Morgan Lewis

TECHNOLOGY MARATHON

Hot Topics in Data Privacy

June 21, 2022

Presenters

Tess Blair
Partner
Philadelphia

William Childress
Senior Attorney
Philadelphia

Dr. Axel Spies
Special Legal Consultant
Washington, DC

Morgan Lewis

Agenda

- EU Data Privacy Regulatory Activity
- Privacy Shield 2.0
- Standard Contractual Clauses
- Data Transfer Impact Assessments
- Data Subject Access Requests
- US Data Privacy Developments
  - Legislative Landscape
  - Biometric Data
  - Artificial Intelligence (AI)

Updates on EU – Regulatory Activity

Morgan Lewis

French Blocking Statute Amendments

1968 Criminal statute enacted to negate US discovery laws

- Prohibits French nationals from disclosing sensitive information outside France
- Practically never enforced in France
- *Aérospatiale*: discovery in US courts, even if it violates the statute

April 1, 2022, change to Blocking Statute

- French company receiving request must report request to French authorities
- Must provide authorities with multiple pieces of information to evaluate request
- Authorities will respond within 1 month on whether requested information is covered by Blocking Statute

Austrian Data Protection Authority (ADPA)

Post-*Schrems II* Decision

- ADPA takes very broad view of what constitutes personal data
  - Any identifier can be personal data
  - Immaterial if importer of data cannot link identifier to actual individual
- ADPA very strict view of supplementary measures for US data transfers
  - Contractual measures ineffective because they don't bind authorities
  - If US importer could access data in plain text, no technical safeguards, including encryption are effective
  - Under FISA, US authorities could demand encryption key for data under importer's custody or control
- 100 + similar cases pending throughout EU

The Dresden Decision

Individuals could be subject to liability for GDPR violations:

> "Both the 1st Defendant and the 2nd Defendant (Managing Director) are responsible within the meaning of Art. 4 No. 7 GDPR, because the connecting factor for a claim under Art. 82 para. 1 GDPR is first of all the "responsibility", which is given whenever a natural or legal person alone or jointly with others can and does determine the purposes and means of the processing of personal data (Gola, ed. Gola, GDPR Commentary, 2nd ed. 2018, Art. 4 para. 48; Ambrock ZD 2020, p. 429 – according to beck-online). This means that, as a rule, the responsibility of employees who are bound by instructions or other employees does not apply, but it does apply to the managing director – the second defendant…"

Privacy Shield 2.0 Background & Developments

Morgan Lewis

What is the EU General Data Protection Regulation (GDPR)?

GDPR	Adopted on May 4, 2016
Background	• Under EU law, personal data can only be gathered legally under strict conditions, and only for a legitimate purpose. • Persons or companies which collect and manage your personal information must protect it from misuse and must respect certain rights of the data subjects which are guaranteed by EU law = a "human right" • Nationality or the residence of the data subject doesn't matter
What is the scope?	• Covers all personal data in and from the EU • "Special categories of data", such as heath data and data on disabilities are especially protected.

EU/US Privacy Shield 2.0 State of Play

- Court of Justice of the European Union (CJEU) in the '*Schrems II*' decision of 16 July 2020 invalidated the Privacy Shield (*Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Case C-311/18)*
- Since 'Schrems II', alternative routes have to be used to transfer data to the US, such as the so-called 'standard contractual clauses' to be accompanied by 'appropriate supplementary measures'
- New political agreement, the so-called Trans-Atlantic Data Privacy Framework (TADPF) announced 02/2022
- 03/25/2022: the White House announced in a press release that the US made "unprecedented commitments".

EU/US Privacy Shield 2.0 State of Play (2)

We are still waiting for the details. Per a statement from the EC, the TADPF will probably cover:

- New safeguards to limit access to data by US surveillance agencies to what is necessary and proportionate in the pursuit of defined national security objectives.
- A two-tier redress system to investigate and resolve complaints of EU individuals on access of data by US surveillance agencies, which includes an independent Data Protection Review Court.
- Enhance oversight of intelligence activities.

BUT:

1. Can it be done by **Executive Orders** only? A subsequent president could reverse executive orders.
2. March 2022 US Supreme Court decision in ***FBI v. Fazaga*** → **the Court** ruled that the US Federal government could invoke its state-secret privilege to prevent disclosure of information to individuals who claimed they had been subject to illegal surveillance from US authorities under the Foreign Intelligence Surveillance Act (FISA)

EU/US Privacy Shield 2.0 State of Play (3)

3. DNI Annual report from April 2022 on FISA 702

Figure 4: **Section 702 Targets (recall that only non-USPs are targeted)**

Section 702 of FISA	CY2019	CY2020	CY2021
Estimated number of targets of such orders *See* 50 U.S.C. § 1873(b)(2)(A).	204,968	202,723	**232,432**

Figure 9: **FBI U.S. Person Queries**

Section 702 of FISA	December 2019 – November 2020	December 2020 – November 2021
Estimated number of U.S. Person queries of unminimized Section 702-aquired contents and noncontents for foreign intelligence information and/or evidence of a crime	**Fewer than 1,324,057**	**Fewer than 3,394,053**

https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf

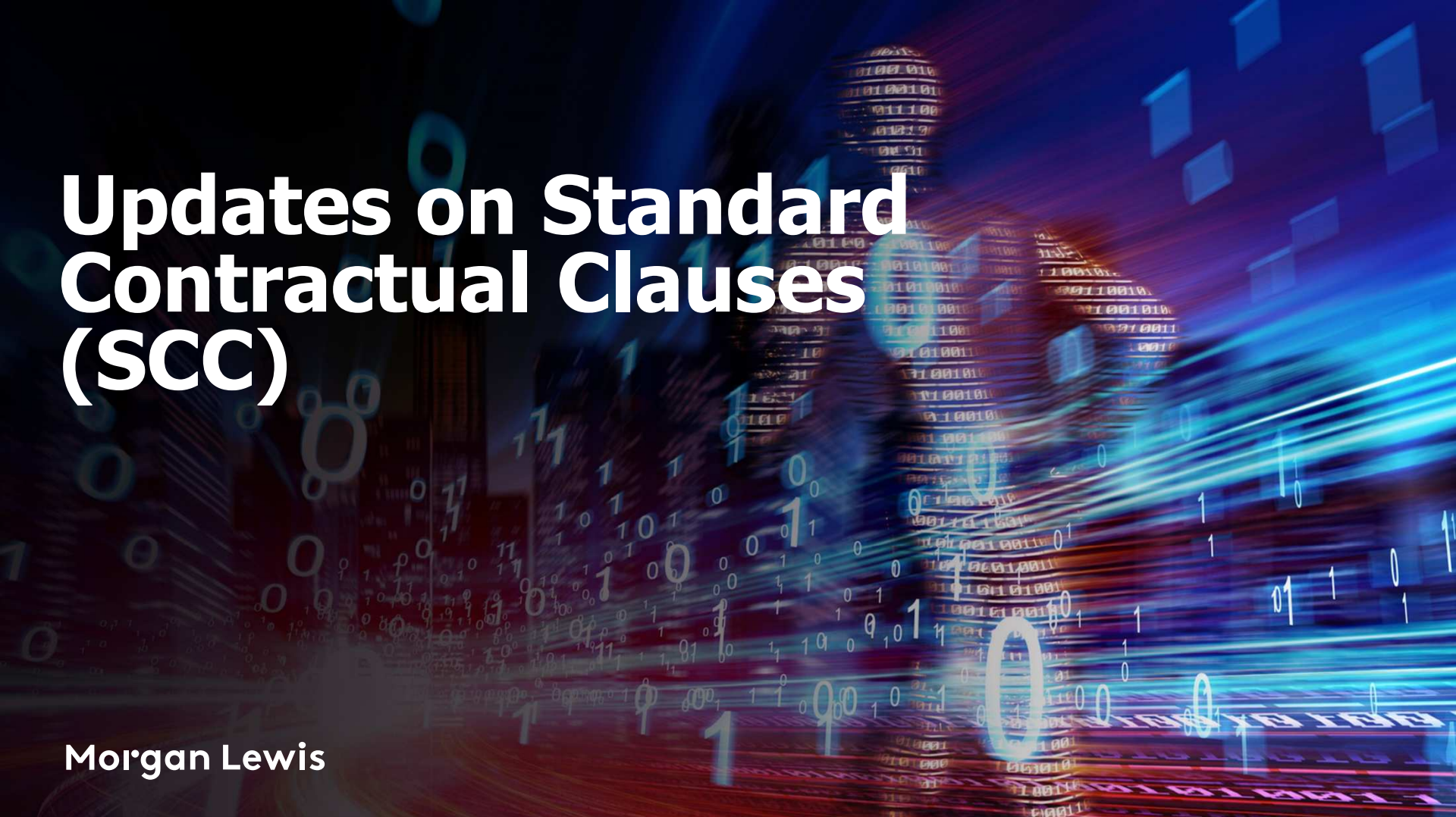
EU/US Privacy Shield 2.0 State of Play (4)

4. **Maximilian Schrems**, lead litigant in the CJEU's decisions 'Schrems I' and 'Schrems II' and founder of the NOYB association: once the final text of the framework is published, NOYB or another activist group will likely challenge the TADPF before the CJEU if it does not comply with EU law.
5. **Cumbersome approval process** at the EC (Art. 45 (3) GDPR):
   - EU Commission is required to provide the **European Data Protection Board** with all necessary documentation, including correspondence with the U.S. government.
   - The EDSA must then issue an **opinion** assessing the adequacy of the level of protection provided in the US.
   - Thereafter, the **Member States** must be involved as part of the comitology procedure.
   - The Commission will not adopt the adequacy decision as an implementing act if the weighted **majority in the Committee representing the Member States delivers a negative opinion** on the draft. In this case, it must renegotiate and resubmit the new result to the committee or refrain from further pursuing the draft.

EU/US Privacy Shield 2.0 State of Play (5)

- Therefore, best guess: EU Adequacy Decision by early 2023
- In any event, worth relying on other data transfer tools (belts and suspenders), such as
  - New EU Standard Contractual Clauses (4 Modules – issued 2021) or
  - Derogations, such as consents (Art. 49 (1) (a) GDPR – but only in rare instances.
- What will the UK do?
- What will Schrems/NOYB do? →

Max Schrems



Updates on Standard Contractual Clauses (SCC)

Morgan Lewis

SCC: Overview of Transfer Mechanism

- Model data protection clauses approved by European Commission (EC)
- Act as an "appropriate safeguard" (tool) for data transfers from EU
- Allow for free-flow of personal data, when incorporated into a contract
- Common transfer mechanism to countries without adequacy decision
- EC approved three SCCs under 1995 Data Protection Directive
  - Two EU-controller to non-EU controller clauses
  - One EU-controller to non-EU processor clause
- Used following GDPR enactment
- *Schrems II* required updates to "old" SCCs

SCC: New Requirements

"New" SCCs issued by EC in June 2021

- New agreements to transfer data must be based on new SCCs as of 9/27/2021
- Old agreements can be relied on until 12/27/2022, if data processing operations are not modified
- After 12/27/2022 cannot lawfully rely on old SCCs to transfer data to third countries

EDPB FAQS:

- Guidance on how to use SCC and comply with requirements
- Address multiple scenarios

Four Modules adapted for different transfer scenarios

- Controller (exporter) to Controller (importer)
- Controller (exporter) to Processor (importer)
- Processor (exporter) to Sub-processor (importer)
- Processor (exporter) to Controller (importer)

SCC:
New Requirements

Includes "docking clauses"

- Parties can choose to add additional parties in future (e.g. sub-processor)
- Adds flexibility to contract Lifecyle

Negates need for data processing agreement (DPA)

Must now conduct Transfer Impact Assessments to document:

- Specific circumstances of the transfer
- Laws of importing country
- Additional safeguard put in place

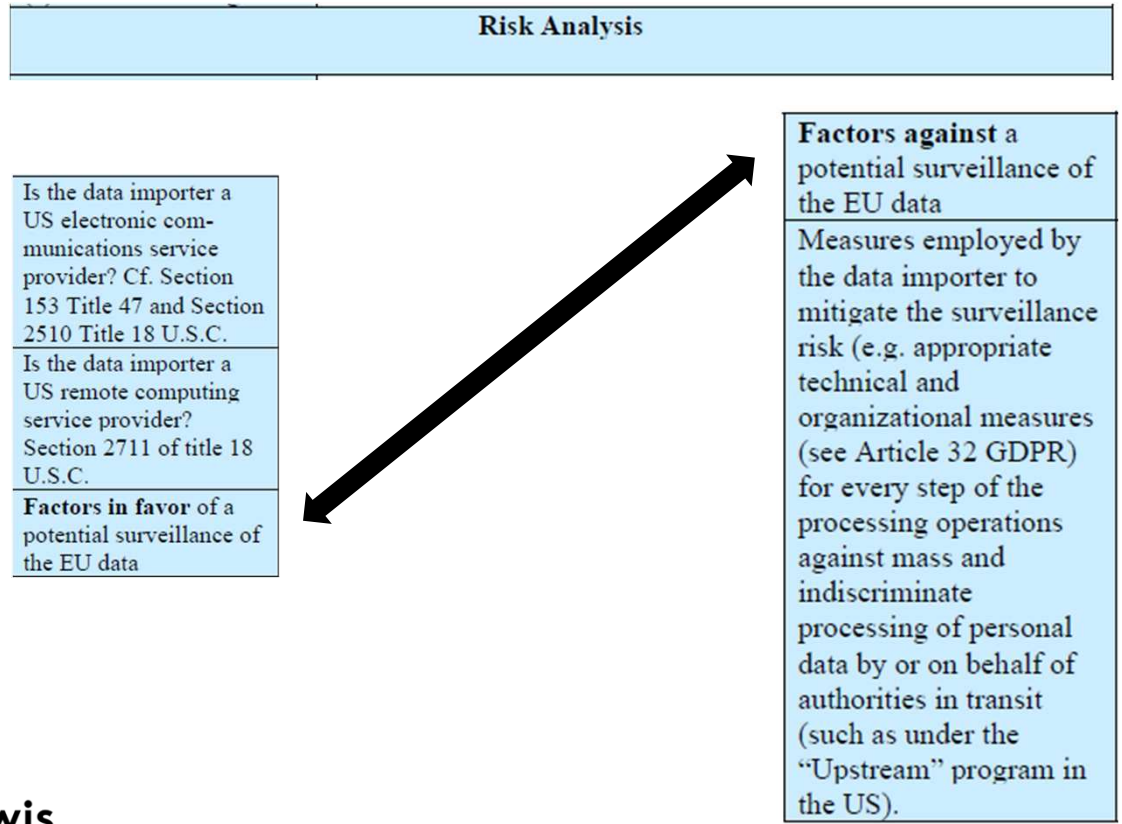
Data Transfer Impact Assessments

Morgan Lewis

Data Transfer Impact Assessment (DTIA) – Step 1

Data Importers with contact information	
Data Exporters with contact information	
Version of Standard Contractual Clauses Used	
Country/ countries from where EU personal data are exported	
Country to which EU personal data are transferred	
Categories of EU personal data transferred (a) special categories of data (b) other data categories	

Data Transfer Impact Assessment (DTIA) – Step 2



Data Transfer Impact Assessment – Practical Obstacles

A few **practical comments** on the DTIA:

- The European DPA and the EDPB intentionally make it difficult. 40+ pages of "guidance from the the EDPB
- There is no template; the DPA expect an individual, thorough risk assessment.
- Art. 14 SCC Data exporters and data importers must cooperate.
- EU data exporters have complained that the EDPB forces them to become "experts" in foreign surveillance laws, which may not be publicly available.
- Challenge: How to get reliable info from sources in the target countries?
- Argument: "There is no alternative to the data transfers?"
- Enforcement?

Data Transfer Impact Assessement: Does the individual surveillance risk count?

Can I consider the individual risk of the data being disclosed to the NSA and other US authorities?

- Article 44 GDPR expressly says that it is "subject to the other provisions" of the GDPR.
- Article 44 is subject to Article 24(1) which requires the controller to identify the risks to the rights and freedoms of natural persons and to take into account the likelihood and severity of those risks in relation to the nature, scope, circumstances and purposes of the processing for each data processing operation.
- Thus, Article 24(1) sets forth the fundamental obligations of the controller and makes assessing risk part of the accountability principle set forth in Article 5(2).
- Since, pursuant to Article 24(1), the controller must assess the risk to natural persons of any data transfer, it is incorrect for the Austrian DPA and others to have concluded that Chapter V is not risk-based.

Data Subject Access Rights

Morgan Lewis

DSARs: The Scope of Access Rights

Privacy Laws Granting Access Rights	What are the key individual's (consumer) rights?
• GDPR • UK GDPR • California (CCPA, CPRA) • Virginia • Colorado • Utah • Connecticut	• Access • Correct (Rectification) • Delete (Erasure) • Portability • Restrict processing

DSARs: Key Considerations When Responding

Response Deadlines

- State Privacy Laws (CA, VA, CO, UT, & CONN)
  - **45 days to respond**
  - 45-day extension in some circumstances
  - Right to Appeal (VA, CO, & CONN)
  - 10 days to confirm receipt (CA-draft CCPA regs)
- GDPR
  - **1 month to respond *(not 30 days)***
  - Extension by 2 months in **exceptional** cases
  - No right to Appeal

Know Data Sources

Verify Identity

- Use reasonable measures to verify individual's identity
- Do not release personal data without verifying request
- Securely send any personal information

DSARs: Planning for Compliance

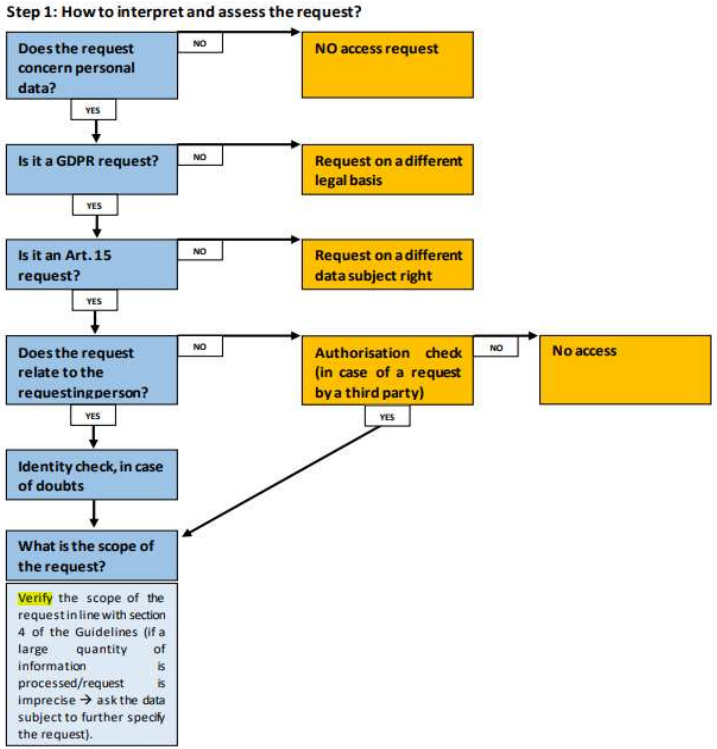
State Privacy Rights

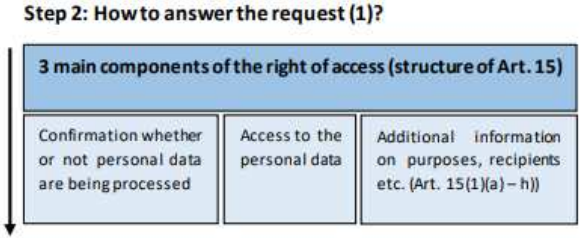
- 2023 will be a significant year for DSARS in US
  - How common will requests be?
  - Types of companies and industries targeted?
- 2024 and beyond – expansion to other states?

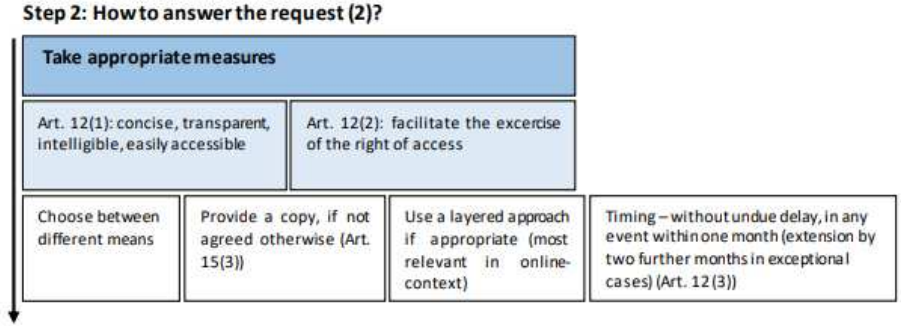
Learn from GDPR/ UK GDPR Guidance & Experiences

- UK Information Commissioner's Office (ICO)
- European Data Protection Board (EDPB)
  - Draft Guidelines on Data Subject Rights- The Right of Access
  - Issued January 18, 2022
  - Comments Received through March 11, 2022

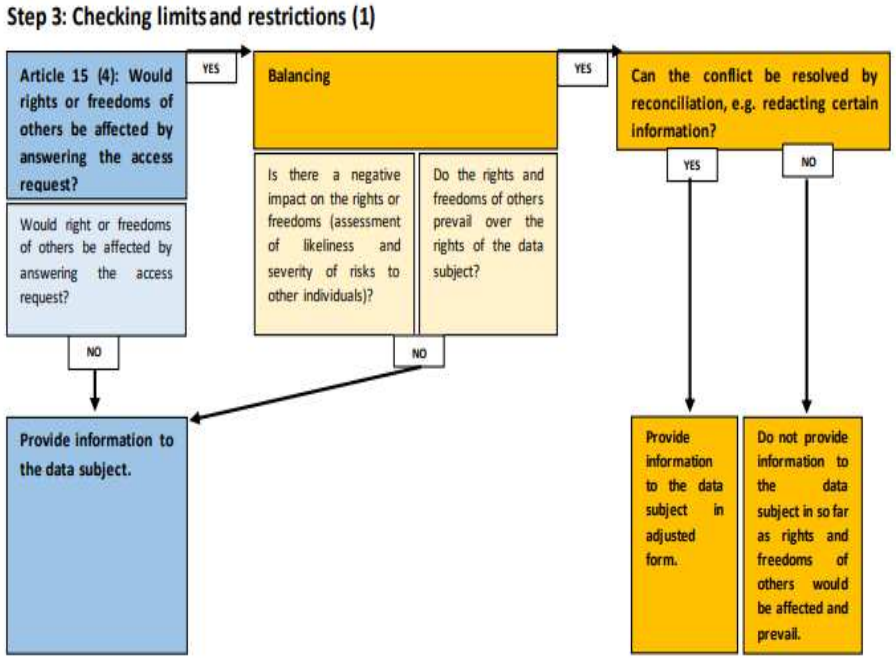
DSARs: Planning for Compliance – EDPB Flowchart

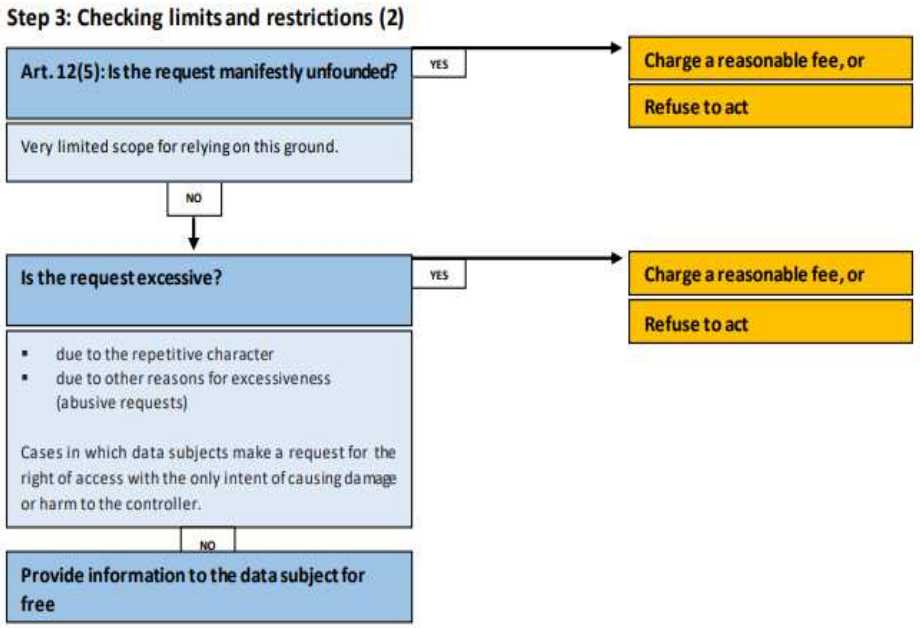






DSARs: Planning for Compliance – EDPB Flowchart





US Data Privacy - Regulatory Landscape

Morgan Lewis

Tracking Data Privacy Developments

Morgan Lewis

Our Practice Our People Our Approach Our Thinking Our Firm Careers

Home > Our Thinking > Publications > US Privacy and Data Protection Law Tracker SUBSCRIBE

REPORT

US PRIVACY AND DATA PROTECTION LAW TRACKER

April 29, 2022

Organizations across the United States have devoted significant resources since 2018 to ensure compliance with the California Consumer Privacy Act (CCPA) and subsequent data privacy laws introduced by other state and local governments. To help companies and institutions of all sizes navigate the myriad challenges of this evolving regulatory landscape, Morgan Lewis is tracking developments in all 50 states as new data privacy legislation is proposed, enacted, and amended.

Organizations can leverage our US Privacy and Data Protection Law Tracker to stay up to date on the latest data privacy laws in the United States. Using the CCPA as a baseline, our tracker identifies key provisions of each proposed or enacted legislation, specifying individual rights, business requirements, data protection, breach notification, third-party requirements, and biometrics in each jurisdiction.

RELATED RESOURCES

SERVICES

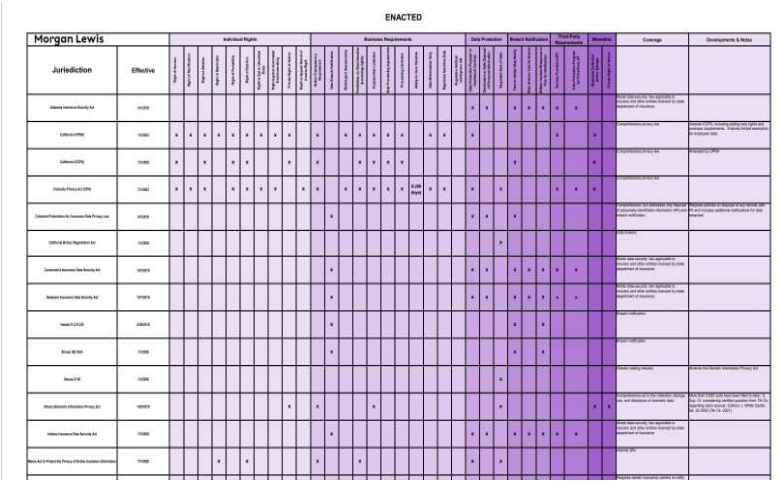
- eData
- Privacy & Cybersecurity

REGIONS

- North America

TRENDING TOPICS

- US Consumer Privacy Acts



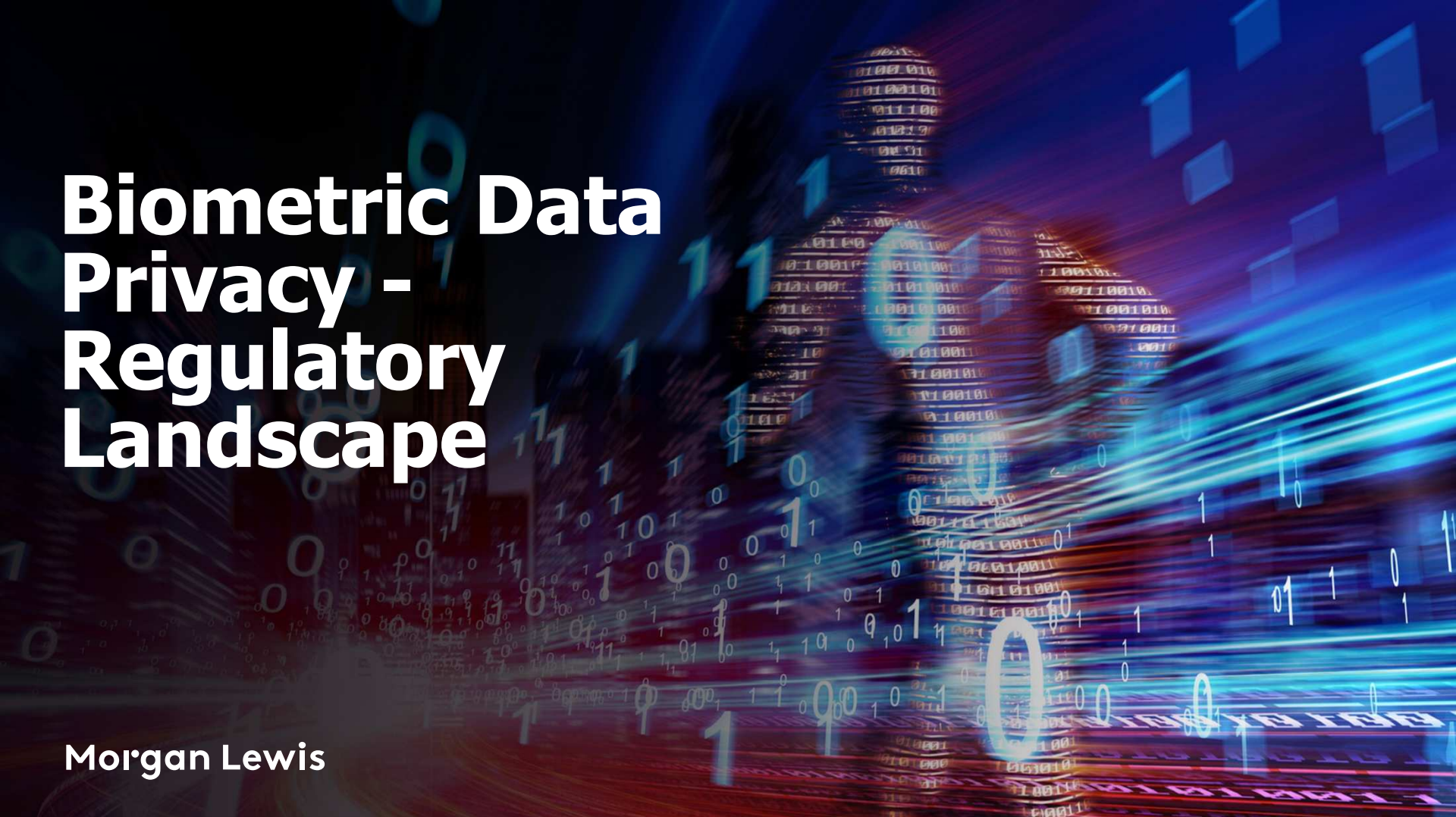
[US Privacy and Data Protection Law Tracker – Publications | Morgan Lewis]

Morgan Lewis

US Data Privacy Laws

California	CCPA – *effective Jan. 1, 2020* *&* CPRA – *effective Jan. 1, 2023*
Virginia	Consumer Data Protection Act – *effective July 1, 2023*
Colorado	Privacy Act – *effective July 1, 2023*
Utah	Consumer Privacy Act – *effective December 31, 2023*
Connecticut	Personal Data Privacy and Online Monitoring Act – *effective July 1, 2023*

Biometric Data Privacy - Regulatory Landscape



Morgan Lewis

Illinois Biometric Data Privacy Act (BIPA)

Regulates collection, processing, disclosure of biometric information and identifiers

Biometric identifiers include:

- Retina or iris scan
- Fingerprint,
- Voiceprint,
- Scan of hand or face geometry

Grants private right of action for violations

- No actual harm required, technical violation enough for liability
- $1,000 per negligent violation, $5,000 per intentional violation
- Attorneys' fees
- Injunctive relief

Illinois Biometric Data Privacy Act (BIPA)

Obligations for covered businesses

- Develop written policy
- Provide written notice about purpose of biometric collection and retention
- Obtain consent before collection and storage of biometric data
- Destroy biometric data in timely manner
- Prohibits selling, leasing, or otherwise profiting from use of biometric data

Significant BIPA Class-Actions against Social Media Companies

- $650 million settlement
- $92 million settlement

Other State Biometric Data Privacy Laws

- In 2022, new Biometric laws considered in at least 8 states
- Texas Biometric Protection Act (2009)
- Washington Biometric Identifiers Act (2017)
- No private rights of action in TX or WA
- Violations enforced by State Attorney General only
  - Still creates significant liability for violations
    - Texas seeking billions in damages for use of facial recognition technology against a social media company
    - Claims violations for up to 20 million Texas consumers

Local Biometric Data Privacy Laws

New York City – Biometric Information Law (2021)

- Regulates collection and use of biometric customer data by businesses

New York City – Tenant Data Privacy Act (2021)

- Regulates biometric data collected by multi-family buildings
- Covers smart-access building controls that use biometrics

Baltimore, Maryland Council Bill 21-0001 (2021)

- Restricts use of face-surveillance systems

Portland, Oregon, City Code 34.10.010 (2021)

- Prohibits use of facial recognition technology by businesses offering public accommodations


Artificial Intelligence (AI) Regulatory Landscape
Morgan Lewis

Data Privacy Laws & AI

- Data Privacy Laws Regulate "Profiling" & "Automated Decision Making"
  - Profiling:
    - Involves large-scale collection of personal data and use of algorithms, AI or machine-learning
    - Evaluates aspects of an individual's personality, interests and habits to make predictions or decisions
    - Uses algorithms to find correlations between separate datasets
  - Automated Decision Making
    - Involves profiling but does not have to
    - Process of making decisions by automated means
    - No human involvement
    - Decisions can be based on factual data, digitally created data or inferred data
- Examples:
  - Marketing (profiling)
  - Prediction of medical outcomes based on group characteristics (profiling)
  - Online decision to extend credit (automated decision)

Federal: Federal Trade Commission (FTC)

- Considers AI discrimination and related data misuse to be within its purview
  - Sale or use of racially biased algorithm could be unfair or deceptive practice under Section 5 of FTC Act
  - Use of algorithm to deny employment, housing, credit, insurance, or other benefits could implicate Fair Credit Reporting Act (FCRA)
  - Use of biased algorithm that results in credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or because a person receives public assistance could violate Equal Credit Opportunity Act
- FTC considering regulations to "curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination."

Federal: Other Agencies

Food & Drug Administration

- Developing regulatory framework for medical devices that use AI software

Equal Employment Opportunity Commission

- New initiative on AI and algorithmic fairness in hiring and employment decisions

Department of Housing & Urban Development

- Rule allowing discrimination claims for housing-related algorithms

Department of Transportation

- Developed Comprehensive Plan for future regulation of Automated Driving Systems

Federal: Congressional Action

Algorithmic Accountability Act of 2022

- Pending in House and Senate
- Requires companies to assess the impacts of the automated systems they use and sell
- Creates new transparency about when and how automated systems are used
- Allows consumers to make informed choices about the automation of critical decisions
- Grants additional regulatory authority to FTC on AI use by companies

State Laws

- AI bills introduced 17 states in 2021
- Multiple state commissions and working groups established to study AI-related issues
- Key laws
  - Illinois' Artificial Intelligence Video Interview Act (2020)
    - Regulates use of AI during video interviews
  - Colorado's Unfair Discrimination in Insurance Practices (2021)
    - Prohibits use of external consumer data in algorithms or predictive modeling to make discriminatory decisions

Biography

Tess Blair
Partner | Philadelphia
+1.215.963.5161
tess.blair@morganlewis.com

Tess is a litigator and legal entrepreneur who has practiced at the intersection of law, technology, and design for more than two decades. Tess is the founder and leader of Morgan Lewis's eData practice, a data-driven practice that combines great lawyering with technology and design to enhance the delivery of legal services.

Biography

William Childress
Senior Attorney | Philadelphia
+1.215.963.4999
william.childress@morganlewis.com

William counsels clients on electronic discovery. William's practice focuses on negotiations with opposing counsel, motion practice related to discovery, and litigating discovery disputes. He has handled all phases of litigation. Prior to joining the firm, William clerked for Judge P. James Jones in the US District Court for the Western District of Virginia, worked as an associate in the litigation practice of an international law firm, and as a staff attorney for the Supreme Court of Virginia.

Biography

Dr. Axel Spies
Special Legal Consultant |
Washington, DC / Frankfurt
+1.202.739.6145
axel.spies@morganlewis.com

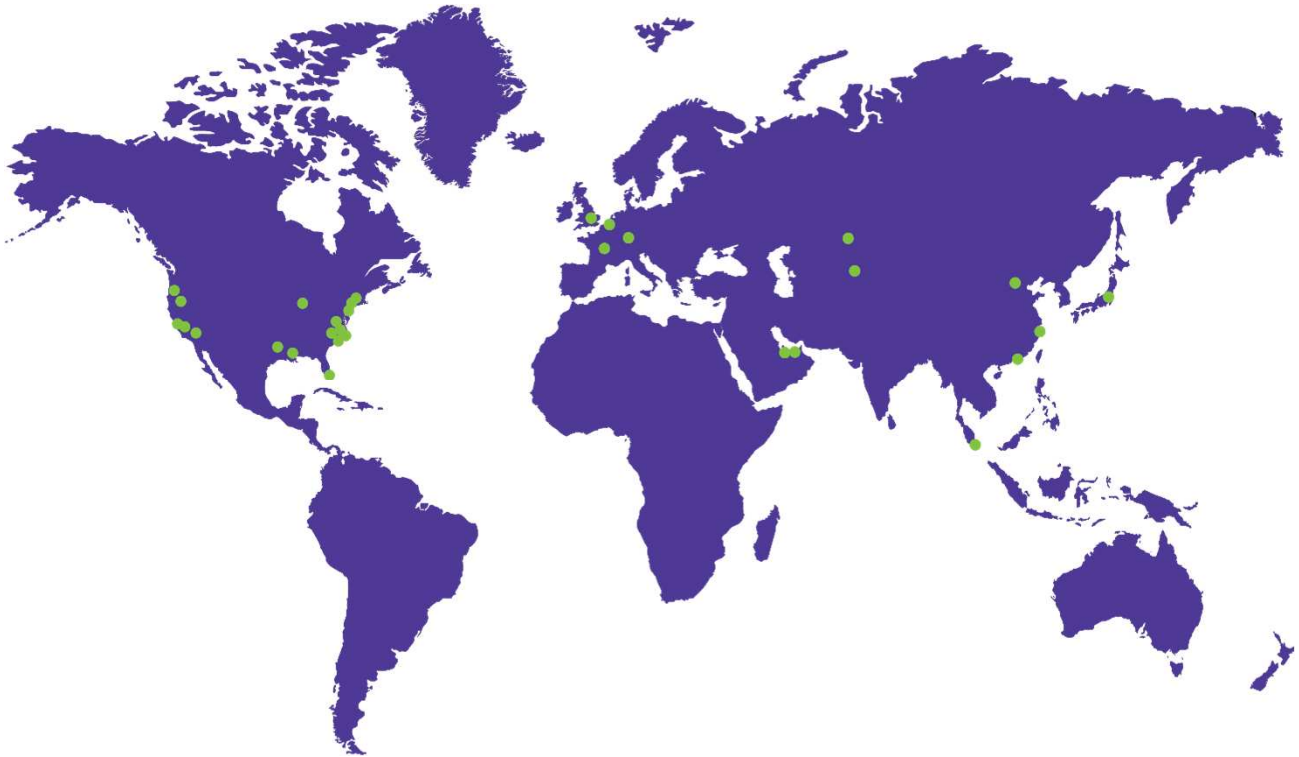
Axel has advised clients for many years on various international issues, including licensing, competition, corporate issues, and new technologies such as cloud computing and international telecommunications licensing. He counsels on international data protection (EU General Data Protection Regulation), international data transfers and compliance, healthcare, technology licensing, e-discovery, and equity purchases. A member of the Sedona Conference on Electronic Discovery, Dr. Spies is frequently quoted in the media for his telecommunications and privacy knowledge.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU