Morgan Lewis

SILICON VALLEY FIRST CUP OF COFFEE BRIEFING SERIES:

EU DATA TRANSFER AND US IP LITIGATION AFTER SCHREMS II

November 19, 2020

Morgan Lewis

SILICON VALLEY FIRST CUP OF COFFEE BRIEFING SERIES:

ARTIFICIAL INTELLIGENCE (AI) BOOT CAMP

JANUARY 12 – FEBRUARY 16

- Bioinformatics
- M&A and Investment into AI Companies
- AI in Digital Health
- Patentability of AI Inventions
- AI in Hiring and Recruiting
- AI and Copyright
- The Ethics of Artificial Intelligence for the Legal Profession
- AI and Data Privacy
- Patents for MedTech AI: Opportunities and Pitfalls
- IP Landscape of AI Hardware Startups
- Fallibility of AI Algorithms in Making Correct Decisions about Human Behavior
- AI in Digital Advisory Offerings
- Bias Issues and AI

Morgan Lewis

SILICON VALLEY FIRST CUP OF COFFEE BRIEFING SERIES:

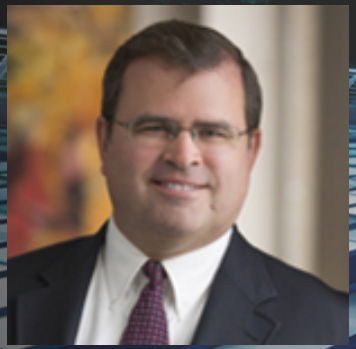
EU DATA TRANSFER AND US IP LITIGATION AFTER SCHREMS II

November 19, 2020

Presenters

Robert C. Bertin

Dr. Axel Spies



Andrew J. Gray IV

Morgan Lewis

Agenda for today

- E-discovery for data from the EU after Schrems 2
- Discover in US IP Litigation – Effects of Schrems 2

E-discovery for data from the EU after Schrems 2

Morgan Lewis

The European Union's and US's Approach to Data Protection

- The U.S. and the EU have different approaches to data privacy protection

- U.S. System based on:
  - **Self-regulation**
  - **Sector specific legislation in highly sensitive areas such as financial, medical, children's and genetic information**
  - **Enforcement (FTC Section 5 Authority)**
  - **Mostly state law - *e.g.*, data breach notifications, CCPA**

European Approach

- Top down, GDPR, directly applicable in all EU Member States
- Additional national Data Protection Laws
- DPAs in each country who can impose fine, perform audits etc.
- A fundamental right (European Charter of Fundamental Rights), right does not depend on citizenship

Article 8
Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Data Transfer from EU Countries to Non-EU Countries Permitted If (the Top Four):

- Non-EU country provides "adequate" data protection → to date, only a handful of countries/territories, such as Argentina, Canada, Japan, Israel, Switzerland, Uruguay…
- Recipient of EU personal data entered into a contract assuring adequate data protection (*e.g.*, incorporates EU standard contractual clauses);
- Data subject "unambiguously" consented to transfer; OR
- Transfer necessary to perform a contract between the controller and the data subject;

... And more.

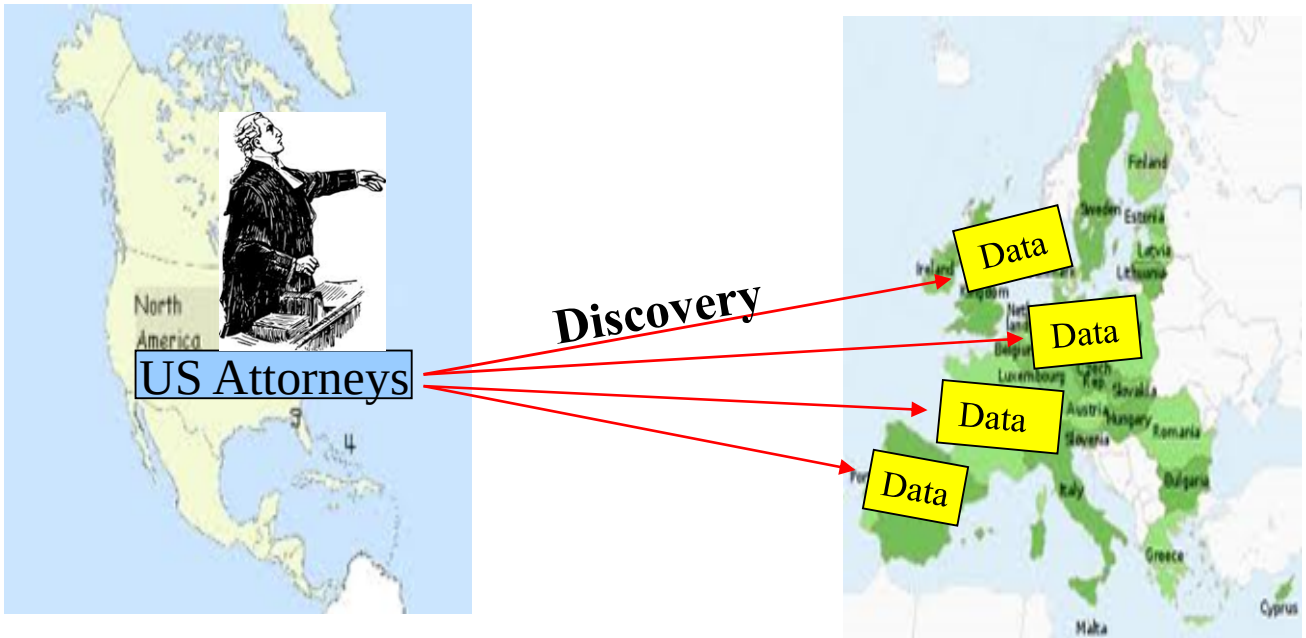
Aerospatiale Factors

US Supreme Court No. 85-1695.
Argued Jan. 14, 1987.
Decided June 15, 1987

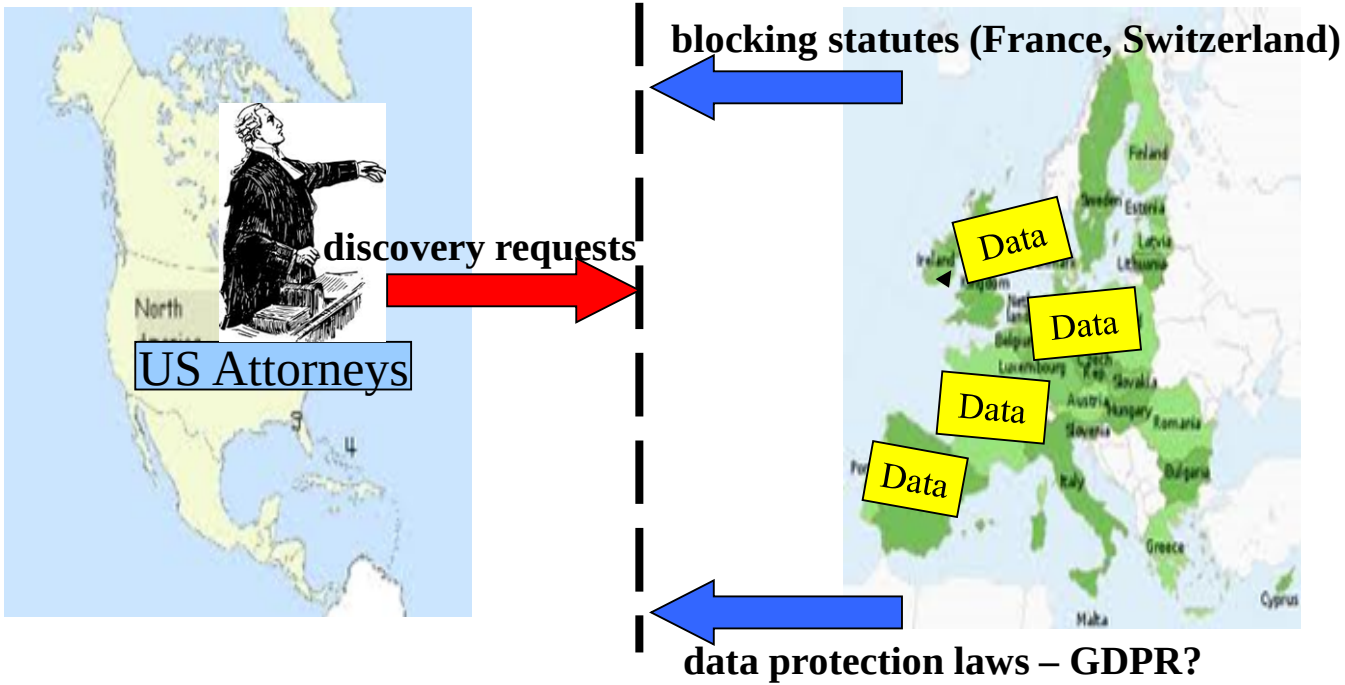
Still the guiding case. Cited in hundreds of US court decisions

- Importance of documents to litigation
- Degree of specificity of discovery request
- Whether information originated in US
- Alternative means of obtaining info
- Balance of US and foreign interests

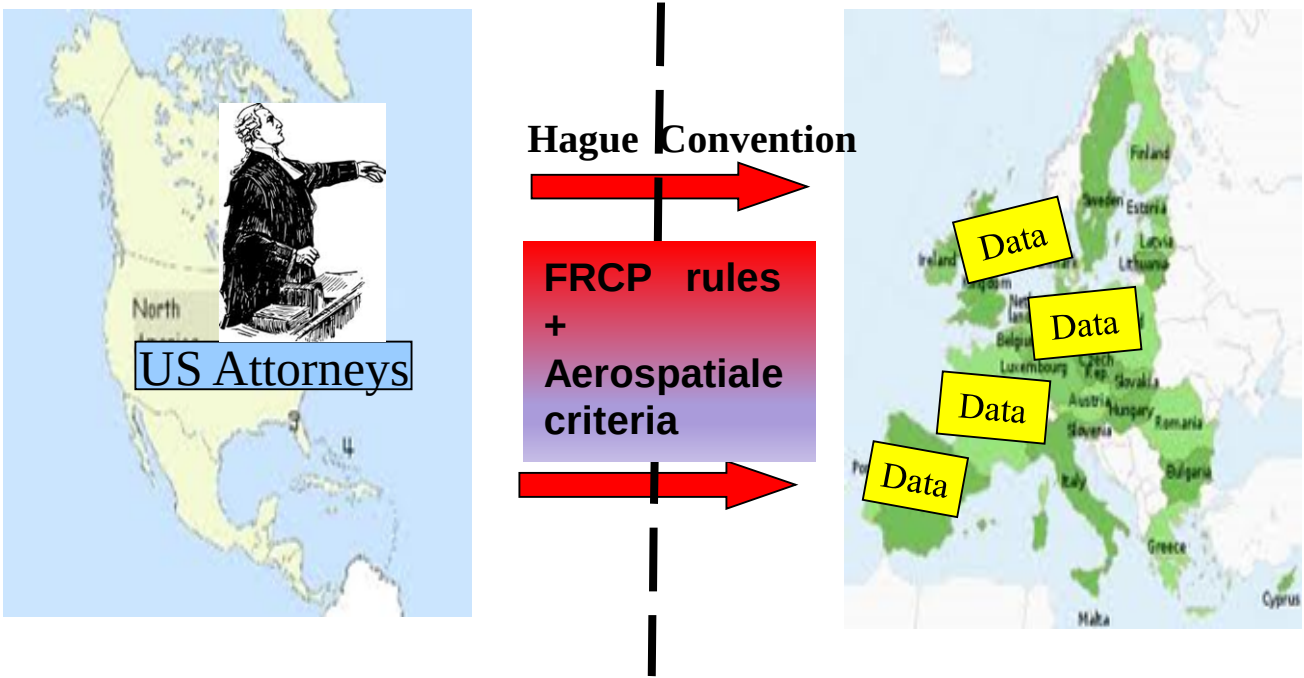
Scenario: US Litigation requires data from the EU



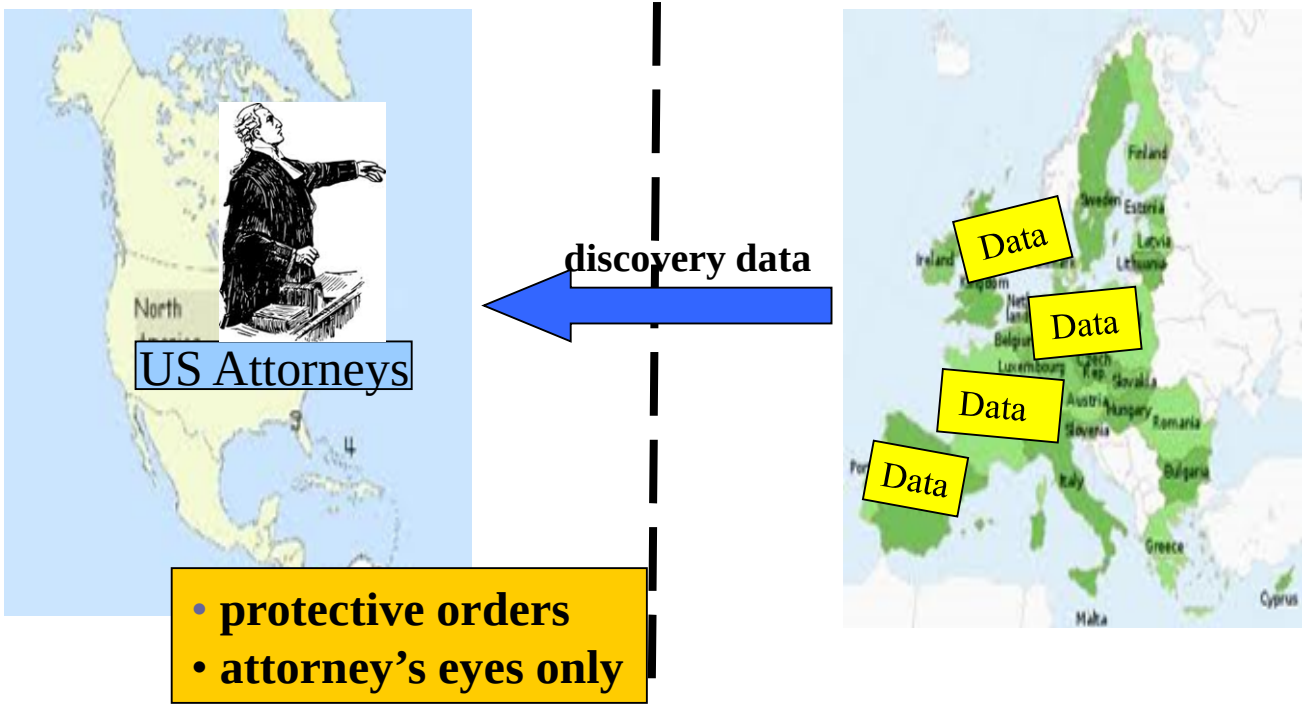
Scenario US Litigation (2)



Scenario US Litigation (3)



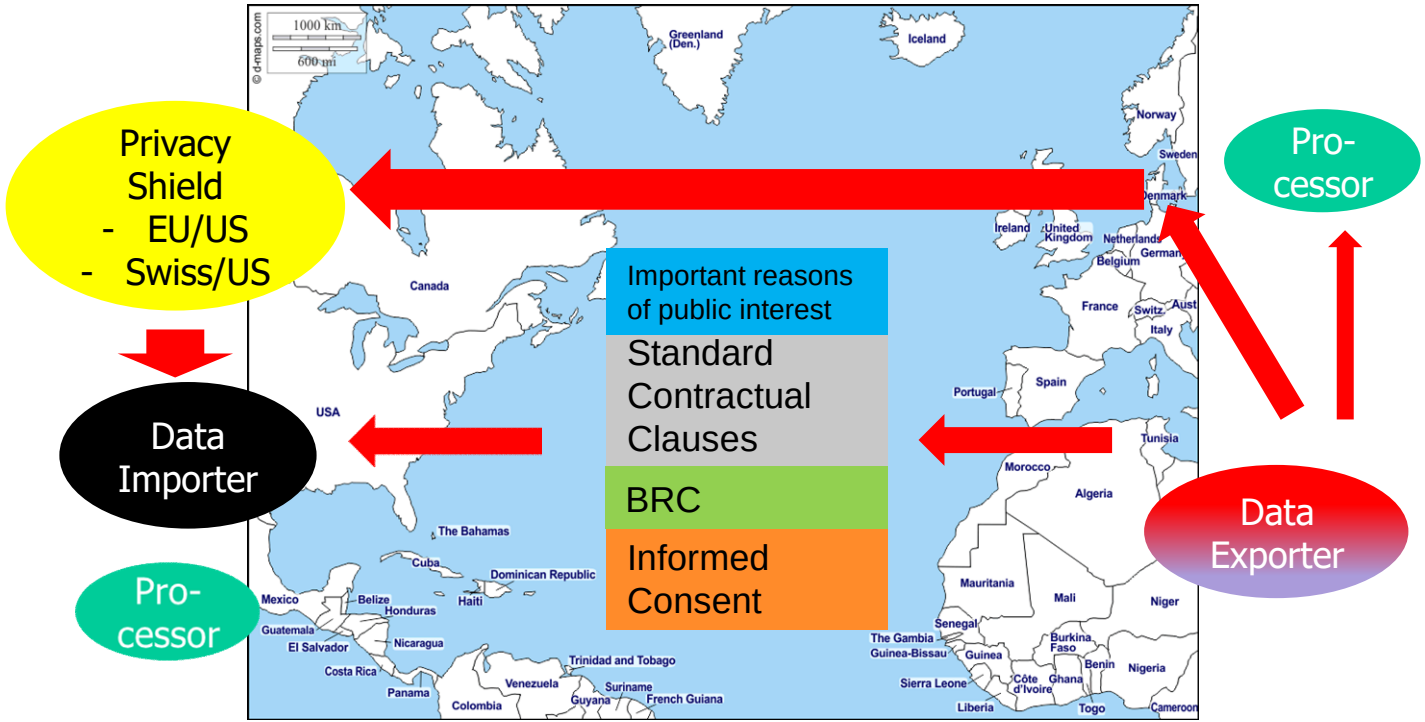
Scenario US Litigation (3)



A few basics on EU-US data transfers specifically

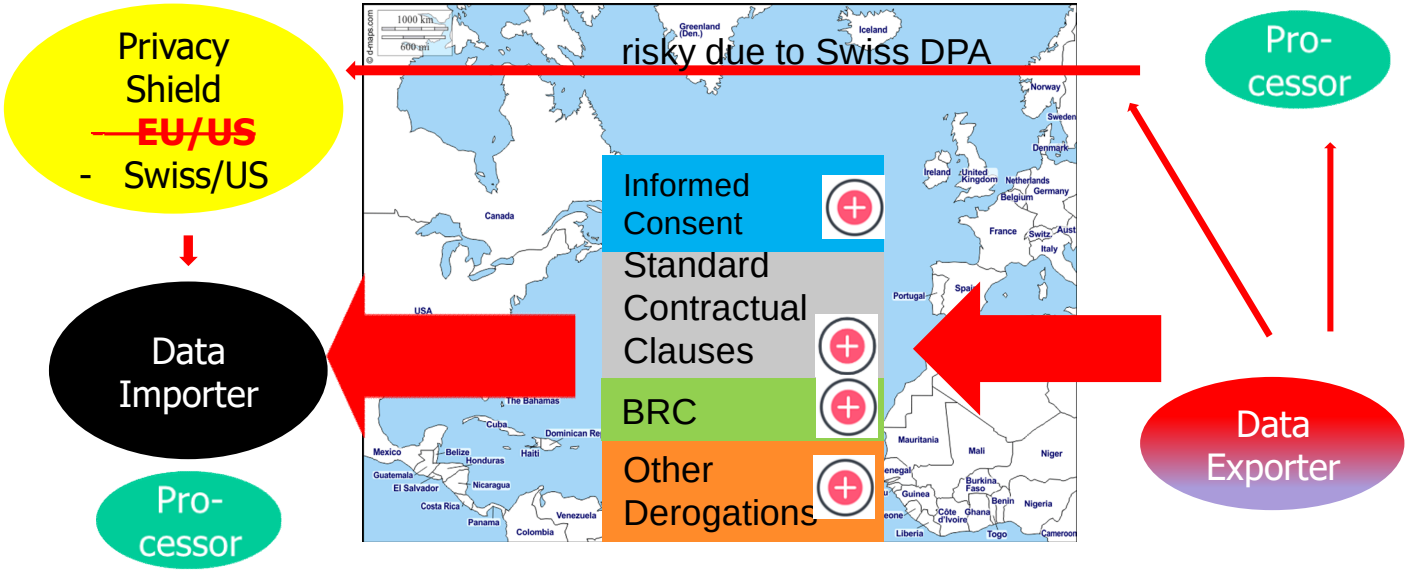
- The GDPR broadly prohibits the transfer of personal data to so-called "third countries", subject to certain exceptions.
- One such exception where the European Commission has made an 'adequacy decision': a finding that the receiving country has in place adequate protection for the rights and freedoms relating to individuals' personal data, equivalent to those available within the EU.
- US was deemed **not** to provide protections equivalent to those available in the EU.
- US Department of Commerce and the European Commission devised the **Privacy Shield** in 2016/17 as a set of principles designed to ensure equivalent protection via self-certification.
  - Administered by Department of Commerce
  - Enforced by FTC
  - As of July, 5,000+ data importers registered

The Data Transfer World from the EU before July 16, 2020



Enter Mr Schrems → CJEU “Schrems 2”

The Data Transfer World from the EU After July 16, 2020



CJEU Case C-311/18 - "Schrems II"

16 July 2020→ Court of Justice of the European Union (CJEU) → judgment (ruling):

- EU Privacy Shield Framework decision for data transfer between the EU **is invalid from the EU perspective**
- **No grace period**
- Reducing the available options for the sharing of personal data between the two regions.
- "**Additional measures**" may be required before companies may rely on traditional means to justify international data transfers.

Data Exporters and Importers:

- risk balancing exercise with insufficient guidance from the DPA → **they want a case-by-case analysis and not only for EU-US data flows.**
- fine line between compliance with their obligations under GDPR and their need to export data outside the EEA to conduct their business.

→ New EDPB Roadmap ("recommendations") released 11/11/2020

What does the GDPR state on data transfers for litigation purposes?

- **Art. 49 (1) Derogation**

[…] a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

- **Art. 48 GDPR**

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data **may only be recognised or enforceable in any manner if based on an international agreement**, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

How does "Schrems II" influence the interpretation of these two GDPR Provisions?

- "Schrems II" does not mention "discovery" and Article 48, 49 (1) (e) GDPR explicitly

- **BUT**
- As the Privacy Shield is no more available, how do companies bring discoverable information into the U.S.?
- Must companies interpret **Article 49 (1) (e) GDPR** more narrowly now?

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

→ When is a transfer "necessary"

→ Which legal claims are covered?

- **EC Standard Contractual Clauses** (new set released 11/12/2020)

Tool 1: Article 29 Group (Opinion issued in 2009)

- In February 2009, the group of representatives of the data protection authorities at EU level, the Art. 29 Working Party, published an opinion on e-discovery from a data protection perspective. Not legally binding.
- Opinion: There are legitimate legal interests to view, evaluate and transmit documents in Europe for US proceedings.
- However, the legal protection interests of the persons concerned must be weighed against them.
- The balancing with the interests of data protection has to be done during all phases of the e-discovery.
- Parties must involve data protection officers in the procedure as early as possible.

Tool 2: Solution suggested by the French data protection authority CNIL (2008/2009)

- CNIL distinguishes between data transfers that are one-off and involve, to a limited extent, personal data for defense purposes, and data transfers in which large amounts of data are transferred.

Tool 3: US Sedona Conference

- US Sedona Conference - a non-profit organization in the US
- Its Working Group 6 focuses on questions of international e-discovery. It has prepared a paper with detailed proposals.
- Introduction of a data protection certificate (Compliance Certificate).

US Sedona Conference (2)

- Suggested Contents of the Compliance Certificate issued by the data exporter:
  (1) the purpose of the data collection
  (2) Type and duration of data collection
  (3) Measures to limit data collection such as search terms used or information about filtering the data
  (4) Listing the type of data collected - Word, emails, etc.
  (5) Confirmation that the estimated data of a Protective Order or other party agreement for their protection
  (6) Resources that allow the data subject to be informed about his/her rights
  (7) Measures against data loss and for data protection
  (8) Indication whether the certificate has been submitted to a data protection authority or is submitted to it
  (9) Information on the basis of which the data transfer to the USA is carried out (consent, EU Model Clauses)
  (10) Designation of a person responsible for the proper execution of the data transmission.

Tool 4: European Data Protection Board on Art. 49 (1) (e) GDPR - Guidelines 2/2018

RELEVANT QUOTES:

- "This [provision] covers a range of activities for example, in the context of a criminal or administrative investigation in a third country (e.g. anti-trust law, corruption, insider trading or similar situations), where the derogation may apply to a transfer of data for the purpose of defending oneself or for obtaining a reduction or waiver of a fine legally foreseen e.g. in anti-trust investigations."
- "As well, data transfers for the purpose of formal pre-trial discovery procedures in civil litigation may fall under this derogation."
- "The derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future."
- "Data controllers and data processors need to be aware that national law may also contain so-called "blocking statutes", prohibiting them from or restricting them in transferring personal data to foreign courts or possibly other foreign official bodies."

European Data Protection Board on Art. 49 (1) (e) GDPR - Guidelines 2/2018 (2)

- **Necessity of the data transfer** "A data transfer in question may only take place when it is necessary for the establishment, exercise or defense of the legal claim in question. This "necessity test" requires a close and substantial connection between the data in question and the specific establishment, exercise or defense of the legal position. The mere interest of third country authorities or possible "good will" to be obtained from the third country authority as such would not be sufficient."
- **"As a first step**, there should be a careful assessment of whether anonymized data would be sufficient in the particular case. If this is not the case, then transfer of pseudonymized data could be considered. If it is necessary to send personal data to a third country, its relevance to the particular matter should be assessed before the transfer – so only a set of personal data that is actually necessary is transferred and disclosed."

European Data Protection Board on Art. 49 (1) (e) GDPR - Guidelines 2/2018 (3)

- **Occasional transfer** Such transfers should only be made if they are occasional. For information on the definition of occasional transfers please see the relevant section on "occasional and "non-repetitive" transfers.
- Data exporters would need to carefully assess each specific case.
- EDPB confirms this narrow interpretation in its recent Roadmap (11/11/2020).

→ **Is eDiscovery, involving thousands of more of documents prohibited?**

What to do? General Considerations

- **Rule:** Limit the number of documents to be submitted as much as possible. Risk: GDPR civil and administrative fines for unauthorized data transfer of sensitive sanctions.
- **But not too much:** The court in the USA could qualify a general ban on data transfer as a blocking statute.
- "Clean Hands" Doctrine.

- Recommendations for action by the Art. 29 Working Group are not specific enough. EDPB better.
- European data protection authorities, with the exception of the French CNIL, are reluctant to go alone on this issue.
- Preliminary inquiries to the data protection authority concerned are usually without success: answer cannot usually be provided in a time frame acceptable to all, lack of personnel, lack of expertise.
- Ensure that the recipient in the US provides adequate protection to the data.
- United States is on the radar of the DPAs. Some are more proactive than others.

What to do? Meet and Confer + Filtering on the ground

- Be well prepared
- Know legal and organizational challenges of an international e-discovery beforehand.
- Be aware that the production schedule is tight; there is a risk that the risk assessment for the data transfer will be take a back seat or will not take place at all.
- Sift through documents with keywords for their relevance and limit the scope of the e-discovery by agreement with the other party including a production schedule.
- A general blackening of names cannot be derived from the data protection requirements.

How to deal with Schrems II within the company that must produce EU documents.

- **DO not** rely on the Privacy Shield to transfer data into the US.
- **But:** Store as much data as possible on servers in the EU (plus U.K.?).
- **And:** Having Standard Contractual Clauses in place is a good idea
- **But:** They may not always work (same entity as data exporter and data importer) → guarantee? EDPB Roadmap?

- **DO not** solely rely on Art. 49 (1) (e) GDPR
- **Consider:** Consents of the data subject – practical, but not always feasible (Data subject must be able to withdraw consent, consent "voluntarily given"?).
- **Consider:** SCC Risk Assessment - cf. EDPB Roadmap
- **Always** involve the Data Protection Officer and the works council of the data exporter, exemptions apply.

Discovery in US IP Litigation – Effects of Schrems 2

Morgan Lewis

Discovery of Parties In US Federal Court - General

The General Rule:

- Federal Rule of Civil Procedure 34(a)(1) specifies that parties may only request the production of documents or electronically stored information (ESI) "in the responding party's possession, custody or control."

Discovery of Parties In US Federal Court - General

The General Rule:

- Federal Rule of Civil Procedure 34(a)(1) specifies that parties may only request the production of documents or electronically stored information (ESI) "in the responding party's possession, custody or control."

Actual Possession vs. Legal Right to Obtain:

- Courts have held that ESI is within a party's custody or control not only when the party has actual possession or ownership of the information, but also when the party has "**the legal right** to obtain the documents on demand," *In re Bankers Trust*, 61 F.3d 465, 469 (6th Cir. 1995), *cert. dismissed*, 517 US 1205 (1996). This legal right may be based on contractual clauses creating the legal right between corporate affiliates or with third parties.
  - see *Flagg v. City of Detroit*, 252 F.R.D. at 352 (court held that defendant was obligated to produce text messages stored with its third-party service provider because messages were within the defendant's control); *Tomlinson v. El Paso*, 245 F.R.D. at 477 (court held company had control of certain electronic ERISA records maintained for the company by a third-party service provider and, therefore, had to produce them).

Discovery of Parties In US Federal Court - General

The General Rule:

- Federal Rule of Civil Procedure 34(a)(1) specifies that parties may only request the production of documents or electronically stored information (ESI) "in the responding party's possession, custody or control."

Actual Possession vs. Practical Ability to Obtain ESI:

- Some jurisdictions have held that documents are under a party's control when the party has the '**practical ability**' to obtain documents from a non-party to the action," as in *Bank of New York v. Meridien BIAO Bank Tanzania*, 171 F.R.D. 135, 146 (S.D.N.Y. 1997);
  - See *Tomlinson v. El Paso*, 245 F.R.D. 474, 477 (D. Colo. 2007) (documents are within a party's control "if such party has retained any right or ability to influence the person in whose possession the documents lie");
  - But see *Phillip M. Adams & Associates v. Dell*, 2007 WL 626355, at *3 (D. Utah Feb. 22, 2007) (noting how district courts have rejected the "practical ability" test). Application of the 'practical ability test' is difficult in practice.

Discovery of Parties In US Federal Court - General

- **International Discovery Occurs in two primary ways:**
  - **Discovery of a party**
  - **Discovery of third parties**

- **International Discovery from a Party**
  - **Testimony and Documents may be sought through the federal rules of civil procedure, after a Court obtains jurisdiction over the party.**
  - **The U.S. Supreme Courts' *Aeropostale* case sets forth how parties seeking discovery can obtain the information they need successfully.**
    - **There may be international constraints that the Court and the parties have to work with.**
- **International Discovery from a Third Party**
  - **Testimony and Documents may be sought through the Federal Rules of Civil Procedure and the Hague Convention.**
    - **Discovery requires procedures before both the Federal District Court and foreign authorities and can be time consuming and limited in scope**

International Discovery from Parties - Aeropostale

- *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa* ("*Aerospatiale*")
  - This is one of the leading cases, decided by the Supreme Court, on International Discovery when there is a conflicting foreign statute.
  - In it, the Court affirmed the general rule:
    - Foreign laws precluding the disclosure of evidence "do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [foreign] statute."
    - When a U.S. court has jurisdiction, the Federal Rules of Civil Procedure apply. It may not be necessary in all cases to resort to, for instance, Hague Convention procedures when data is located abroad.

International Discovery from Parties - Aeropostale

- To determine whether an international treaty must be complied with, the *Aerospatiale* Court set out five factors for consideration:
  (1) the importance to the litigation of the documents or other information requested;
  (2) the degree of specificity of the request;
  (3) whether the information originated in the United States;
  (4) the availability of alternative means of securing the information; and
  (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine the important interests of the state where the information is located.
- Many courts, such as the Ninth Circuit in *Richmark* also considered the hardship the producing party will face by non-compliance with the foreign law.
- In applying *Aerospatiale* before GDPR, U.S. courts overwhelmingly held in favor of disclosure when litigants sought to withhold discovery covered by foreign data protection laws.

Discovery of Information in Europe - Recent Cases

- Post GDPR Cases:
  - Some assiduously apply Aeropostale
  - Others have dismissed discovery attempts without all of the rigor when the discovery request is not properly justified.

- Example: Finjan, Inc. v. Zcaler, Inc. (N.D. Cal. 2019)
  - Applies *Aeropostale factors*.
  - The plaintiff sought discovery of emails defendant's employee who had worked in the United Kingdom.
  - The defendant refused to produce the emails, citing GDPR as justification.
  - The court ultimately compelled disclosure of the emails.

International Discovery from Parties – Recent Cases

- Finjan Rationale:
  - The requested data was directly relevant to the infringement issue,
  - The email request was narrow and a protective order applied to its production.
  - The Court also focused on the **balance of national interests**, finding
    - This factor weighed heavily in favor of disclosure of the emails.
    - The United States has a strong interest in protecting U.S. patents, while noting the U.K.'s interest in protecting the privacy of its citizens.
    - There is doubt that U.K interests were implicated by the discovery request because (i) GDPR permits information to be transferred for litigation and (ii) the defendant admitted that "the GDPR permits 'the discovery of personal data to that which is objectively relevant to the issues being litigated.'"
    - The court noted that the weight of the foreign privacy interest to be considered is "diminished where the court has entered a protective order preventing disclosure of the secret information."
    - The defendant produced no evidence that disclosure of the emails would lead to hardship or an enforcement action from an EU data protection supervisory authority.

Discovery of Information in Europe - Recent Cases

- *Pearlstine v. Blackberry Limited*, 332 F.R.D. 117, 122 (S.D. N.Y. 2019)
  - The Court denied plaintiff's motion to compel defendant to reveal a person's private home address
  - "Defendants have represented that, under the European Union's General Data Protection Regulation, they are unable to disclose his address without his consent, which they have not received."
  - The court did not analyze the issue in terms of explaining its weighing of the Aérospatiale factors.
  - This case might have been more successful if Plaintiffs themselves had followed or been able to follow the Aeropostale factors.

Cloud Data - Schrems

- **Parties to Litigation with ESI "in the cloud"**
  - Cloud service providers epitomize decentralization of data and storing and transferring it across national boundaries in many cases.
  - A US party using a cloud service provider may have access to information associated with European Citizens.
  - US Companies may also have agreements with third parties or affiliates that directly or indirectly store and transfer data across national boundaries, or in any event .
  - United States v. Microsoft Corp. in the criminal warrant context raised some of the issues
  - Schrems provides a further justification for plaintiffs to argue that they do not need to produce requested discovery when in implicates privacy rights of EU citizens.

US CLOUD Act (2018)

- **US CLOUD Act** amends the Stored Communications Act (SCA) of 1986
- Allows federal law enforcement to compel U.S.-based "*provider of electronic communication service or remote computing service*" via an SCA order
- to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.
- no direct mechanism for individuals to challenge an order under the CLOUD Act.
- BUT a US court will (i) consider a provider's challenge of an order for disclosure of data and (ii) review the request under a multi-factor "comity" analysis to assess foreign and other interests at stake.

→ Criticized by EU Commission and others

Cloud Data - Schrems

- **Schrems Factors**
  - The "standards contractual clauses" between entities in the U.S. and Europe that will be adopted as a result of Schrems may provide a "**legal right**" to access data that implicates such privacy rights.
    - In such instances, an Aeropostale analysis may be conducted to determine whether to order production that includes weighing penalties of not complying with the Schrems ruling.
  - Standard contractual clauses and the course of doing business may also lead some jurisdictions to order production if a US party has a practical ability to get the information.
- **Additional Judicial Tools in the US to Enforce Discovery**
  - Spoliation has become an increasingly important issue in discovery disputes.
  - Ephemeral data and the failure to store or produce it in some cases has met with severe sanctions.
  - We Ride v. Huang (N.D. Cal. 2020) resulted in terminating sanctions against we ride for failure to change a messaging policy after litigation began that resulted in the failure to produce relevant documents.

Questions?

Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at **www.morganlewis.com/topics/coronavirus-covid-19**

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to **subscribe** using the purple "Stay Up to Date" button.

Morgan Lewis

Biography

Robert C. Bertin
Washington, DC
T +1.202.373.6672
robert.bertin@morganlewis.com

Rob Bertin has nearly 20 years of experience litigating patent, trademark, trade secret and copyright cases throughout the United States, counseling clients on intellectual property (IP) and negotiating transactions involving IP. He has represented clients at the center of some of the largest patent portfolio sale and licensing events in the high tech industry, including the Nortel and Kodak transactions. Rob leverages a technical background to represent large and small companies primarily in high technology industries.

Biography

Dr. Axel Spies
Washington, DC
+1.202.739.6145
axel.spies@morganlewis.com

Dr. Axel Spies has advised clients for many years on various international issues, including licensing, competition, corporate issues, and new technologies such as cloud computing. He counsels on international data protection (EU General Data Protection Regulation), international data transfers (Privacy Shield), healthcare, technology licensing, e-discovery, and M&A. He is a co-publisher of the German Journals ZD (Journal of Data Protection) and MMR (Multimedia Law) and a co-author on two GDPR-related German handbooks. He is a member of the Sedona Conference WP 6.

Biography

Andrew J. Gray IV
Silicon Valley
+1.650.843.7575
andrew.gray@morganlewis.com

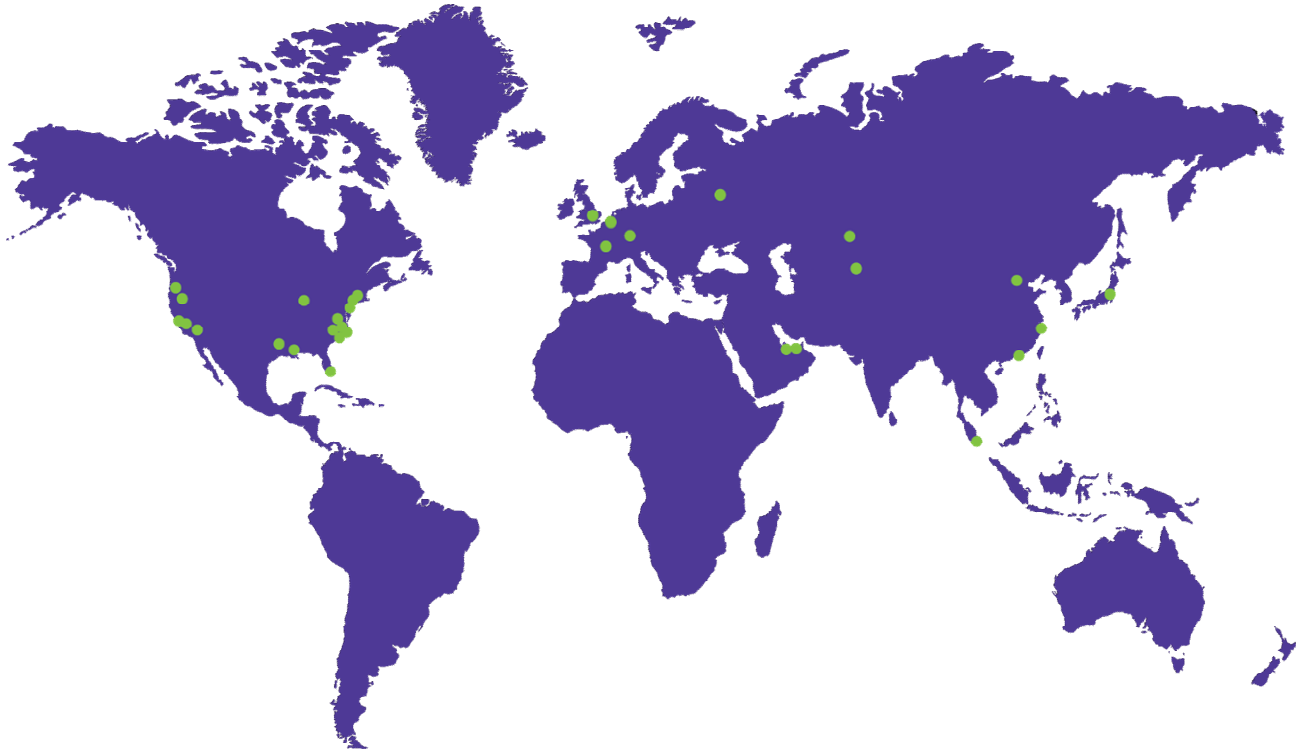
Serving as the leader of Morgan Lewis's semiconductor practice and as a member of the firm's fintech and technology practices, Andrew J. Gray IV concentrates his practice on intellectual property (IP) litigation and prosecution and on strategic IP counseling. Andrew advises both established companies and startups on Blockchain, cryptocurrency, computer, and Internet law issues, financing and transactional matters that involve technology firms, and the sale and licensing of technology. He represents clients in patent, trademark, copyright, and trade secret cases before state and federal trial and appellate courts throughout the United States, before the US Patent and Trademark Office's Patent Trial and Appeal Board, and before the US International Trade Commission.

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
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU