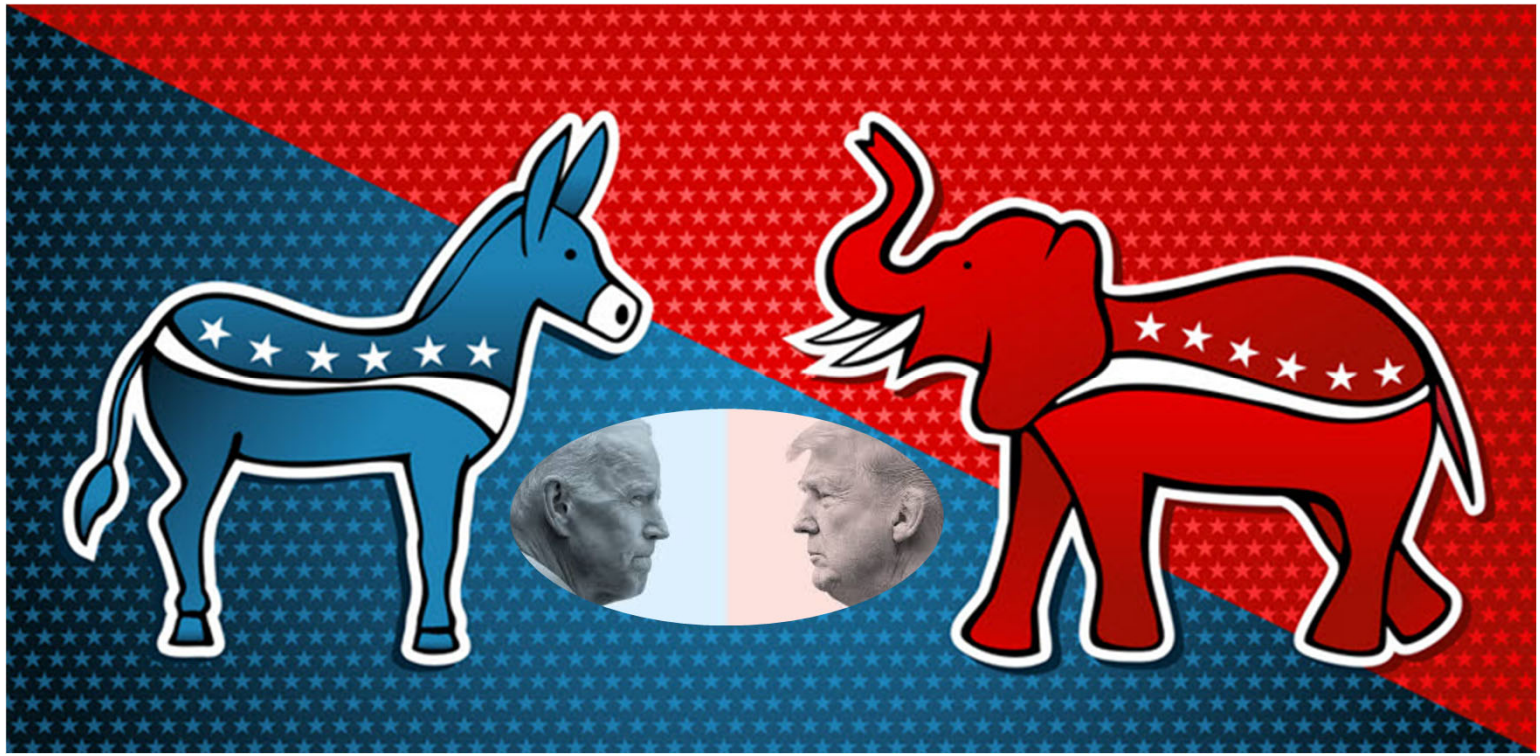
Associate

London

Data & Technology Transactions

E calum.docherty@lw.com
T +44.20.7710.1079

Do US Politics Sway Privacy Approach?



US Policy: National Security Approach

- Response to the ability of countries of concern and covered persons to acquire sensitive data for purposes hostile to national interests
- DOJ cites investigations:
  - > Mobile-phone location data
  - > Genomic material
  - > Behavioral profiling datasets
- Data previously regulated through privacy and consumer protection laws now increasingly being treated as national asset with potential strategic consequences
- Access to sensitive data / government data by countries of concern / covered persons now never purely commercial – either:
  - > Outright prohibited
  - > Severely restricted

DSP Scope of Covered Data

Bulk U.S. Sensitive Personal Data (linked or linkable to a US person)

- Omic Data, including biospecimens (1,000)
  - > Genomic Data (100)
- Biometric Data (1,000)
- Precise Geolocation Data (1,000)
- Personal Health Data (10,000)
- Personal Financial Data (10,000)
- Covered Personal Identifiers Data (100,000)

U.S. Government-Related Data

- Any volume
- Within enumerated sensitive areas

Important:

Anonymization, deidentification, aggregation, encryption **do not matter**

Parties: US Person & Covered Person

US Person & Covered Person

The DSP applies to the flow of data *from a* **US person** *to a* **covered person**

US Person

- U.S. citizen, national or lawful permanent resident;
- Refugees or Asylees;
- Entities organized solely under the laws of the U.S. (and any foreign branches);
- Any person in the U.S; or

Covered Person

- Foreign entities 50% or more owned by a country of concern, organized under its laws, or with their principal place of business there;
- Foreign entities 50% or more owned by a covered person;
- Foreign employees or contractors of countries of concern or entities that are covered persons; or
- Foreign individuals primarily residing in countries of concern.
- Any person (regardless of location) designated by the AG

- Six countries designated as “countries of concern” due to adverse conduct towards US national Security: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela
- Foreign Person is anyone who is not a US Person or Covered Person

Covered Data Transactions

What data transactions are restricted or prohibited?

US Person

- U.S. citizen, national or lawful permanent resident;
- Refugees or Asylees;
- Entities organized solely under the laws of the U.S. (and any foreign branches); ***or***
- Any person in the U.S.

Covered Person

Any **foreign entity** that is 50 percent or more owned, directly or indirectly, by a **country of concern** or **covered person**, or that is organized or chartered under the laws of, or has its principal place of business in, a **country of concern**.

A **foreign person** who is an employee or contractor of a **country of concern** or of a **covered person** or who is primarily resident in a **country of concern**.

Any **person** (including a **US Person**) designated by the Attorney General.

Covered Data

- Bulk U.S. Sensitive Personal Data

or

- Any Volume of U.S. Government-related Data

Transaction Type

- Data brokerage;
- Vendor agreement;
- Employee agreement; or
- Investment agreement

Prohibited vs. Restricted Transactions

Prohibited Transactions:

Five Buckets

US persons knowingly engaging in a covered data transaction involving:

- Data brokerage with covered person
- Data brokerage with foreign person who transfers data to covered person
- Bulk human 'omic data
- Evasion of DSP
- Knowingly directing prohibited or restricted transactions

Restricted Transactions:

Permitted only if US person implements CISA security restrictions so covered persons cannot access in-scope data:

- **Vendor agreements:** agreement or arrangement in which any person provides goods or services to another person in exchange for payment or other consideration.
- **Employment agreements:** any agreement or arrangement in which an individual, other than an independent contractor, performs work in exchange for payment or other consideration.
- **Investment agreements:** any agreement in which a person, in exchange for payment or other consideration, acquires direct or indirect ownership interests or rights related to real estate located in the US or a US legal entity.

Exemptions:

The DSP provides exemptions for prohibited or restricted transactions in certain narrowly drafted scenarios, including personal communications, clinical trials, financial services, and certain corporate group transactions.

Mandatory, specific “security requirements”

Organizational and Covered System Requirements (all)	◆ Identify, prioritize and document all assets of the covered system ◆ Designate an individual responsible for cybersecurity and governance, risk and compliance ◆ Remediate known exploited vulnerabilities within a risk-informed span of time ◆ Document and maintain all vendor/supplier agreements for covered systems ◆ Develop and maintain an accurate network topology of the covered system and any network interfacing with the covered system ◆ Adopt and implement an administrative policy that requires approval before new hardware or software is deployed on a covered system ◆ Develop and maintain an incident response plan ◆ Enforce MFA on all covered systems ◆ Promptly revoke access when applicable (e.g., upon termination of an individual) ◆ Collect logs ◆ Implement configurations to deny by default all connections to covered systems ◆ Issue and manage credentials for authorized users ◆ Conduct an internal risk assessment
Data-Level Requirements (risk-based combination)	◆ Maintain and implement a data retention and deletion policy ◆ Process data in a way to minimize linkability to U.S. persons ◆ Apply encryption techniques ◆ Apply privacy enhancing techniques, such as use of dummy data ◆ Configure identity and access management techniques to deny authorized access to covered data by covered persons and countries of concern.

https://www.cisa.gov/resources-tools/resources/EO-14117-security-requirements

Subparts J and K

Due diligence, audit, reporting, recordkeeping:

All **U.S. persons** engaged in restricted transactions must develop, implement, and routinely update an individualized, risk-based, written Data Compliance Program designed to prevent, detect, and remediate breaches in company procedures and violations of the DSP.

- **Effective October 6, 2025** – implement or prepare:
  - **Due diligence procedures:** No filing or approval process, so burden falls on U.S. person to assess applicability of DSP
  - **Audit procedures**: comprehensive, independent, and objective
  - **Recordkeeping Requirements:** DOJ may request records on any transaction, or data exchange covered by DSP
  - **Reporting requirements:**
    - Cloud-computing services
    - Rejected prohibited transactions
- **Advisory opinions and licenses** were fundamental to the public policy scheme, modeled on export control regime
- **No DOJ guidance since April**

History of the EU-US Privacy Shield

Schrems II and the adoption of the Data Privacy Framework

The EU-US Privacy Shield was the predecessor to the Data Privacy Framework and was the transfer mechanism used for transfers of personal data from the EEA (at the time including the UK) to the US, to companies who were certified under the Privacy Shield regime. The Data Privacy Framework was granted adequacy by the European Commission in July 2023.

What was the Privacy Shield regime?

The Privacy Shield was the safeguard mechanism for personal data transfers from the EEA to the US, whereby EEA organisations (including the UK) could freely transfer personal data to US companies certified under the framework in compliance with Chapter V of the GDPR, without needing any further data transfer mechanisms such as the Standard Contractual Clauses (the 'SCCs').

Schrems II – Invalidation of the Privacy Shield

In July 2020, the Court of Justice of the European Union ('CJEU') invalidated the EU-US Privacy Shield framework (the '*Schrems II*' decision), finding that the US legal regime did not ensure an essentially equivalent level of protection, compared to the GDPR. The CJEU was particularly focused on access rights to data by US public authorities for national security purposes and associated individual rights and remedies. As for the SCCs, the CJEU did not invalidate these as a transfer mechanism but did stress the importance of analysing transfers on a case-by-case basis.

Negotiation of the DPF

Following lengthy negotiations, the US and the European Commission agreed in principle to a new Data Privacy Framework in the spring of 2022. This negotiation focused on upgrading the framework through measures such as:

- necessary and proportionate signals intelligence collection
- a two-tier redress mechanism
- intelligence agencies adopting new procedures.

Executive Order 14086

The *Executive Order 14086 on Enhancing Safeguards for United States Intelligence Activities* was signed by President Biden on 7 October 2022, which introduced new safeguards to form the basis of the Data Privacy Framework, as well as for other transfer mechanisms such as the SCCs and the Binding Corporate Rules.

Latombe Decision

- European Commission adopted Adequacy Decision (2023)
- Where it stands now
  - > General Court *Latombe* Decision (2025):
    - Standing not considered
    - Action to annul the Adequacy Decision dismissed
    - Data Protection Review Court deemed to provide effective redress
    - US law and practice essentially equivalent
  - > Appeal: Latombe has confirmed he is appealing
- Risk on the horizon
  - > Trump administration impact (2025): special advocate resignation; PCLOB members dismissal

EU to the People's Republic of China Data Transfers

Key learnings from the IDPC's TikTok decision

- Risk based v. zero risk
- Accountability
- Nature of the transfer impact assessment
- Reliance on the transfer impact assessment
- Local counsel or expert input
- Supplementary measures
- Transparency

ByteDance Divestment of US TikTok

TikTok ban timeline: Congress' yearslong case against ByteDance

TikTok CEO Says 'Project Texas' to Allay US Security Concern

- CEO Chew says data security effort is expensive, unprecedented
- Popular TikTok app has come under fire from American officials

TikTok Spent Years Developing Data Security Plan: Washington Ignored It

By Juro Osawa, Jing Yang and Erin Woo

China Approves TikTok Deal, U.S. Treasury Secretary Says, Paving Way for Resolution

By **News Desk Editor** - October 30, 2025

The $14 billion TikTok deal will be 'consummated' on Thursday, Treasury secretary says

Practical Strategies

UK / EU

- Contract
- Know your data and personal data flows
- Get outside counsel involved at an early stage
- Adequacy Decision or a comprehensive impact assessment
- Keep your impact assessment under review
- Limit personal data transferred
- Limit access by those in third countries
- Supplementary measures
- Transparency

US

- “US Person”-centric approach
- Data mapping more critical than ever –”Access”!
- Know your ties to Countries of Concern
- Investment analysis – unique and needs data experts
- Cloud, AdTech, Life Sciences, Financial Services
- Right-size and scope for “data compliance program”
- Documented assessment of how DSP applies and impacts the business – public company disclosures, M&A, outsourcing, non-exempt intragroup activities
- Embedding DSP in corporate policies – procurement, third party risk management, cybersecurity policies
- Training

LathamTECH
LATHAM & WATKINS LLP

Questions?

LathamTECH
LATHAM & WATKINS LLP

Thank You

An Integrated Cross-Border Team

Key Global Contacts

Our significant experience managing cross-border and multi-jurisdictional projects allows us to provide you with integrated and cost-effective legal advice across jurisdictions. Latham's privacy & cyber lawyers work seamlessly across the firm's global network of offices to provide coordinated global advice and solutions through a single point of contact.

UK

Gail Crawford
Partner, London

Ian Felstead
Partner, London

James Lloyd
Partner, London

Fiona Maclean
Partner, London

Hayley Pizzey
Counsel, London

Calum Docherty
Associate, London

France

Myria Saarinen
Partner, Paris

Germany

Tim Wybitul
Partner, Frankfurt

Joachim Grittmann
Counsel, Frankfurt

Wolf-Tassilo Böhm
Counsel, Frankfurt

Singapore

Esther Franks
Counsel, Singapore

Middle East

Brian Meenagh
Partner, Riyadh

Danielle van der Merwe
Counsel, Dubai/London

China

Rhys McWhirter
Partner, Hong Kong

Hui Xu
Partner, Beijing

Xuechu (Sean) Wu
Counsel, Beijing

USA

Michael Rubin
Partner, San Francisco / Silicon Valley

Jennifer Archie
Partner, Washington, D.C.

Serrin Turner
Partner, New York

Tony Kim
Partner, Washington, D.C.

Robert Blamires
Partner, San Francisco

Marissa Boynton
Partner, Washington, D.C

Clayton Northouse
Partner, Washington, D.C

Melanie Blunschi
Partner, San Francisco

Robert C. Collins III
Partner, Chicago

Christopher Garcia
Partner, New York

Michelle Ontiveros Gross
Partner, Silicon Valley / San Francisco

Raquel Kellert
Partner, New York

Heather Deixler
Partner, San Francisco

Robert Brown
Partner, Houston

Francis Acott
Counsel, San Francisco

Max Mazzelli
Counsel, San Francisco

Paul Moura
Counsel, New York

Jennifer Howes
Counsel, San Diego

Please click on any of the links to see the full bio

LathamTECH

LATHAM & WATKINS LLP

North America

Austin
Boston
Chicago
Houston
Los Angeles
New York
Orange County
San Diego
San Francisco
Silicon Valley
Washington, D.C.

Europe & Middle East

Brussels
Dubai
Düsseldorf
Frankfurt
Hamburg
London
Madrid
Milan
Munich
Paris
Riyadh
Tel Aviv

Asia-Pacific

Beijing
Hong Kong
Seoul
Singapore
Tokyo

LW.com