

# Annotated Bibliography of 2020-21 Case Law and Regulatory Activity





The Sedona Conference Working Group Six on International Electronic  
Information Management, Discovery and Disclosure

2022 Annual Meeting, February 3-4, 2022

Annotated Bibliography of 2020-21 Case Law and Regulatory Activity

John Conlon, Hon. James Francis (ret.),  
Christian Schröder, Kenneth J. Withers (ed.)<sup>1</sup>

## I. Cross-Border Discovery in U.S. Litigation

In U.S. civil discovery, Federal Rule of Civil Procedure 34 (“Rule 34”) and its state court equivalents obligate parties to produce, upon request, non-privileged materials, including electronically stored information (ESI), that are within their “possession, custody, or control,” relevant to the claims or defenses in the action, and proportional to the needs of the case. The phrase, “possession, custody, or control” is subject to interpretation and defined differently by different courts.<sup>2</sup> Most courts hold that the “practical ability” to obtain the materials constitutes “possession, custody, or control.” Others hold that the “legal right” to obtain the materials must be present. The analysis become highly complex and fact-specific when the material is in digital form, perhaps stored in the cloud

---

<sup>1</sup> The editor wishes to thank his three contributors to this Annotated Bibliography. The text of this paper, and any errors contained therein, are entirely the editor’s responsibility, and the views expressed are those of the contributors and editor in their individual capacities, and do not reflect consensus views of The Sedona Conference, Working Group 6, or any other organizations with which the contributors and editor are associated.

<sup>2</sup> See generally, *The Sedona Conference Commentary on Rule 34 and Rule 45 “Possession, Custody, or Control”*, August 2016, [https://thesedonaconference.org/publication/Commentary\\_on\\_Rule\\_34\\_and\\_Rule\\_45\\_Possession\\_Custody\\_or\\_Control](https://thesedonaconference.org/publication/Commentary_on_Rule_34_and_Rule_45_Possession_Custody_or_Control).

or on servers world-wide, and perhaps subject to a variety of national data protection laws.

The analysis becomes more complicated when the legal relationship between the party in the U.S. litigation and the foreign custodians of potentially discoverable ESI is more attenuated, or when a data privacy, data protection, or so-called “blocking statute” prevents the legal transfer of the requested data to the U.S. for the purposes of litigation. In those instances, the court is often asked to order discovery either under Rule 34, which requires a finding that the responding party has “possession, custody, or control” over the materials located outside the country (putting the responding party in the awkward position of possibly violating the foreign nation’s laws if it complies with the U.S. court order), or proceeding under the often slow and cumbersome alternative discovery mechanisms, such as “letters rogatory” to the court in which the materials are located, or the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (the “Hague Convention”), if the foreign nation is a signatory.

To resolve this tension, most courts in the United States consider the following five factors, drawn from *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for the S. Dist. of Iowa*:<sup>3</sup>

1. the importance to the investigation or 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.

---

<sup>3</sup> 482 U.S. 522, 544 (1987).

These factors, referred to as the “*Aérospatiale*” test, were based on a draft Restatement (Third) of Foreign Relations Law § 442. In addition, many courts also consider:

6. the hardship of compliance on the party or witness from whom discovery is sought; and
7. the good faith of the party resisting discovery.<sup>4</sup>

The following is a selection of decisions from U.S. courts in the past two years addressing requests for discovery from sources outside the U.S. Most of these decisions involve request for ESI, but in some it is difficult to determine the medium involved. While there may be significant practical differences between the production of ESI and the production of hard-copy documents or physical evidence which may be reflected in the facts of each case or the specific statutory or regulatory considerations involved, the framework for analysis is essentially the same. These decisions are organized in chronological order, to allow the reader to see the progression of the jurisprudence over the past two years.

**Securities and Exchange Comm. (SEC) v. Telegram Group, Inc.**, No. 19 Civ. 9439 (S.D.N.Y. Jan. 13, 2020). The SEC filed an action against Telegram, alleging that the British Virgin Islands-based instant messaging service’s promotion of its cryptocurrency constituted an illegal securities offering. The SEC moved to compel Telegram to produce bank records relevant to its investigation. Telegram opposed, claiming that the disclosure of bank records without redaction of personal information would violate GDPR and that redaction would be unduly burdensome, “given the limited relevance of the information sought.” The court initially denied the SEC’s motion, but the SEC sought reconsideration, asserting that Telegram’s objections were vague and conclusory. The court reversed itself but granted Telegram several weeks to redact personal data, allowing Telegram to determine for itself the applicability

---

<sup>4</sup> *Wultz v. Bank of China Ltd.*, No. 11 Civ. 1266(SAS), 2013 WL 1832186, at \*3-4 (S.D.N.Y. May 1, 2013).

of GDPR to each record. The court also ordered Telegram to provide a log explaining the rationale for each redaction.

**Mercedes-Benz Emissions Litigation**, Civil Action No. 16-cv-881, 2020 WL 487288 (D.N.J. Jan. 30, 2020). The German-based defendant in this class action appealed a Special Master’s ruling ordering the production of employee names, titles, dates of employment, organizational charts, and other materials that implicated personal information protected by GDPR, with a protective order in place. The Magistrate Judge reviewed the Special Master’s ruling, applying an “abuse of discretion” standard, and concluded that the Special Master analyzed each of the five *Aérospatiale* factors correctly to determine that discovery of the requested data should proceed in unredacted form. In doing so, the court noted that the Special Master’s reliance on the existence of a protective order was not an attempt to circumvent GDPR but was an element in balancing the interest of the U.S. in litigating serious allegations of consumer fraud against the German state’s interest in protecting the privacy of its citizens. Finally, in a footnote, the court noted that the defendants failed to produce evidence that the disclosures in this litigation would trigger an enforcement action by any EU data protection authority.

**In re 3M Combat Arms Earplug Products Liability Litigation**, No. 3:19-md-2885, 2020 WL 5578428 (N.D. Fla. Feb. 18, 2020). In this products liability action, the plaintiffs sought discovery from a non-party, the French-German Research Institute of Saint-Louis (“ISL”), which held the patent on the product at issue. ISL objected first to the service of the subpoena via “FedEx International Priority” delivery. The court held that direct service by mail was allowed under the Hague Service Convention, unless the receiving state has objected to that method, which France has not. Secondly, ISL argued that the court lacked personal jurisdiction over the ISL and could not enforce a subpoena for discovery issued under Federal Rule of Civil Procedure 45. The court agreed that Rule 45 was not the appropriate discovery vehicle but went on to consider proceeding under the Hague Evidence Convention. Analyzing the *Aérospatiale* factors, the court summarily dismissed any reliance on the French

Blocking Statute. Instead, the court focused on the nature of the ISL, “an exceptional organization inextricably intertwined with the French government such that ISL's objectives may be indistinguishable from those of the French military. Indeed, France's Ministry of the Army objected to Plaintiffs' initial subpoena on the basis that ISL is charged with assisting France with its national defense and the documents requested would give access to a host of confidential scientific, technical, and financial information.” Consequently, the court concluded that the plaintiffs must attempt discovery through the Hague Convention rather than the Federal Rules of Civil Procedure.

**Behrens v. Arconic, Inc.**, No. 19-2664, 2020 WL 1250956 (E.D. Pa. March 13, 2020). In one of several decisions in the ongoing Grenville Tower fire litigation, the court received the appointed expert’s report on the effect of French law and the Hague Convention on discovery, and after a hearing and consideration, adopted the report and ordered that discovery proceed under the Hague Convention procedures, rather than the Federal Rules of Civil Procedure.

**Proofpoint, Inc. v. Vade Secure, Inc.**, No. 19-cv-04238, 2020 WL 1911195 (N.D. Cal. Apr. 20, 2020). In a trade secret misappropriation action, the court ordered that discovery proceed under the Federal Rules of Civil Procedure rather than the Hague Evidence Convention. The defendants moved for reconsideration, alleging that the Magistrate Judge’s procedures preventing it from submitting “dispositive facts and arguments” regarding French law prohibiting information originating in France from being used in a non-French proceeding. Accompanying their motion for reconsideration, the defendants submitted numerous opinions, declarations, and affidavits from French attorneys and legal experts regarding the French Blocking Statute. The court held a hearing and reviewed the submissions, which it described in detail in this opinion, noting that the submissions were inconsistent and contradictory on the question of whether, as a practical matter, the blocking statute operates to prohibit discovery in foreign courts. The court concluded that “[t]he blocking statute thus is relevant to the court's particularized comity analysis only to the extent that its terms and its enforcement identify the

nature of the sovereign interests in nondisclosure of specific kinds of material,” turning to the *Aérospatiale* comity analysis. Holding that the *Aérospatiale* factors “weigh overwhelmingly in favor of proceeding under the Federal Rules,” reconsideration of the original order was denied.

**Giorgi Global Holdings, Inc. v. Smulski**, No. 17-4416, 2020 WL 2571177 (E.D. Pa. May 21, 2020). One of these defendants in this RICO action, a Polish resident but a U.S. citizen, objected to producing documents in discovery, citing the prohibitions of the GDPR. Considering the *Aérospatiale* factors, the court ordered that discovery proceed, observing that “[i]t is true that Poland has an interest in protecting the personal data of its citizens, but the parties in this matter entered into a Protective Order and ESI Protocol that will protect the personal data of any Polish third parties.”

**Certain Vehicle Control Systems, Vehicles Containing the Same, and Components Thereof**, Inv. No. 337-TA-1235, 337-TA-1235 (ITC Feb. 16, 2021). Citing the United States’ national interest in enforcing its patents, an International Trade Commission Administrative Law Judge issued an order compelling the respondents in this patent action to produce documents without redactions that the respondents claimed were required under GDPR, allowing only redactions “such as an individual’s home addresses, home telephone numbers, business email addresses, and business phone numbers.”

**Ingenico Inc. v. Ioengine, LLC**, No. 18-826, 2021 WL 765757 (D. Del. Feb. 26, 2021). The plaintiffs in this case requested that the court issue letters rogatory under Article 1 of the Hague Evidence Convention to the Israeli courts, seeking documents and depositions of two Israeli residents. The court noted that it was bound under the *Aérospatiale* decision to “exercise special vigilance to protect foreign litigants from the danger that unnecessary, or unduly burdensome, discovery may place them in a disadvantageous position,” in addition to considering each element of the *Aérospatiale* five-factor comity analysis. The court denied the request, holding that the plaintiffs failed to advance more than conclusory assertions regarding the importance of the proposed discovery to the needs of the case, failed to articulate their requests with specificity, and

failed to establish the likely origin or location of the evidence sought. The request was denied “without prejudice to its renewal upon a sufficient presentation.”

**Arcelik A.S. v. E.I. DuPont de Nemours and Co.**, 856 Fed.Appx. 392 (3d Cir. May 20, 2021). The defendant in this manufacturing defect action obtained permission to pursue discovery under the Hague Convention from a non-party located in Germany and India. The non-party sought to have permission vacated, arguing that they violated international comity. The trial court denied the non-party motion and entered a protective order regarding any trade secrets that might be disclosed. The non-party appealed the denial of the motion to vacate to the Third Circuit. As an initial matter, the appellate court considered the trial court’s actions final as regards the non-party, and therefore appealable. The appellate court went on to review the trial court’s application of the *Aérospatiale* factors, finding no abuse of discretion, as the national interest in protecting trade secrets as addressed by the entry of the protective order.

**AnywhereCommerce, Inc. v. Ingenico, Inc.**, No. 19-cv-11457, 2021 WL 2256273 (D. Mass. June 3, 2021). The court entered an order in 2020 compelling the defendants to produce documents over the objections of defendants citing the restrictions of the GDPR, based on representations by the plaintiffs that the requested documents were mostly located in the U.S. and in the possession, custody, or control of U.S.-based defendants. The court later granted reconsideration upon learning that “contrary to Plaintiffs’ previous representations of where the relevant information was located, ‘the key decisionmakers ... and the important documents and evidence relevant to Plaintiffs’ claims are in France.’” In the view of the court, this implicated a significant factor in the *Aérospatiale* analysis, the origin or location of the requested documents. However, the adoption of a protective order in the case, while not an explicit *Aérospatiale* factor, neutralizes the origin or location factor, stating, “far from ignoring the protections of the GDPR, the court’s Order ensures that the protections provided by the GDPR are maintained throughout and following this proceeding.”



**Jaguar Land Rover Limited v. DR. ING. H.C. F. Porsche AG**, No. 21-mc-62, 2021 WL 3075698 (D.C.D.C. June 22, 2021). Parties in a patent infringement action before the International Trade Commission (ITC) petitioned the District Court to issue letters rogatory under the Hague Evidence Convention to obtain discovery from a non-party German company. The request was unopposed and recommended by the ITC administrative law judge. The court noted that even when proceeding unopposed under the Hague Convention, it still must engage in a comity analysis, applying the *Aérospatiale* factors. The court found in favor of the petitioners on all but the final factor, whether the request would undermine important interests of the state where the information is located, stating that when proceeding under the Hague Convention, that factor is to be decided by the court in that state.

**Doubleline Capital LP v. Odebrecht Finance, Ltd.**, No. 17-CV-4576, 2021 WL 4596561 (S.D.N.Y. Sept. 23, 2021). In this long-running international bribery litigation, the court had previously ordered discovery of Brazilian defendants. The parties then filed cross motions for a protective order and to compel discovery. The defendants had been tried in a Brazilian criminal court in which they entered a Leniency Agreement, the details of which had been sealed by the court. The U.S. court granted the defendants' motion for a protective order prohibiting discovery of the sealed documents on the basis of a detailed comity analysis.

**In re Zantac (Ranitidine) Product Liability Litigation**, No. 20-MD-2924, 2021 WL 5105028 (S.D. Fla. Oct. 27, 2021). The defendants in this pharmaceutical products liability class action moved for the issuance of letters rogatory, seeking discovery from a Canadian research scientist. The plaintiffs opposed the motion on proportionality grounds. The parties met and conferred, as required by the rules, and in their report indicated to the court that the nonparty scientist and a Canadian laboratory with which he was associated objected to the discovery request. The court held that the permissible scope of letters rogatory is the same as that allowed for any other discovery device under Federal Rule of Civil Procedure 26(b)(1), and the requests would be directed to scientist in his individual capacity and limited to documents within his possession, custody, or

control. Since the Canadian laboratory did not assert any privilege over the scientist's documents, it had no standing to challenge the request. The court went on to address the plaintiffs' proportionality objection and comity considerations, observing that the court is required pursuant to the *Aerospatiale* factors to limit the scope of any request that is "(1) unreasonably cumulative, (2) can be obtained from a more convenient, less expensive, or less burdensome source, or (3) is outside the scope of Rule 26(b)(1)." The court found that the request was proportional to the needs of the case and no countervailing national interest of Canada had been identified. The court granted the motion but limited the temporal scope of the request.

**In Re Valsartan, Losartan, and Irbesartan Products Liability Litigation**, MDL No. 2875, 2021 WL 6010575 (D.N.J. Dec. 20, 2021). In this pharmaceutical products liability class action, the Special Master closely analyzed several documents that a party objected to producing, citing the Chinese State Secrets Act. The Special Master ordered, and the court approved, the production of 20 documents that the defendants withheld, while denying discovery of three documents found likely to contain protected state secrets.

## II. U.S. Discovery to Assist Non-U.S. Tribunals

In recent years there has been a significant increase in applications by individuals and organizations outside of the U.S. for discovery from sources in the U.S. to assist in proceedings before "foreign tribunals." There may be several reasons for this trend. International trade and commerce have continued to increase, despite the recent pandemic and restrictions on physical travel. Digital commerce, in particular, has grown exponentially, in part because of the growing adoption of global computer systems supported by cloud computing and in part because of the restrictions on physical travel. It is also suggested by commentators—without substantive evidence—that stronger data privacy and protection laws outside of the U.S. has made broad U.S. discovery more attractive. Finally, it is undeniable that many of the most popular social media and

cloud computing platforms are based in the United States, making them the logical targets of discovery requests, even in cases in which they are not a party.

In U.S. federal courts, such requests are governed by 28 U.S.C. §1782, which requires a court to make three findings:

- The applicant is an "interested person" in a foreign proceeding
- The proceeding is before a foreign "tribunal," and
- The person from whom evidence is sought is in the district of the court before which the application has been filed.

In addition, courts have applied discretionary factors, following the U.S. Supreme Court's decision in *Intel Corp. v. Advanced Micro Devices*:<sup>5</sup>

- whether the person from whom discovery is sought is participating in the foreign proceeding
- the nature of the foreign tribunal and its receptiveness to U.S. judicial assistance
- whether the request conceals an attempt to circumvent foreign proof-gathering restrictions, and
- whether the request is unduly intrusive or burdensome.<sup>6</sup>

As in Part I above, the following decisions are arranged in chronological order to allow the reader to see the progression of the jurisprudence over the past two years.

**In re Application of Top Matrix Holdings Ltd.**, 18 Misc. 465, 2020 WL 248716 (S.D.N.Y. Jan. 16, 2020). The applicant alleged that Credit Suisse failed to detect and prevent fraud committed by one of its employees, resulting in hundreds of millions of dollars in losses, for which it intends to sue the bank. It requested discovery of several U.S.-based Credit Suisse entities. The bank opposed the application as onerous and better suited for adjudication in Swiss courts. The court granted the application

---

<sup>5</sup> 542 U.S. 241 (2004).

<sup>6</sup> *Id.* at 264-65.

in part, considering the *Intel* factors to determine that the proposed discovery would not circumvent Swiss law, but narrowed the scope of the requests, directing the parties to meet, confer, and submit a revised request.

**In re Application of Iraq Telecom Limited**, 18 Misc. 458, 2020 WL 1876301 (S.D.N.Y. Apr. 15, 2020). Court refused to issue an emergency stay of an order for discovery filed by an intervenor who claimed that the Lebanese Banking Secrecy Law substantially limited what information could be produced, and that discovery had already started although the intervenor's opposition to the discovery order was under appeal. The court stated that stay of an interlocutory discovery order requires heightened showing of success on appeal, and that the Magistrate Judge's interpretation of Lebanese law was not erroneous, even under de novo review standards, as the Lebanese law did not apply extraterritorially to the U.S.-based respondent.

**In re Apple Retail UK Limited**, 20-mc-80109, 2020 WL 3833392 (N.D. Cal. July 8, 2020). In a UK patent dispute, a party was granted discovery of a nonparty U.S. firm's relevant patent and license portfolio to establish "fair, reasonable, and non-discriminatory" license terms. Although the application was unopposed, court granted discovery without prejudice to any later motions to quash or modify.

**deLeon v. Clorox Company**, No. 19-mc-80296, 2020 WL 6381351 (N.D. Cal. Oct. 30, 2020). The petitioner, a U.S. citizen and widow of Saudi citizen, was granted her application for discovery in aid of litigation in Saudi Arabia to determine the distribution of her late husband's estate.

**In re National Bank Trust**, 20-mc-85, 2021 WL 118531 (D. Conn. Jan. 13, 2021). The court granted an application for discovery in aid of an action to enforce an estimated \$900 million judgment entered by a UK court against a Russian defendant. The defendant claimed to have little or no cash assets but is alleged to have amassed a gun collection worth nearly \$4 million in the U.S. The court ordered discovery of a Connecticut-based gun dealer and related financial institutions.

**In re Application of Daniel Snyder**, No. 20-mc-00199, 2021 WL 848193 (D. Colo. Mar. 5, 2021). The principal owner of the Washington Football Team initiated a defamation action in India and was granted discovery in the U.S. in aid of that action by a federal court in an *ex parte* proceeding. The instant action was initiated by the respondents, claiming that the resulting subpoenas were overbroad and designed to harass the suspected sources of unrelated unfavorable news reports regarding the team. The court agreed and narrowed the scope of the discovery significantly.

**Snowflake Inc. v. Yeti Data, Inc.**, No. 20-mc-80190, 2021 WL 1056550 (N.D. Cal. Mar. 18, 2021). In aid of a trademark infringement action filed in German court, Snowflake obtained an order allowing discovery of Yeti from a U.S. court, but the court ordered the parties to meet and confer regarding the scope of the discovery request. Yeti failed to produce requested documents and moved to have the order vacated, which was denied by the Magistrate Judge. On appeal to the District Judge, Yeti *inter alia* took the position that any discovery in the U.S. must adhere to German discovery rules, which was rejected by the court. The court went on to affirm the original discovery order and sanction Yeti for non-compliance that was not substantially justified, imposing a fine of \$10,000 per day plus attorneys' fees.

**Fund for Protection of Investor Rights in Foreign States v. AlixPartners, LLP**, 5 F.4th 216 (5th Cir. July 15, 2021). The Russian assignee of funds of bankrupt bank sought discovery of a U.S. entity in aid of arbitration conducted under a Lithuanian/Russian investment treaty. The circuit court upheld District Court's grant of application. Certiorari to the Supreme Court was granted on December 10, 2021.

**In re Tovmasyan**, No. 21-353, 2021 WL 3737184 (D.P.R. Aug. 20, 2021). A group of investors alleging to have been victims of a fraudulent investment scheme planned to initiate an action in the UK courts and sought discovery of a managing director of the scheme, resident in Puerto Rico, who was not anticipated to be a party to the UK action. Analyzing the statutory requirements and the *Intel* factors in detail, the court granted the application.

**In re Republic of The Gambia**, No. 20-mc-36, 2021 WL 4304851 (D.C.D.C. Sept. 22, 2021). The Gambia filed action in International Court of Justice against Myanmar alleging attempted genocide of Myanmar's Rohingya minority. The Gambia sought discovery of Facebook's internal investigation into the Myanmar government's and individual's use of the platform to organize and execute genocidal activities. The court granted The Gambia's application for discovery, finding that Facebook was not prevented by the Stored Communications Act from producing the report, including the content of messages from "de-platformed" accounts.

**In re Application of JSC Commercial Bank Privatbank**, No. 21-mc-80216, 2021 WL 4355334 (N.D. Cal. Sept. 24, 2021). The court granted a bank's application for discovery in aid of litigation in the UK to recover approximately \$1.9 billion allegedly misappropriated by Russian administrators, who claimed they could not access their Google email accounts and had provided written consent to Google for disclosure.

**In re Application of Hattori**, No. 21-mc-80236, 2021 WL 4804375 (N.D. Cal. Oct. 14, 2021). The court granted the application of a Japanese citizen for discovery in aid of prospective civil and criminal actions sounding in "reputation tort" through the posting of allegedly defamatory reviews on Google. Under Japanese law, the applicant is required to provide the identity of the alleged perpetrator before filing a civil action or criminal complaint.

**In re Application of Yuzo Takai**, No. 21-mc-80245, 2021 WL 5205583 (N.D. Cal. Nov. 9, 2021). In an application similar to that of Hattori, decided in the same court the previous month, a Japanese dental practice sought discovery of Google in aid of prospective civil and criminal actions, alleging that an unknown Google account holder was changing the name of the applicant's practice and the description of services on Google, resulting in significant loss of business. The court granted the application. The decision includes major portions of the proposed subpoena language to demonstrate its narrowness and specificity.

**IS Prime Limited v. Glassdoor, Inc.**, No. 21-mc-80178, 2021 WL 5889373 (N.D. Cal. Dec. 13, 2021). IS Prime filed an action in UK courts in a

contract dispute over the provision of foreign exchange services to a brokerage. IS Prime alleged that a senior officer of the defendant in that suit proceeded to launch a smear campaign against IS Prime in social media, resulting in a parallel suit for defamation. In this application, IS Prime sought discovery of a U.S.-based social media platform, Glassdoor, on which two of the allegedly defamatory statements were posted, to confirm the source of the postings. The court granted the application, with the proviso that Glassdoor provide copies of the subpoena to the individuals who posted the messages, with 30 days to file any objections.

**In re Application of Credit Suisse Voirtuoso**, No. 21-mc-80308 (N.D. Cal. Jan 4, 2022). In a one-page decision, the court granted a Swiss investment bank discovery in aid of anticipated litigation in UK to recover funds allegedly owed from failed venture, without prejudice to any later motions to quash or modify.

### **III. Non-U.S. Data Privacy and Security Investigations and Enforcement Actions**

For several months after the General Protection Data Regulation (GDPR) went into effect on May 25, 2018, European Data Protection Authorities (DPAs) concentrated on education and consultation to obtain compliance with the new law. In the past two years, however, DPAs have evidenced a willingness to impose more significant sanctions for violations of the law, ranging from relatively small “immaterial damage” awards to individual complainants for technical data privacy violations to significant multi-million-euro fines for egregious violations with widespread public impact.

The seriousness with which DPAs are enforcing the law against their own citizens and those of fellow European countries undercuts the argument, often heard in U.S. courts, that these laws are simply protectionist trade barriers or “blocking statutes,” concerned mainly with frustrating foreign businesses and courts. This may alter the conventional balance of considerations in the U.S. under the *Aérospatiale* factors to give more weight to the data host country’s interests in protecting data from

disclosure or production outside of the country or for purposes other than those for which it was originally collected with the data subject's consent.

### **A. Enforcement Actions Against EU- and EEC-based Entities**

Among recent enforcement actions involving European entities, an Italian university was fined €200,000 for a variety of GDPR violations, including a lack of a legal basis for data collection (invalid consent) and the retention of personal data for a period longer than necessary, but also for using a service to monitor students during remote exams that relied on the Privacy Shield for data transfers to the U.S.<sup>7</sup>

A Norwegian toll company was fined €496,000 for a variety of GDPR violations by transferring large amounts of personal data to a processor in China. The company had not conducted a risk assessment prior to the transfer, and it had not concluded a proper data processing agreement with the processor. However, no actual damages were proven, which had a mitigating effect on the amount of the fine.<sup>8</sup>

A fine of €8,150,000 was imposed by Spanish authorities on Vodafone España S.A.U., against which 162 complaints were lodged over a two-year period involving a variety of unlawful marketing tactics, including cold calling, ignoring data subjects' objections, and ignoring entries on a "Robinson" direct marketing opt-out list. As part of this fine, €2 million were imposed just for the breach of GDPR Art. 44.<sup>9</sup>

A €225 million fine was levied against WhatsApp Ireland, Ltd. for breaches of GDPR Art. 5(1)(a) (transparency) and Art. 12, 13, and 14, after WhatsApp announced that it would revise its terms of service to allow data sharing with parent company Facebook. In imposing the fine, the European Data Protection Board (EDPB) resolved a dispute between the Irish DPC and objecting DPAs of other Member States over the amount of the fine, which Irish authorities originally set at €50 million.

---

<sup>7</sup> Garante, 16 September 2021.

<sup>8</sup> Datatilsynet, 27 September 2021.

<sup>9</sup> AEPD, 11 March 2021.



The EDPB also clarified that in calculating an appropriate fine, a parent company's consolidated turnover is relevant.<sup>10</sup>

The Administrative Court Wiesbaden decided that a university may not rely on the "Cookiebot" consent management tool since it lacks a sufficient transfer mechanism. The transfer, the court held, was in violation of GDPR Art. 48 and 49. Since the service provider employed by Cookiebot has its headquarters in the U.S., the court found the CLOUD Act to be applicable. As no decision based on an international agreement under Art. 48 was existent, the court examined Art. 49 derogations, but found that none of these exceptions applied. Therefore, the court took the view that the transfer of the cookie data (IP address, cookie keys, device data, etc.) was unlawful. The court did not decide on the efficacy of any Standard Contractual Clause (SCC) since no SCCs were proven to have been signed by the parties.<sup>11</sup>

In what may be the clearest example of the seriousness with which European data protection authorities enforce data privacy and protection regulation within the EU, the European Data Protection Supervisor (EDPS) reprimanded the European Parliament itself for using Google Analytics and the payment provider Stripe, both of which U.S.-based companies, on its COVID-19 test booking website. The reprimand follows several complaints by members of Parliament and the privacy campaign group *noyb*. The transfers to the U.S. were held to be in violation of the *Schrems II* judgment, since the Parliament provided no documentation, evidence, or other information regarding the contractual, technical, or organizational measures in place to ensure an essentially equivalent level of protection over the personal data transferred to the U.S. in the context of the use of cookies on its COVID testing website.<sup>12</sup>

On the other hand, the Conseil d'Etat — France's highest administrative court — ruled that personal data on a platform used to book COVID-19 vaccinations, managed by Doctolib and hosted by Amazon Web Services, was sufficiently protected under GDPR because sufficient safeguards,

---

<sup>10</sup> Legaltech News, 2 Sept. 2021.

<sup>11</sup> Administrative Court Wiesbaden Decision of 1 December 2021, 6 L 738/21.WI.

<sup>12</sup> EDPS, Case 2020-1013, 5 January 2022.

both legal and technical, were put in place in case of an access request from U.S. authorities.<sup>13</sup>

### **B. Actions Against U.S.-based Entities**

The authors of this paper found no reported decision during 2020-21 by a tribunal outside of the U.S. that squarely addressed a request for discovery in U.S. civil litigation. However, there were several decisions that implicated the transfer of data to the U.S. (or to U.S.-based entities) for other purposes.

At the end of 2020, French regulators fined Google €100 million and Amazon €35 million for placing advertising cookies on users' computers without obtaining prior consent or providing adequate information.<sup>14</sup>

That same month, Irish regulators imposed their first fine on a U.S.-based company, levying a €450,000 fine against Twitter for failing to timely report a data breach or adequately document it. The amount of the fine, which was initially much lower, was determined after consultation with other EU data protection authorities, pursuant to GDPR's dispute resolution system, which requires that the lead national regulator in a cross-border online privacy case must consult with the EU's other national privacy regulators.<sup>15</sup>

The British data protection authority, the Information Commissioner's Office (ICO), announced in November 2021 that in conjunction with Office of the Australian Information Commissioner (OAIC), it intends to fine a U.S.-based facial recognition company, Clearview, £17 million, in addition to issuing a cease-and-desist order, for collecting facial images of British and Australian consumers without their knowledge or consent.<sup>16</sup>

A probe of Amazon's data management practices initiated in 2018 by the French privacy rights group La Quadrature du Net resulted in the largest fine levied to date by any European DPA. On July 16, 2021,

---

<sup>13</sup> IAPP, 15 March 2021.

<sup>14</sup> Legaltech News, 11 December 2020.

<sup>15</sup> Legaltech News, 15 December 2020.

<sup>16</sup> Biometrics News, 30 November 2021.

Luxembourg's CNPD found that Amazon's processing of personal data did not comply with GDPR rules and imposed a fine of €746 million in addition to ordering "practice revisions."<sup>17</sup>

During 2021, the power of European DPAs to investigate overseas entities and enforce GDPR regulation was confirmed in two opinions. In January, Court of Justice for the European Union (CJEU) Advocate General Michal Bobek issued an opinion that any EU country can take legal action against companies over violations of data privacy rules—not just the main regulator in charge of the company. The opinion was issued in an action by the Belgian DPA against Facebook, which is headquartered in Ireland for GDPR oversight purposes, over allegations that Facebook placed cookies on the users' devices without their consent.<sup>18</sup> Later in December, CJEU Advocate General Richard de la Tour opined that Facebook could be sued by consumer groups for privacy violations in a German online gaming case. The Advocate General is quoted as saying "[m]ember states may allow consumer protection associations to bring representative actions against infringements of the protection of personal data." While civil procedure rules differ from country to country, this has been interpreted by commentators as opening the door to U.S.-style class actions, in addition to regulatory enforcement by DPAs.<sup>19</sup>

### C. "Immaterial Damages"

During 2021, there was debate regarding the concept of "immaterial" or "nonmaterial" damages for technical violation or violations that affect only an individual or small number of claimants, without evidence significant monetary damages or injury. In June of 2021, the Austrian Supreme Court formally requested the Court of Justice of the European Union (CJEU) to give a preliminary ruling on immaterial damages.<sup>20</sup> The German Supreme Labor Court has also requested the CJEU to give a

---

<sup>17</sup> Amazon.com, Inc., Form 10-Q for Period Ended June 30, 2021, <https://www.sec.gov/ix?doc=/Archives/edgar/data/1018724/000101872421000020/amzn-20210630.htm>.

<sup>18</sup> Legaltech News, 14 January 2021.

<sup>19</sup> Reuters, 2 December 2021.

<sup>20</sup> Austrian Supreme Court, 6 Ob 56/21k, June 2021.

preliminary ruling on immaterial damages. That court holds the view that (i) any violation of Art. 15 GDPR or the GDPR in general automatically leads to damage claims, (ii) compensation amounts must be dissuasive and (iii) data subjects do not need to prove that they have suffered immaterial damages;<sup>21</sup>

Some local, regional and labor courts in Germany have granted immaterial damages ranging from approximately €300 to approximately €5,000, arguing that the notion of "immaterial damages" must be interpreted broadly so that data subjects receive the "full and effective" compensation allowed under Recital 146.

During 2020, the Düsseldorf Local Labor Court awarded a claimant €5,000 for a two month-delay in responding to a data subject request and for providing an incomplete response.<sup>22</sup> The Darmstadt Regional Court awarded a claimant €1,000 for sending applicant data to the wrong recipient.<sup>23</sup> The Higher Regional Labor Court Cologne entered a judgment for €300 to a former employee of a firm that allowed their CV to remain accessible online.<sup>24</sup> And the Lüneburg Regional Court awarded a consumer €1,000 for a negative entry by a credit agency.<sup>25</sup>

Continuing into 2021, the Hamm Regional Labour Court awarded a claimant €1,000 for a five-month delay in responding to a data subject request and for an incomplete response.<sup>26</sup>

Perhaps most significantly, the Munich Regional Court awarded €2,500 in non-material damages to a data subject affected by a data breach at Scalable Capital, an online asset management company. The breach occurred due to a security vulnerability and lead to the leak of 33,000 user data records to third parties, with addresses and personally identifiable data, as well as tax and securities account information. The data subject complainant was also awarded compensation for material damages that had occurred and are likely to occur in the future. The

---

<sup>21</sup> 8 AZR 254/20 (A), August 2021.

<sup>22</sup> March 2020, 9 Ca 6557/18.

<sup>23</sup> May 2020, 13 O 244/19.

<sup>24</sup> September 2020, 2 Sa 358/20.

<sup>25</sup> July 2020, 9 O 145/19

<sup>26</sup> May 2021, 6 Sa 1260/20.

claimant was supported by the EuGD, the European Society for Data Protection.<sup>27</sup>

On the other hand, some local, regional, higher regional, and labour courts have denied claims, referring to a "*de minimis* threshold". Examples include the Higher Regional Court Dresden rejecting a claim concerning a 30-day blocking of a social media account;<sup>28</sup> the Regional Court Karlsruhe rejecting a claim concerning the dissemination of name, address, gender, e-mail address or a data subject;<sup>29</sup> and the Local Court Frankfurt holding that there were no damages for merely "perceived impairment".<sup>30</sup>

#### **D. Limitations on Extraterritorial Investigative Powers**

**R (on the application of KBR, Inc) (Appellant) v Director of the Serious Fraud Office (Respondent)** [2021] UKSC 2. KBR is a U.S.-based business in the aerospace, defense, energy, chemicals, intel and data science markets. Following media reports alleging bribery and corruption in the oil industry, centered on Monaco-based Unaoil, securities regulators in the U.S. and UK initiated investigations that implicated KBR in the U.S. and subsidiary KBR UK in the UK. The Serious Fraud Office (SFO) in the UK issued a "notice" – effectively a subpoena, with potential criminal penalties for noncompliance – to KBR UK. KBR UK responded by producing various responsive material, but claimed it did not have "possession, custody, or control" over responsive material held by KBR in the U.S. The SFO then issued a second notice directly to KBR, which moved to quash the notice as it called for production of materials from extra-territorial sources by a foreign entity. The UK Supreme Court ruled for KBR, holding that notices issued by the SFO cannot be validly served on a foreign company that has no fixed place of business in the UK, has never carried on business in the UK, nor has a registered office or other presence in the UK.

---

<sup>27</sup> eugd.org, 21 December 2021.

<sup>28</sup> August 2020, 4 U 784/20.

<sup>29</sup> February 2021, 4 O 67/20.

<sup>30</sup> July 2020, 385 C 155/19.