



Selected Court and Regulatory Cross-Border
Discovery and Data Protection Actions
2018 – May 31, 2019

Kenneth J. Withers, editor

[Updated June 9, 2019]

Preface

Students of social, legal, and technological history will look back at 2018 as a watershed year for privacy and data protection. This was the year that the General Data Protection Regulation (GDPR) went into effect in the European Union (EU) and the California Consumer Privacy Act was passed in the United States (U.S.). 2018 also witnessed a parade of high-tech entrepreneurs justifying their data collection and processing practices before regulatory agencies and legislators, related in part to continued fallout from the Cambridge Analytical scandal of the previous year. We were even treated to the unusual spectacle of a U.S. tech executive, while on a business trip in London, being escorted by the U.K. Parliament's Serjeant at Arms to face a Parliamentary inquiry, where his documents related to a California lawsuit against Facebook were seized, even though the documents were subject to a sealing order by the California court.¹

This paper presents a high-level overview of developments in privacy and data protection law during 2018 and the first half of 2019, concentrating on regulatory enforcement actions and court decisions affecting—directly or indirectly—the processing and transfer of protected data across international borders to meet legal disclosure and discovery obligations. Part I reports actions by courts and regulators outside of the U.S. to enforce their privacy and data protection laws, with a primary focus on enforcement of GDPR. Part II reports a small number of actions in which U.S. litigants sought the aid of non-U.S. courts to obtain discovery. Part III reports U.S. court decisions addressing discovery requests for data from outside the U.S. Part IV discusses the apparently growing trend for non-U.S. parties to seek discovery in the U.S. in aid of litigation in other countries. Part V highlights the tension between the tradition in the U.S. of public access to court files and proceedings, and the privacy expectations of EU citizens who find themselves in U.S. courts. Finally, the Appendix addresses enforcement of privacy and data protection laws in general in the Asia-Pacific region.

No one person can effectively keep up with these developments worldwide, and the Editor is grateful to the many volunteers who have spotted court decisions, regulatory actions, legislative proposals, agency press releases, and news articles related to these issues. In particular, the Editor thanks Natascha Gerlach and Elizabeth Macher of Cleary Gottlieb Steen & Hamilton LLP; Jeane A. Thomas of Crowell & Moring LLP; Philip Favro of Driven, Inc.; Denise E. Backhouse and Gretchen N. Marty of Littler Mendelson P.C; and David Kessler of Norton Rose Fulbright US LLP, for their contributions to this collection. Special thanks go to California attorney William E. Hoffman for his invaluable editing assistance and to Cathy Choi and Natascha Gerlach for their work creating the Appendix. However, the analysis and opinions expressed herein, unless otherwise attributed, are entirely those of the Editor, and do not necessarily reflect the views of the many valued contributors or their respective organizations.

¹ “Parliament seizes cache of Facebook internal papers,” *The Guardian*, November 24, 2018, at <https://www.theguardian.com/technology/2018/nov/24/mps-seize-cache-facebook-internal-papers>.

I. Enforcement of privacy and data protection laws outside the United States

The implementation of GDPR in Europe is clear evidence of the depth of concern EU citizens and their governments have for protecting personal privacy, in line with many other nations around the world. The broad scope of GDPR has data controllers and processors scrambling to comply with the new regulations. Sedona Conference Working Group 6 members in Europe report that since May 25, 2018, when GDPR went into effect, Data Protection Authorities (DPAs) have been flooded with routine questions and data breach notifications, as entities opt for a “better safe than sorry” approach to compliance and reporting.

In the lead-up to May 25, 2018, it was common for data controllers and processors to focus on the possibility of heavy fines for GDPR violations—up to 4% of a company’s global turnover. DPAs attempted to quell those fears by placing emphasis on education and day-to-day compliance activities, reserving the threat of multi-million Euro fines for only the most egregious cases. However, the specter of significant monetary penalties for non-compliance remains, reinforced by several penalty notices throughout 2018, stemming from investigations initiated prior to the effective date of GDPR.

Since GDPR went into effect last year, the contributors to this article have identified 75 enforcement actions by various Data Protection Authorities resulting in fines. The total in fines imposed, as of this writing, is €449,000, with the average fine amounting to €6,000. The highest fine so far, €80,000, was imposed by the data protection authority of Baden-Wurttemberg in Germany, in a case in which a data controller had published health data online which inadvertently included personal data due to a lack of internal controls. The controller cooperated with the authorities and invested sums far exceeding the fine to remedy its internal data protection shortcomings. Coming in second was the Berlin data protection authority, imposing a €50,000 fine against a bank which had continued to process data of former clients. Baden-Wurttemberg also took third place in this list, with a €20,000 fine imposed on the social network Knuddels for a data leak leading to the unencrypted exposure of personal data of almost two million users. That fine has been regarded as moderate in relation to the scope of the incident; Knuddels cooperated fully with the authorities and implemented the authority’s instructions and recommendation immediately.

The imposition of fines for violations of privacy and data protection laws is not new, of course. The first half of 2018 saw several significant fines levied by data protection authorities under pre-GDPR laws, and many enforcement actions commenced before May 25, 2018 are ongoing. Perhaps the most high-profile court activity on privacy and data protection in Europe are the *Schrems* cases, in which Austrian privacy campaigner Max Schrems challenged Facebook’s data collection, processing, and transfer policies, and in the process, upended previously-accepted mechanisms for the routine transfer of data

across borders. The actions have their roots in a 2013 complaint against Facebook, whose European operations are based in Ireland. Schrems alleged that his data was being transferred by Facebook Ireland to Facebook, Inc. in the United States, where it was not protected by robust privacy laws and potentially subject to unauthorized access by the U.S. government, under the covert surveillance programs disclosed by Edward Snowden. Ultimately the initial case went to the Court of Justice of the European Union (CJEU), which determined that the framework for data transfer to the U.S. utilized by Facebook (and hundreds of other entities at the time), called “Safe Harbor,” no longer adequately protected EU citizens, and was invalid.² Schrems amended and resubmitted his complaint in Ireland, as Facebook was continuing to transfer data, but under a different well-established framework, Standard Contractual Clauses (SCCs). Irish regulators and courts were not satisfied that this cured the underlying deficiencies in data protection. Facebook appealed the Irish High Court’s reference of the case to the Irish Supreme Court, which rejected that appeal on May 31, 2019.³ Meanwhile, the High Court’s reference remains valid and is pending before the CJEU.⁴

We have far fewer examples of court enforcement, as GDPR and other recently-adopted national privacy laws have yet to generate more than a handful of court proceedings. But during this period, courts and data protection authorities outside the U.S. demonstrated have that they take these issues very seriously.

Selected Court Opinions and Regulatory Actions⁵

Centro Hospitalar Barreiro Montijo, Comissão Nacional de Protecção de Dados (Oct. 22, 2018). A major Lisbon-based hospital was fined €400,000 by the Portuguese Data Protection Authority for three categories of violations of GDPR: Violation of Article 5(1)(c) by allowing indiscriminate access to an excessive number of users; violations of Article 5(1)(f) and Article 83(5)(a) by failing to institute reasonable technical and organizational measures to prevent unlawful access to personal data; and violation of Article 32(1)(b) by failing to institute technical and organizational measures more generally

² After many months of negotiation, Safe Harbor was replaced with a new framework for data transfers between the EU and U.S., “Privacy Shield.” While critics contended that none of the underlying concerns had been resolved, nevertheless Privacy Shield was endorsed by the European Commission in July 2016, subject to an annual evaluation. The second annual review was released on December 19, 2018, which found that the framework was adequate overall, but made ten recommendations for improvement, the most significant being that the U.S. needs to fill the vacant “Ombudsman” enforcement position in the Department of Commerce. European Commission, *Report from the Commission to the European Parliament and the Council*, Brussels, 19.12.2018 COM(2018) 860 final, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en#privacyshieldannualreview.

³ Padraic Halpin, “Irish Supreme Court rejects Facebook bid to block ECJ data case,” Reuters, May 31, 2019, <https://www.reuters.com/article/us-europe-privacy-ireland/irish-supreme-court-rejects-facebook-bid-to-block-ecj-data-case-idUSKCN1T112I>.

⁴ See generally, Data Protection Commissioner (Ireland), Final Report, 1 January – 24 May 2018, https://www.dataprotection.ie/sites/default/files/uploads/2018-11/DPC%20annual%20Report%202018_0.pdf.

⁵ The editor apologizes to readers for the informal and idiosyncratic citation styles of the following case summaries, but many of these court and administrative decisions fall outside the scope of conventional legal scholarship. Wherever possible, a link to a primary source or reliable news account is provided in the footnotes.

to ensure a level of security adequate to the risk, including a process to regularly testing, assessing and evaluating the technical and organizational measures to ensure the security of the processing. While the total fine was significant, it fell well short of the maximum fine authorized by law.⁶

Bisnode, Polish Personal Data Protection Office (“UODO”), Mar. 15, 2019. A Swedish-based digital marketing firm was fined €220,000 for failing to comply with Article 14 data subject notification requirements. It was also ordered to notify approximately six million data subjects, at an estimated cost of €8 million, or delete the records. The ruling is viewed as a strict application of Article 14 of GDPR and a *de facto* ban on “data scraping” techniques.⁷

Carphone Warehouse Ltd Monetary Penalty Notice, U.K. Information Commissioner’s Office, Jan. 6, 2018. Mobile phone retailer Carphone was fined £400,000 for violation of Data Protection Principle 7 of the Data Protection Act of 1998, which requires “[a]ppropriate technical and organization measures” to protect against unauthorized process, destruction, or loss of personal data.⁸

Equifax Ltd Monetary Penalty Notice, U.K. Information Commissioner’s Office, Sept. 19, 2018. Credit reporting agency Equifax was fined £500,000 for violation of Data Protection Principle 7, and also for the unauthorized and unnecessary transfer of data to the U.S.⁹

Facebook Ireland Ltd Monetary Penalty Notice, U.K. Information Commissioner’s Office, Oct. 24, 2018. Social media giant Facebook was fined £500,000 for violation of Data Protection Principle 1, which prohibits the intentional “unfair” processing of personal data, as well as for violation of Principle 7, in relation to the Cambridge Analytical incident. The Irish Data Protection Commission announced in early October 2018 that it was launching a full-scale investigation of the extensive data breach Facebook reported in September, an entirely separate incident involving approximately 50 million Facebook users, an unknown percentage of whom may be EU citizens.¹⁰

Facebook, Higher Administrative Court of Hamburg, Mar. 1, 2018. An appellate court in Hamburg confirmed a lower court's ruling that Facebook must cease collecting and storing data on users of its German WhatsApp subsidiary, because the company may be violating

⁶ Dr. Ana Menezes Monteiro, “First GDPR fine in Portugal issued against hospital for three violations,” IAPP, Jan. 3, 2019, <https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/>.

⁷ Natasha Lomas, “Covert data-scraping on watch as EU DPA lays down ‘radical’ GDPR red-line,” TechCrunch, Mar. 30, 2019, <https://techcrunch.com/2019/03/30/covert-data-scraping-on-watch-as-eu-dpa-lays-down-radical-gdpr-red-line/>.

⁸ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/01/carphone-warehouse-fined-400-000-after-serious-failures-placed-customer-and-employee-data-at-risk/>.

⁹ <https://ico.org.uk/media/action-weve-taken/mpns/2259808/equifax-ltd-mpn-20180919.pdf>.

¹⁰ <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf>.

the German Federal Data Protection Act (BDSG), even though data collection and storage practices are disclosed in its terms and conditions.¹¹

Facebook, Brazil Superior Court of Justice, Feb. 19, 2018. Brazil's Superior Court of Justice upheld a \$33 million fine levied against the Brazilian unit of Facebook by a federal court in the state of São Paulo. Law enforcement sought WhatsApp messages of Facebook users suspected of unlawfully importing and selling prescription drugs. Facebook Inc. failed to persuade the court to rescind its fines for refusing to turn over information stored outside the country.¹²

Facebook, Court of Appeals of Brussels – 18N – 2018/AR/410, May 8, 2019. Facebook was convicted by the Court of First Instance in Brussels of non-compliance with Belgian privacy and cookie rules, imposing a fine of €250,000 per day, up to €100 million, for continued non-compliance. Facebook appealed, stating that the Belgian court has no jurisdiction, as its “national supervisory authority” is Ireland. The Court of Appeals certified several questions to the Court of Justice of the European Union (CJEU) that go to the efficacy of GDPR's “one stop shop” provisions for supervision and enforcement actions, including:

- Does the right of a national supervisory authority to commence legal proceedings regarding infringements of the GDPR in its Member State (art. 58.5) not apply in case of cross-border processing for which it is not the lead supervisory authority?
- Does it make a difference if the controller of this cross-border processing does not have its main establishment in that Member State but has another establishment in this Member State?
- Does it make a difference whether the national supervisory authority brings the action against the main establishment of the controller or against the establishment in its own Member State?
- Does it make a difference if the national supervisory authority has already initiated the action prior to the entry into effect of the GDPR?
- Does art. 58.5 have direct effect, so that it can be relied upon by the national supervisory authority to initiate or continue proceedings against private parties, even if art. 58.5 has not been specifically transposed in the legislation of the Member State?
- If the national supervisory authority is allowed to bring claims, could the outcome of such procedures stand in the way of a contrary finding/decision

¹¹ Hamburg Commissioner for Data Protection and Freedom of Information, Press Release, Mar. 2, 2018, https://datenschutz-hamburg.de/assets/pdf/Press_Release_2018-03-02_Higher_Administrative_Court_Facebook.pdf.

¹² Reuters, “Facebook fined \$33 million for failing to aid Brazil graft probe”, Apr. 5, 2019, <https://www.reuters.com/article/us-facebook-brazil/facebook-fined-33-million-for-failing-to-aid-brazil-graft-probe-idUSKCN1HC2NL>.

of the lead supervisory authority in case the lead supervisory authority investigates the same or similar cross-border processing activities?¹³

Google, Commission Nationale de l'Informatique et des Libertés (CNIL), Jan. 21, 2019. French data protection officials levied a €50 million fine against Google for lack of transparency and failure to obtain valid consent regarding ad personalization. French authorities initiated their investigation and enforcement action despite Google being headquartered in Ireland for GDPR supervisory and enforcement purposes, on the theory that the data processing operations to set up user accounts did not physically take place in Ireland, and therefore were not subject to GDPR's "one stop shop" mechanism.¹⁴

Knuddels GmbH & Co KG., Baden-Württemberg Landesbeauftragte für den Datenschutz und die Informationsfreiheit ("LfDI"), Nov. 22, 2018. A German social media app was fined €20,000, stemming from the theft of personal data on 330,00 subscribers. The supervisory authority noted that the company notified law enforcement and the affected subscribers fully and promptly, and took extensive measures to avoid a repeat attack, resulting in a relatively light fine.¹⁵

Kolibit, Hessian Data Protection Commissioner, Dec. 17, 2018. A small shipping company in Hamburg, Kolibri Image, requested advice from the data protection authority. They had a Spanish service provider process customer data for them, and the service provider refused to set up a written data processing agreement for its services. The authority clarified that the duty to have a written data processing agreement in place is shared by both the data controller and data processor, and that the controller could not unilaterally shift that responsibility on the processor. The company would have to draft a data processing agreement itself and send it to the processor for signing. The company replied that it considered this requirement unduly burdensome. Additionally, the company's lawyer sent a statement clarifying that the request for advice had been made only by way of precaution, and that there was actually no data processing going on at the time. The data protection authority did not accept this explanation and imposed a fine of €5,000 on the company for failing to conclude a data processing agreement. Aggravating factors justifying the penalty were the continued processing even after the authority had explained the legal obligations to the company and the fact that the duty to conclude data protection agreements already existed pre-GDPR. Kolibri Image subsequently posted a statement on its website that after

¹³ English-language case summary with links to original judgment and certified questions may be found at <https://www.dataprotectionauthority.be/news/court-appeal-brussels-refers-facebook-case-court-justice-european-union>.

¹⁴ CNIL, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC," 21 Jan. 2019, <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>.

¹⁵ <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/11/LfDI-Baden-W%C3%BCrttemberg-verh%C3%A4ngt-sein-erstes-Bußgeld-in-Deutschland-nach-der-DS-GVO.pdf>.

further discussions with the data protection authority, the fine was withdrawn, since the authority could not prove that the infringement was in fact ongoing.¹⁶

Lloyd v. Google [2018] EWHC 2599 (QB), Oct. 8, 2018. In a putative representative action against Google for unauthorized tracking of Apple iPhone users Internet activity, the claimant sought permission of the U.K. court to serve process on Google, headquartered in Delaware. The case stems from Google’s “Safari Workaround,” which placed cookies on user’s devices without their knowledge of consent, and used the data generated by the cookies to develop profile groups, such as “football lovers,” to offer potential advertisers. The court first determined that the allegations were serious, the potential class was large, and the claimant had the resources to fairly represent the class. However, the Court found no support in the data protection law or court precedent for the plaintiff’s theory of damages, nor that the members of the putative class had sufficient commonality for the case to move forward. The Court declined to authorize extraterritorial service of process on Google.¹⁷

NT1 and NT 2 v. Google LLC, [2018] EWHC 799 (QB), Apr. 13, 2018. In a case of first impression, the High Court of Justice, Queen’s Bench Division, Media and Communications List, applied a balancing test to order Google to “delist” links to the petitioners’ past criminal convictions, but not to recent proceedings with greater public interest. It is important to note that the petitioners were not requesting that the court itself expunge or seal the underlying legal proceedings – they requested that the court order Google to remove their names from its searchable database.¹⁸

Rousseau Associates, Ruling on Data Breach, Garante per la Protezione dei Dati Personali, No. 9101974, Apr. 4, 2019. The Italian DPA, the Garante, levied a fine of €50,000 against Rousseau Association, which runs online platforms associated with the 5 Star Movement, a political party currently forming part of the Italian government. The Rousseau platform provides online direct e-voting services to Italian citizens for 5 Star. Rousseau had already been under investigation under the pre-GDPR data protection act after a data breach in 2017, which resulted in a requirement to implement a series of improvements to the technical security of the systems as well as updates to the privacy notices. An inspection of the technical and organizational measures revealed continuing security concerns. Two extensions had been given and while the Garante found that significant improvements had been made, the inspection found, among other things, concerns regarding the anonymization of voter information after the vote had been cast as well as concerns regarding the possibility of tampering with a vote after the fact by individuals at Rousseau without sufficient logging to make detection of such tampering possible. Apart from being

¹⁶ Daniel Hunter, “Small business in Germany hit with €5,000 GDPR fine,” PrivSec Report, Jan. 23, 2019, <https://gdpr.report/news/2019/01/23/small-business-in-germany-hit-with-e5000-gdpr-fine/>.

¹⁷ <https://www.judiciary.uk/wp-content/uploads/2018/10/lloyd-v-google-judgment.pdf>.

¹⁸ <https://www.judiciary.uk/wp-content/uploads/2018/04/nt1-Nnt2-v-google-2018-Eewhc-799-QB.pdf>.

the first decision from the Garante, it is also remarkable for having been levied against a processor, Rousseau, without also charging the controller, 5 Star Movement.¹⁹

Uber B.V., et al. Monetary Penalty Notice, U.K. Information Commissioner's Office, Nov. 26, 2018. Ride-hailing service Uber was fined £385,000 for violation of Principle 7 by virtue of its failure to prevent an attack on its cloud-based data repository.²⁰ On the same day, the Dutch Data Protection Authority announced that it was levying a €600,000 fine against Uber stemming from the same set of facts.²¹

Unidentified Limited Liability Company, Austrian Data Protection Authority ("DSB"), Sept. 12, 2018. The Austrian Data Protection Authority issued its first fine under GDPR against a sports betting establishment for failing to configure its CCTV surveillance system to comply with privacy and data security regulations. Specifically, the DPA found that the limited liability company that operated the facility was a "data controller" within the meaning of GDPR; the CCTV system as deployed was over-extensive, covering public streets and parking areas beyond the premises; there was inadequate signage regarding the CCTV system; the system did not delete images within 72 hours and the controller stated no justification of keeping the data longer; and the controller kept no logs of CCTV data processing operations. The controller was fined €5.280,00.²²

WM Morrisons Supermarkets Plc v. Various Claimants, [2018] EWCA Civ 2339, Oct. 22, 2018. In a data breach action stemming from before GDPR went into effect, the trial court held, and the appellate court affirmed, that the actions of a rogue employee who intentionally disclosed personal data of 100,000 current and former employees (and was convicted for fraud) gave rise to vicarious liability on the part of the employer for failing to take reasonable steps to protect the information.²³

Yahoo, Brazil Superior Court of Justice, Feb. 7, 2018. Emails between three executives of Brazil's state-owned federal savings bank dealing with the bank's home loan policy were published on a Brazilian website and then in news media. Law enforcement alleged the website owner that published the emails had violated Brazilian law and requested that Yahoo Brazil turn over emails on the website owner's account. Yahoo Brazil refused to comply with the order because the emails were stored in the U.S. and could only be provided by the U.S. parent company. The court ordered Yahoo Brazil to turn over customer emails to a criminal court—even though the messages were stored on servers outside the country—or face daily fines of \$15,000. Brazil's Superior Court of Justice held that Brazilian units of multinational companies are subject to Brazilian laws and

¹⁹ <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974>.

²⁰ <https://ico.org.uk/media/2553890/uber-monetary-penalty-notice-26-november-2018.pdf>.

²¹ "British and Dutch regulators fine Uber for 2016 data hack," Reuters, November 27, 2019, <https://www.reuters.com/article/us-uber-fine/british-and-dutch-regulators-fine-uber-for-2016-data-hack-idUSKCN1NW0VR>.

²² European Data Protection Board, "First Austrian Fine: CCTV Coverage – Summary," https://edpb.europa.eu/news/national-news/2018/first-austrian-fine-cctv-coverage-summary_en.

²³ <https://www.bailii.org/ew/cases/EWCA/Civ/2018/2339.html>.

international law enforcement cooperation agreements to access emails were not needed to force Yahoo to comply.

II. Consideration of discovery requests in aid of U.S. litigation by non-U.S. authorities

Dreymoor Fertilisers Overseas Pte Ltd. v. Eurochem Trading GmbH, [2018] EWHC 2267 (Comm), Aug. 24, 2018. The High Court of Justice Business and Property Courts of England and Wales, Queen’s Bench Division, Commercial Court, declined to enjoin the enforcement of a discovery order, entered by a U.S. court in the Middle District of Tennessee, to aid litigation in the Virgin Islands and Cyprus. The proposed discovery would likely also be used in arbitration proceedings in London. The court declined to find that the order was “unconscionable” under English law.²⁴

ACL Netherlands BV, et. al v. Lynch, [2019] EWHC 249 (Ch), Feb. 12, 2019. A U.K. judge denied HP’s petition for permission to produce documents obtained in civil litigation in England to U.S. authorities, despite the company’s claims that failure to do so meant it can be held in contempt in the US. Justice Hildyard commented: “I do not accept that the discretion of this court is so limited or its exercise so mechanistic, whether in the context of a foreign subpoena or otherwise.”²⁵

Omers Admin. Corp. v. Tesco PLC, [2019] EWHC 109 (Ch), Jan. 25, 2019. In the ongoing Tesco stock manipulation scandal in the U.K., the Serious Fraud Office (SFO) obtained significant documents and witness statements in its criminal investigation, to be protected under SFO’s tight confidentiality restrictions. SFO shared these with Tesco’s holding company in negotiations toward a plea deal. Subsequently, parallel civil suits were filed by investors who demanded access to the documents in discovery. Neither the SFO nor Tesco’s holding company objected. However, nonparty witnesses in the criminal investigation intervened to object on privacy and confidentiality grounds. The Court closely examined the tensions between the civil discovery rules, the SFO’s strict confidentiality rules, and privacy protections, holding that no one rule or factor was absolute, nor could a simple “balancing test” adequately resolve the various tensions in all situations. In the end, the Court allowed the discovery, with additional non-disclosure provisions and the ability for each of the intervenors to review and redact their documents before production.²⁶

III. Parties in U.S. litigation seeking discovery from non-U.S. sources (*Aérospatiale* factors)

In U.S. civil litigation, Federal Rule of Civil Procedure 34 and its state court equivalents (referred to collectively as “Rule 34”) obligate parties to produce, upon request, non-privileged materials, including electronically stored information (ESI), that are within their

²⁴ <https://www.bailii.org/ew/cases/EWHC/Comm/2018/2267.html>.

²⁵ <https://www.bailii.org/ew/cases/EWHC/Ch/2019/249.html>.

²⁶ <https://www.bailii.org/ew/cases/EWHC/Ch/2019/109.html>.

“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. 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.²⁷ The analysis becomes highly complex and fact-specific when the material is in digital form, perhaps stored in the cloud or on servers world-wide. The analysis becomes even more complicated when the legal relationship between the parties in the U.S. litigation and the foreign custodians of discoverable information is attenuated, when a foreign “blocking statute” or economic regulation prevents the legal transfer of the requested data to the U.S. for the purposes of litigation, or when the privacy and data protections laws of country in which the documents or data is located restrict or prohibit its transfer to third parties outside that country.

In those instances, the court is often asked to order the parties to produce discovery directly under Rule 34, putting the responding party in the awkward position of possibly violating the foreign nation’s laws if it complies with the order, or proceeding under the often slow and cumbersome alternative discovery mechanisms, such as “letters rogatory” to the appropriate court in the country where the materials are located, or the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (the “Hague Evidence Convention”), if the foreign nation is a signatory. The decision requires an analysis based on the factors enumerated in the Restatement (Third) of Foreign Relations Law §442(1)(c), commonly referred to as the *Aérospatiale* factors, after the leading U.S. Supreme Court decision endorsing them:²⁸

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.

These factors were based on the then-existing draft of the American Law Institute’s RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW, §442. Many courts also consider:

6. the hardship of compliance on the party or witness from whom discovery is sought; and

²⁷ 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.

²⁸ *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, 482 U.S. 522 (1987).

7. the good faith of the party resisting discovery.

In addition, some courts have considered the extent and the nature of the hardship that inconsistent enforcement would impose upon the foreign party, and the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state.²⁹ The application of these tests is discussed at length in The Sedona Conference's *Framework for Analysis of Cross-Border Discovery Conflicts* (2008)³⁰ and *International Litigation Principles on Discovery, Disclosure & Data Protection in Civil Litigation* (Transitional Edition) (2017).³¹

Historically, U.S. courts considering proceeding via letters rogatory or the Hague Evidence Convention perform the analysis diligently and almost invariably conclude that the interests of the United States in fully litigating the dispute dictate that discovery should proceed under Rule 34, often making the observation that the foreign data protection laws cited by the parties resisting such discovery are seldom or lightly enforced, indicating that the host country had little interest in privacy or data protection.

The almost-daily reports of data breaches worldwide, the implementation of GDPR and similar privacy and data protection laws in other countries, and the passage of state privacy laws in the United States itself, have significantly altered the environment in which U.S. courts are considering privacy and data security as a factor in evaluating the scope and methods of discovery. While a survey of reported court opinions and press reports of civil actions provides a foggy and incomplete picture, it indicates some overall trends since. It appears that a few U.S. courts are taking foreign privacy and data protection laws more seriously distinguishing them from “blocking statutes,” in which the primary interest being advanced is hostility to foreign litigation in general.

Selected court opinions

Brooks Sports, Inc. v. Anta (China) Co., Ltd., No. 1:17-cv-1458, 2018 WL 7488924 (E.D. Va. Nov. 30, 2018) *report and recommendation adopted*, 2019 WL 969572 (Jan. 11, 2019); *judgment modified*, 2019 WL 969569 (Feb. 5, 2019). This Lanham Act litigation was filed as an appeal against a rejection by the Patent and Trademark Appeals of the plaintiff's claims of trademark infringement and dilution. The plaintiff sought default judgment due to alleged discovery misconduct. In discovery, the defendant identified only one witness and failed to produce documents in several categories, including relevant business plans; agreements with third parties in the U.S.; WeChat messages, and sales, revenue, and income records. The court entered an order compelling further production, with which the defendant failed to comply despite two deadline extensions. Regarding the WeChat messages, counsel for the defendant represented that of the 14 custodians identified, only one (a California resident) provided the required consent under Chinese law for a search of their WeChat. When specifically asked by the court why the Chairman

²⁹ See, e.g., *United States v. Vetco Inc.*, 691 F.2d 1281, 1288 (9th Cir. 1981).

³⁰ https://thesedonaconference.org/publication/Framework_for_Analysis_of_Cross-Border_Discovery_Conflicts.

³¹ https://thesedonaconference.org/publication/International_Litigation_Principles.

of the defendant company refused to consent, no explanation was provided. The Magistrate Judge declined to enter into an analysis of relevant Chinese law and assumed that the refusals were lawful, but stated that the “Court remains very troubled that high-level executives, including Anta’s co-founder and Dacheng Peng—the person who was initially identified in Anta’s Rule 26(a) disclosures as the only person having information related to this litigation—refused to allow the company to search their WeChats. Their refusal is even more concerning given the evidence before the Court that WeChat is used extensively by Anta employees to conduct business.” The Judge went on to hold that “Anta may not avoid penalties for their claimed inability to produce those communications. Anta clearly knowingly allowed its employees to use WeChat for substantive business communications through only their personal accounts and devices. . . . Anta should not be able to conveniently use Chinese law to shield production of communications responsive to discovery requests when it could have set up Anta-controlled WeChat accounts for its employees’ use which would not have the same issues regarding Chinese privacy laws.” The Magistrate Judge found that this refusal to engage in discovery, along with ample evidence that other requested information existed and was withheld in bad faith and in violation of a court order, justifying the sanction of default judgment under Fed. R. Civ. P. 37(b) and the court’s inherent authority.

Finjan, Inc. v. Zscaler, Inc., No. 17-cv-06946, 2019 WL 618554 (N.D. Cal. Feb 14, 2019). In a patent infringement suit, the plaintiff sought discovery of its former sales manager, a British citizen, now an employee of the defendant. The defendant asserted that the discovery of the British citizen’s emails would violate the General Data Protection regulation (GDPR) unless the scope of the request was significantly narrow, the emails could be “anonymized,” and the plaintiff pay part of the cost. The plaintiff countered that production of the emails would be permissible under an “attorney’s eyes only” protective order. Applying the *Aérospatiale* factors, the court found that the requested emails would be important to the case; the search terms proposed to locate the responsive emails were adequately narrow; that while the former employee is a British citizen, the defendant corporation is based in the U.S.; and the discovery sought cannot be obtained from another source. In balancing the national interests, the court found that the United States has a strong interest in patent enforcement, and that while the United Kingdom has an interest in protecting the privacy of its citizens, to the extent that any of the requested discovery implicates personal data, any danger of exposure would be obviated by the imposition of a protective order. Finally, the defendant, although citing to the Sedona Conference International Litigation principles, failed to provide any evidence that it would actually face legal jeopardy by producing the emails.

Grupo Petrotex, SA De CV v. Polymetrix AG, No. 16-cv-2401, 2019 WL 2241862 (D. Minn. May 24, 2019). In a patent infringement case the defendants sought to prevent discovery, asserting that its data was inextricably intertwined with confidential third-party data, which it was forbidden from producing under Art. 162 of the Swiss Criminal Code and contract. Defendants also asserted the Swiss Data Protection Act and Swiss Federal Unfair Competition Act. The court noted that the appropriate scope of discovery

was limited to a specific manufacturing process at a plant in Poland, but that plaintiffs sought wide-ranging information on a global basis. As the court had independent obligation under Fed. R. Civ. P. 1 to prevent a “fishing expedition,” it would not compel global discovery but would allow “reasonable and proportional discovery” related to the specific process and patent claims. However, the court found that Art. 162 of the Swiss Criminal Code would apply to technical engineering and manufacturing drawings and specifications for the process at issue, even within a narrowed scope of discovery, as the defendant had sufficiently established that protected third-party confidential information would be compromised by the proposed discovery. In addition, Art. 273 of the Code prevents disclosure of third-party manufacturing or business secret information to a foreign entity. On balance, the court found that documents within the permissible scope of discovery should be produced under Rule 34 as opposed to the Hague Evidence Convention, allowing for the redaction or withholding of privileged and work product material, and under an “attorneys eyes only” protective order. Non-responsive sections discussing competitively sensitive specific customers of otherwise responsive documents could be redacted. The defendant was ordered to produce a log of privileged and withheld material within 10 days of production.

In re Davol, Inc./C.R. Bard, Inc., No. 2:18-md-2846, 2019 WL 341909 (S.D. Ohio Jan. 28, 2019). In a medical products liability lawsuit, the court granted, in part, the plaintiffs’ motion to compel discovery of communications by Bard foreign affiliates and subsidiaries with foreign regulators in the EC, U.K., Germany, Canada, Australia, and Japan. The court noted that the plaintiffs met their initial burden of showing the relevance of their proposed discovery, after an initial request was narrowed during the meet-and-confer process and further narrowed by the court to cover only official communications with specified authorities and only regarding the specific product at issue in the U.S. litigation, distinguishing this request from the one rejected by another court in *In re Bard IVC Filters Product Liability Litigation*, 317 F.R.D. 562 (D. Ariz. 2016). The burden then shifted to the defendants, who failed to show that the discovery was not proportional and provided only conclusory statements regarding burden without supporting affidavits, prompting the court to order the requested discovery, with the limited scope.

Larson Manufacturing Co. of South Dakota, Inc. v. Western Showcase Homes, Inc., 4:16-CV-04118, 2019 WL 102252 (D.S.D. Jan. 4, 2019). In a contract dispute involving the production, sale, and financing of modular housing units, the parties had engaged in parallel litigation in Canada, and the defendant sought letters rogatory to obtain documents from Canadian individual and entities related to the Canadian litigation. In denying the defendant’s request, the court noted that the defendant failed to establish the relevance of the proposed discovery, conform the proposed letter rogatory to Canadian law, and inform the court regarding what possible restrictions there might be on discovery under Canadian law.

Moretti v. The Hertz Corp., No. 14-469, 2018 WL 4693473 (D. Del. Sept. 30, 2018). In a consumer class action alleging overcharging for rental car insurance, discovery of the

defendants' Mexican franchisees was allowed under Federal Rule of Civil Procedure 34. The court followed Third Circuit precedent in applying the "legal right" test to determine that the defendant in the U.S. had "possession, custody, or control" of the relevant records by virtue of the franchise agreements. The defendants had bargained for legal access to the franchisees' records, and had obtained them previously for audit purposes, so they could not now argue that they did not have "possession, custody, or control," even if the records were physically in Mexico.

Motorola Solutions, Inc. v. Hytera Communications Corp., No. 17-C-1973, 365 F. Supp. 3d 916 (N.D. Ill. March 15, 2019). In copyright infringement/misappropriation of trade secrets case, the plaintiff renewed a motion to compel inspection of computers of competitor located in China, after losing a motion for summary judgment. The plaintiff claimed that the intrusive discovery was necessary to combat the defendant's ongoing denials of liability. The court concluded that the mere desire for more evidence, and suspicion that opponent had not produced everything, did not warrant intrusive discovery even without the consideration of the tensions with foreign data protection laws, but conducted a "brief excursion" Chinese law based on parties' dueling expert opinions regarding the effect Art. 277 of Chinese Civil Procedure Law, which provides:

The request for and provision of judicial assistance shall be conducted through the channels stipulated in the international treaties concluded or acceded to by the People's Republic of China. Where no treaty relations exist, the request for and provision of judicial assistance shall be conducted through diplomatic channels.

The embassy or a consulate in the People's Republic of China of a foreign state may serve documents on, investigate, and take evidence from its citizens, provided that the law of the People's Republic of China is not violated and that no compulsory measures are adopted.

Except for the circumstances set forth in the preceding paragraph, no foreign agency or individual may, without the consent of the competent authorities of the People's Republic of China, serve documents, carry out an investigation or collect evidence within the territory of the People's Republic of China.

The plaintiff submitted an affidavit of a Chinese lawyer asserting that the rule did not prevent voluntary party disclosures, but court noted that response to a court order would not be voluntary. The plaintiff also argued that discovery should be granted under *Aérospatiale* comity analysis. The court conducted a brief comity analysis and found most factors weighed against the plaintiff. The evidence would be cumulative; forensic examination was inherently intrusive; the evidence probably originated outside of the U.S.; and the comparison of different national interests resulted in a "toss up." In the end, the court declined to rule on the applicability of Chinese law, as the plaintiff failed to show

relevance, and even if it had, forensic examination of computers in China was “far out of proportion.”

Nike, Inc. v. Wu, 349 F.Supp.3d 346 (S.D.N.Y. 2018). The famous sports apparel manufacturer brought trademark infringement actions against several retailers and obtained default judgements, which were assigned to an investment firm for collection. The firm subpoenaed several nonparty Chinese banks seeking account information on the defendant retailers, which the banks opposed. The magistrate judge held, and the district judge affirmed, that the banks had sufficient business operations in the Southern District of New York to support the court’s exercise of jurisdiction in enforcing the subpoenas. The banks objected, asserting that the magistrate judge failed to adequately take China’s bank secrecy law into account, which they claimed posed the burden of being “forc[ed] to violate the laws of their home country” if they complied with the subpoena. The court rejected that argument, saying that it was irrelevant to the due process considerations in finding jurisdiction. That factor was considered by the magistrate judge in a separate comity analysis but balanced against the interest in combatting counterfeit goods. As stated by the court, “In fact, [the magistrate judge] balanced this factor against the burden claimed by the Banks. If the Banks failed to brief this issue adequately below, focusing only on the breadth of the Subpoenas and the violation of bank secrecy laws, and neglecting to include facts such as the location of key documents, actors, and assets, they cannot now claim that Judge Freeman committed clear error. The Magistrate Judge properly found that ‘the Banks ha[d] failed to meet their burden to demonstrate that exercising jurisdiction over them would be unreasonable.’” The magistrate judge also found that resort to the Hague Convention would likely not produce results, as the banks presented little evidence beyond form documents and public reports that the Chinese Ministry of Justice would be willing and able to facilitate the process, as required by treaty.

Phoenix Process Equipment Co. v. Capital Equipment & Trading Corp., No. 3:15CV-00024, 2019 WL 1261352 (W.D. Ky. Mar. 19, 2019) In unfair competition action, the court found no substantive conflict between federal civil discovery rules and Russian data protection laws and issued an order compelling discovery under Rule 34.

Randall v. Offplan Millionaire AG, No: 6:17-cv-2103, 2019 WL 1003167 (M.D. Fla. Mar. 1, 2019). In a complex real estate fraud action, the court granted the plaintiff’s motion to compel jurisdictional discovery, including document production and a deposition, from an individual defendant who was a German national and Swiss resident. The defendant asserted that he had already provided 6,000+ documents to his attorneys to review, but they advised against production of the documents or sitting for a deposition, as these actions would contravene Swiss law. The court was not persuaded, as the documents were already in Florida, which is where the deposition was proposed to take place, the defendant had already been participating in discovery, and the defendant cited no case law regarding non-Swiss citizens being precluded from producing his or her own documents in litigation. The court also rejected the defendant’s proposal to proceed under Chapter II of the Hague Evidence Convention, as the request was narrow and no Swiss national interests were at

stake. The discovery was ordered under the Federal rules, with the plaintiff assuming the travel costs to depose the defendant in Florida.

Route1 Inc. v. Airwatch LLC, No. 1:17-cv-00331, 2018 WL 6427145 (D. Del. Dec. 7, 2018). In a patent dispute, the defendant sought letters rogatory to obtain discovery from Canadian nonparties who held large blocks of shares in the plaintiff corporation, on the theory that such significant shareholders would be able to provide relevant information on the value of the patents in dispute for damage calculations. The court noted that if this were simply a request for discovery from domestic nonparties, it would likely decline the request on relevance grounds, finding the defendant's theory "speculative." The court saw no reason why it should grant the defendant's application in this case but noted that other courts have held that the burden is on a party opposing an application for letters rogatory to show "good cause" for denying the request, and that this court likewise should "provide reasons for the denial to ensure deference on appeal." Therefore, the court expressly stated, "There is insufficient reason to engage in the complication, delay, and expense inherent to letters rogatory where Plaintiff can provide the same facts and it is complete speculation that the opinions sought exist."

Royal Park Investments SA/NV v. HSBC Bank USA, N.A., 14 Civ. 8175, 2018 WL 745994 (S.D.N.Y. Feb. 6, 2018). In a putative class action, the plaintiff investment fund's assignor bank withheld document custodial information and redacted individual names and email addresses in deference to the Belgian Data Privacy Act. The court held that the law of the case obligated the plaintiff to produce the requested documents, despite the fact that they had been transferred to the Belgian-based bank as part of the assignment, and that the Magistrate Judge's comity analysis, articulated in a previous unreported decision, weighs in favor of compelling the bank to produce documents in unredacted form, with custodial information restored.

Salt River Project v. Trench France SAS, No. CV-17-01468, 2018 WL 1382529 (D. Ariz. March 19, 2018). In a public construction project dispute involving the Canadian subsidiary of a French engineering company, the court opted to utilize the Hague Convention procedure and in particular Chapter II, which allows for the appointment of a private attorney approved by the host country to serve as a "commissioner" for the taking of evidence. This is considerably more efficient than proceeding under Chapter I, which is similar to the "letters rogatory" procedure, in that it requests the authorities in a foreign country to appoint a judge to oversee discovery. Unfortunately for students of civil procedure, the case was settled shortly after the court ordered discovery under Chapter II, and we have no report of its effectiveness.³²

Securities Investor Protection Corp. v. Madoff Investment Secs. LLC, No. 08-01789, 2019 WL 1055958 (S.D.N.Y. Mar. 5, 2019). In a complex securities fraud action, the court granted a limited deposition of a non-party Bermuda citizen. The court examined the

³² The author recommends this case for its brevity and clarity, compared with other court decisions addressing the *Aérospatiale* factors.

conflicts between U.S. and Bermuda discovery law and applied the *Aérospatiale* comity analysis noting that the requested discovery involved a citizen of non-Hague signatory country.

TRP Co., Inc. v. Similasan AG, No. 2:17-cv-02197, 2019 WL 1382491 (D. Nev. Mar. 27, 2019). In a trademark dispute regarding homeopathic eyedrops, the plaintiff requested that the court issue a letter of request under the Hague Evidence Convention to obtain physical evidence from the defendant, a Swiss corporation. The plaintiff argued letter was necessary because the defendant contested personal jurisdiction and declined to produce discovery, and the court would be unable to address the merits of the case without the evidence sought in interrogatories and document requests. The court granted the plaintiff's request, including in its order a detailed letter under Hague Evidence Convention Art. 3, addressed to the Swiss court, setting out and explaining reasons for discovery requests.

IV. Parties in non-U.S. litigation seeking discovery from U.S. sources (28 U.S.C §1782 and *Intel* factors)

There appears to be a significant uptick in applications to U.S. courts by foreign litigants seeking discovery to assist in foreign actions, perhaps with the view that they could obtain document, records, and witness testimony that would be unavailable under the laws and procedures in their home countries. In U.S. federal courts, such applications are made pursuant to 28 U.S.C §1782, which sets out a short and relatively simple set of questions for the court to answer in granting or denying the request:

1. whether the person from whom the discovery is sought reside within the district;
2. whether the request seeks evidence for use in a “foreign proceeding;”
3. whether the request is made by “any interested person;” and
4. whether the material sought is not protected by a legally applicable privilege.

The U.S. Supreme Court in *Intel Corp. v. Advanced Micro Devices*, 542 U.S. 214 (2014) established four additional discretionary factors for courts to consider:

5. whether the person from whom the discovery is sought is a party to the foreign proceeding;
6. the nature and character of the foreign tribunal and proceeding;
7. whether the request is an attempt to circumvent the rules of the foreign tribunal; and
8. whether the request is unduly intrusive or burdensome.³³

These are referred to as the *Intel* factors, and courts are permitted to decline an application based on one or more of the *Intel* factors, even if all the statutory factors have been met.

Selected Court Opinions

³³ *Intel Corp. v. Advanced Micro Devices*, 542 U.S. at 264-65.

In re Accent Delight Internat'l Ltd. and Xitrans Finance Ltd., 16-MC-125, 18-MC-50, 2018 WL 2849724 (S.D.N.Y. June 11, 2018) (appeal to 2d Circuit pending). In opposing an application under 28 U.S.C §1782, fine arts dealer Sotheby's asserted that European Union and Swiss privacy laws prevented it from producing records in a long-running \$1 billion international art fraud legal battle. Although Sotheby's now sought to halt document production, its lack of redaction in prior productions contradicted its newly-found privacy concerns, the judge ruled. Sotheby's will be required to turn over the requested documents even if it must redact, "document-by-document," any personal protected information including data on racial or ethnic origin, political opinions, sexual life, and religious beliefs to avoid violation of EU data protection laws.

In re Biomet Orthopaedics Switzerland GmbH, No. 17-3787, 2018 WL 3738618 (3d Cir. Aug. 6, 2018). The appellate court vacated the district court's blanket denial of discovery under 28 U.S.C §1782 and remanded for further development of the factual records and reconsideration of relevant factors.

In re Frederico Da Costa Pinto, No. 17-22784, 2018 WL 6620905 (S.D. Fla. Aug. 27, 2018). The Magistrate Judge issued a Report and Recommendation that a nonparty be allowed to intervene to quash a 28 U.S.C. §1782 order and to permit a modified application to be filed.

In re Furstenberg Finance SAAS, 18-mc-44, 2018 WL 3392882 (S.D.N.Y. July 12, 2018). The court granted an application for discovery to be used to initiate a Belgian criminal complaint, which was a sufficiently certain procedure to satisfy the statutory requirement, even if petitioner would not be a formal party to the Belgian action.

In re H.M.B. Ltd., No. 17-21459, 2018 WL 4778459 (S.D. Fla. July 2, 2018). In aid of a foreign judgment collection action, the court granted an application under 28 U.S.C. §1782 but ordered the parties to confer regarding narrowing the scope of the requested discovery and limiting it to certain transactions.

In re Hansainvest Hanseatische Investment-GMBH, 364 F. Supp. 3d 243 (S.D.N.Y. 2018). The court granted an order sought by a German party to obtain discovery for use in a contemplated proceeding in Germany regarding alleged violations of German law in connection with the sale of a business to foreign investors.

In re Hanwei Guo, No. 18-MC-561, 2019 WL 917076 (S.D.N.Y. Feb. 25, 2019). An application for judicial assistance under 28 U.S.C. §1782(a) denied, as the intent would be to use the discovery in an arbitration proceeding, which the Second Circuit does not consider to be "a proceeding in a foreign or international tribunal" under the statute.

In re Hornbeam Corp., No. 14-24887, 2018 WL 1998912 (S.D. Fla. Apr. 27, 2018); *reconsideration denied*, 2018 WL 7577230 (S.D. Fla. July 6, 2018) The court denied an application under 28 U.S.C. §1782, as the foreign action had already been dismissed, and it was unclear whether an appeal was pending or that evidence could be introduced on appeal.

In re Hoteles City Express, No. 18-mc-80112, 2018 WL 3417551 (N.D. Cal. July 13, 2018); *application approved*, 2018 WL 3753865 (N.D. Cal. Aug. 8, 2018). In an action for defamation, Hoteles was preparing to file a lawsuit in Mexico seeking damages from individual(s) responsible for making defamatory statements about Hoteles and republishing such statements in a video posted on Facebook. The court found that Hoteles' application satisfied the minimum requirements of 28 U.S.C. §1782, but the court initially denied the application without prejudice because Hoteles had failed to provide sufficient information regarding the defamatory statements. Hoteles' renewed application resolved the court's concerns, and the court granted the application.

In re Levi Strauss & Co., No. 18-mc-80123, 2018 WL 3872790 (N.D. Cal. Aug. 15, 2018). The court granted Levi Strauss's application under 28 U.S.C. §1782 to subpoena the Internet Archive to assist with Belgian trademark litigation.

In re MTS Bank, No. 17-21545, 2018 WL 3364475 (S.D. Fla. July 10, 2018). In aid of a bankruptcy proceeding involving a privately-owned Russian airline, the court granted an application for discovery under 28 U.S.C. §1782 limited to a jurisdictional deposition of a Russian citizen living in Florida.

In re Pioneer Corp., No. MC 18-0037, 2018 WL 2146412 (C.D. Cal. May 9, 2018). Pioneer initiated a patent license dispute in German court, seeking reimbursement of license fees paid on allegedly expired patents. The German court dismissed the action, but Pioneer applied for discovery in aid of an appeal. The Magistrate Judge denied the application, holding that the discovery requested was likely irrelevant to the appeal, facially overbroad, and likely to be in the possession of a party to the German action.

In re Pioneer Corp., No. LA CV18-04524, 2018 WL 4963126 (S.D. Cal. Aug. 27, 2018); 2018 WL 4961911 (S.D. Cal. Sept. 12, 2018). After discussion of the appropriate standard of review for an order under 28 U.S.C. §1782, the District Judge upheld the Magistrate Judge's denial of the requested order, finding no showing of "clear error."

In re Postalis, No. 18-mc-497, 2018 WL 6725406 (S.D.N.Y. Dec. 20, 2018). The court denied an application under 28 U.S.C. §1782 where the foreign action was speculative, the discovery sought was overbroad, and foreign courts would be able to obtain the evidence without assistance.

In re: Request for Judicial Assistance from the First Instance Court in Civil & Commercial Matters No. 12 in Buenos Aires, Argentina, No. 3:19-MC-2-J-32, 2019 WL 645213 (M.D. Fla. Feb. 15, 2019). In response to a request from a court in Argentina, the court appointed a commissioner to seek discovery under 28 U.S.C. §1782 of certain bank records in the United States, finding that the Right to Financial Privacy Act does not bar requests from foreign authorities acting pursuant to the discovery statute under the supervision of a U.S. court.

In re Schlich, 893 F.3d 40 (1st Cir. 2018). The Court of Appeals for the First Circuit upheld a district court's denial of discovery under 28 U.S.C. §1782 in aid of a proceeding before

the European Patent Office (“EPO”). The petitioner was seeking information concerning an inventorship study, as well as information regarding the assignment of the rights to the corresponding inventions. In opposing the petitioner’s request, the target entities submitted, among other things, a declaration from a former EPO official that discovery concerning these issues would not be considered relevant by the EPO. The district court found the petitioner had satisfied the four statutory requirements of 28 U.S.C. §1782, but the nature and character of the tribunal and proceeding weighed in favor of denying the request for assistance. The First Circuit affirmed the trial court’s denial of the request, noting that the trial court had appropriately considered whether the EPO would be receptive to the requested evidence, and it concluded that it would not. The First Circuit noted that §1782 does not put the burden of proof on either the petitioner or the respondent but allows them to present their evidence for the trial court to make the ultimate decision. Notably, the First Circuit stated that a trial court could be justified in denying the request even when all of the statutory requirements have been satisfied, as long as it determines that the discretionary factors favor denying the request.

JSC MCC Eurochem v. Chauhan, No. 3:17-mc-00005, 2018 WL 3872197 (M.D. Tenn. Aug. 15, 2018). In a billion-dollar international corruption action being adjudicated in the British Virgin Islands and Cyprus (related to *Dreymoor Fertilisers Overseas Pte Ltd. v. Eurochem Trading GmbH*, [2018] EWHC 2267 (Comm)), Eurochem petitioned under 28 U.S.C. §1782 for a discovery order, which was granted by the magistrate judge. The respondent objected, but the magistrate’s order was affirmed by the district judge with a thorough analysis of the statutory and discretionary factors.

Kiobel v. Cravath, Swaine & Moore, LLP, 895 F.3d 238 (2nd Cir. 2018). The District Court granted a petition under 28 U.S.C. §1782 to subpoena documents from a law firm in aid of a lawsuit against a corporation in the Netherlands. The law firm appealed, and the appellate court reversed, stating that the district court abused its discretion by granting the petition. The documents sought had been collected from a former client in another litigation and were subject to a non-disclosure protective order, which the district court should not have modified absent a compelling need.

Leutheusser-Schnarrenberger v. Kogan, No.18-mc-80171, 2018 WL 5095133 (N.D. Cal. Oct. 17, 2018). The petitioners, French and German privacy advocates, applied *ex parte* for judicial assistance under 28 U.S.C. §1782 to take discovery of a California resident associated with the Cambridge Analytics affair. The application was denied, as court founds no “proceeding” pending or reasonably contemplated.

Mangouras v. Squire Patton Boggs, No. 17-3633, 2018 WL 5733599 (2d Cir. Oct. 31, 2018) (Summary Order). The Second Circuit held that a district court’s decision in a 28 U.S.C §1782 matter may be “final” for the purposes of appeal, even if the actual discovery has not been completed.

Qualcomm Inc., No. 18-mc-80134, 2018 WL 6660068 (N.D. Cal. Dec. 19, 2018). Qualcomm and Apple were engaged in a contract action before the European Commission,

which Qualcomm lost and was now appealing to the General Court of the European Union. Qualcomm applied under 28 U.S.C §1782 to take discovery from Apple in the United States for use in the appeal. Apple objected, asserting that the proposed discovery would be inadmissible in the German proceeding. The court rejected Apple’s argument as conclusory and granted Qualcomm’s motion to compel.

V. Non-U.S. litigants seeking U.S. recognition of foreign data privacy laws

Article 17(1) of the General Data Protection Regulation provides that “[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.” This provision, colloquially referred to as the “right to be forgotten,” can complicate U.S. litigation that involves European citizens as parties or witnesses.

The constitutional and common law tradition in the United States is that civil litigation conducted in state or federal courts is a public proceeding, and documents filed with the court are presumptively public. In discovery, the parties may agree to a protective order that keeps discovery confidential, which the court will grant routinely upon a finding of “good cause.” However, any proceedings conducted by the court itself, or documents filed with the court, cannot be sealed except upon a finding of “compelling reasons,” which is rare. In some jurisdictions, that rule is relaxed slightly to allow sealing of personal information unrelated to the merits of the action.³⁴ But it is clear that the U.S. courts’ strong tradition of public access is in tension with the GDPR’s recognition of EU citizens’ “right to be forgotten.” The courts of England and Wales have a similar common law tradition, but the lack of a written constitutional guarantee of public access to the courts provides more flexibility.

In addition to the tension of legal cultures, U.S. courts, government agencies, and other actors in the legal system face logistical structural challenges in accommodating foreign litigants’ and attorneys’ desire to have the same level of privacy and data protection as they enjoy in their home countries. This is a difficult practical issue that is beginning to emerge in a number of quarters, as the selected opinions below demonstrate.

Selected Court Opinions

Chabert et al. v. Bujaldon et al., 1:16-cv-00293-DLH-CSM (D.N.D.). A French citizen named as defendant in a real estate and securities fraud action in North Dakota demanded that several websites hosting public court dockets remove his name from their databases, invoking the “right to be forgotten” under GDPR. One U.S.-based site, CourtListener, flatly refused on the basis that it was not subject to GDPR, and alternatively, that GDPR allows for the archiving of information in the public interest, for scientific or historical research purposes, or statistical purposes. A second site, PlainSite, acquiesced and replaced his name with initials wherever it appeared in their index, in response to pressure from its

³⁴ See generally, *The Sedona Guidelines: Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases*, March 2007, https://thesedonaconference.org/publication/Working_Group_2_Guidelines.

German-based Internet Service Provider. A third site, Pacer Monitor, deleted the entries entirely. As of this writing, the full docket is still available on the U.S. Courts' Pacer system, and it indicates that a default was entered against the defendant January 4, 2019.

Dry D.A.C. v. Nikka Finance, Inc., CA 18-0284, 2018 WL 5116094 (S.D. Ala. Oct. 19, 2018). In an action in admiralty to collect on a foreign judgment, the defendant moved for a protective order, grounded in GDPR, to prohibit the videotaping of a deposition of an English witness in Greece. The court denied the motion but ordered that the videotape not be publicly disclosed or utilized in any other proceeding.

Georgia Dept. of Labor v. McConnell, S18G1316, S18G1317, 2019 WL 2167323 (Ga. May 20, 2019). In a putative class action against the State of Georgia, the plaintiffs alleged that personal information regarding 4,757 unemployment compensation applicants was collected on a spreadsheet that was negligently emailed to approximately 1,000 recipients. The Georgia Supreme Court held that while the State's Torts Claims Acts waived sovereign immunity, the statute narrowly restricted such actions to situations in which the tort was intentionally committed by a state employee for personal benefit and did not contemplate negligence actions. The court held that the State has no general legal duty not to subject others to an unreasonable risk of harm.

Ironburg Inventions Ltd. v. Valve Corp., No. 17-1182, 2018 WL 4031231 (W.D. Wash. Aug. 22, 2018); *motion to compel granted*, 2018 WL 4281531 (Sept. 7, 2019). Two English witnesses in a patent action invoked GDPR and Article 8 of the European Convention on Human Rights to move that transcripts of their depositions and hearing testimony be sealed, arguing that sensitive personal information related to the witnesses' medical conditions should not be made public. Citing the 9th Circuit's rule that documents filed with the court cannot be sealed except on a showing of "compelling reasons," the court granted the motion only to the extent that personal information unrelated to the merits of the case appear in the transcripts. The court refused to seal the transcript of a prior related Patent Trial and Appeals Board hearing that had already been made public.

Maryland State Bar Ethics Opinion No. 2018-06. In response to an attorney inquiry, the Maryland State Bar explored the tension between obligations under GDPR to delete references to former European clients upon request and provisions of the Maryland Rules of Professional Conduct (similar to other state rules) requiring attorneys to avoid conflicts in representation. The Bar's opinion notes that while its regulations do not require an attorney necessarily to maintain records, and therefore do not prevent the deletion of former client's names, effective conflict checks are impossible without those records. The Bar also noted that former clients may waive a claim of conflict. Therefore, the bar resolved the tension by holding:

If a former client asks an attorney to delete the information needed to manage conflicts of interest, and the GDPR requires the attorney do so, we believe that the client's request can act as a waiver of conflicts that could have been discovered had the data been retained if: (1) the firm provides

written advice to the former client that fully informs the former client that deleting the information could result in a conflict and that by requiring such deletion the client consents to the firm's potential future representation of other clients with conflicts that might otherwise have been discovered, and (2) none of the attorneys who handle the matter for the firm have any retained knowledge of the former client's information.³⁵

³⁵ Maryland State Bar Ethics Opinion No. 2018-06 at 2.

Appendix

APAC Region Recent Data and Privacy Enforcement

May 15, 2019

Draft Prepared by Cathy Choi and Natascha Gerlach, Cleary Gottlieb Steen & Hamilton LLP

1. China

Overview. The reigning data protection law in China is the Cyber Security Law (“CSL”), which was passed on November 7, 2016, and went into effect on June 1, 2017. See [KPMG 2017 Report](#). The Cyberspace Administration of China (“CAC”) is the primary authority charged with supervising and enforcing the CSL. Both the CAC and local-level enforcement authorities have been investigating incidents involving CSL violations and imposing fines. See [Reed Smith 2018 Report](#).

Enforcement Actions and Court Decisions. There have been a number of recent court decisions and enforcement actions to address data and privacy mismanagement or misuse.

- The CAC and its local counterparts have ordered the closure or suspension of some popular mobile apps (e.g., Toutiao (Bytedance), Kuaishou, TikTok, and Microblog) based on the inappropriate or illegal content transmitted on platforms such as online news, social networking, short-video, online music, and e-commerce apps. <https://www.lexology.com/library/detail.aspx?g=f54cc716-d5e1-47fd-b90f-64983b61f992>
- On March 20, 2019, the People’s Court in Tianjin ruled that two mobile apps must stop sharing user information. Specifically, TikTok must immediately stop providing the WeChat/QQ open platform authorized login to Duoshan. At the same time, Duoshan was also required to stop using WeChat/QQ user profile photos and nicknames previously obtained through TikTok. <https://www.lexology.com/library/detail.aspx?g=88874226-7e13-471d-81d3-3903d35c96db>
- On March 15, 2019, China Central Television exposed the role of telecommunications companies in a harassment-industry chain, in which intelligent robots made harassing calls and big data was used to analyze private information. The Ministry of Industry and Information Technology ordered that the companies shut down the chain responsible for making the harassing calls immediately, stop the transmission of illegal numbers, and strengthen the management of telecommunication resources. The exposed call-center enterprises (YiGe Technology, YiLongXinKe, MiaoDi Technology, and LingWo Network) were also investigated. <https://www.lexology.com/library/detail.aspx?g=88874226-7e13-471d-81d3-3903d35c96db>

New Regulations. On January 10, 2019, the CAC approved new rules for blockchain service providers called the "Provisions on the Administration of Blockchain Information Services," which came into effect on February 15, 2019 (see Zhang, Karl, "Provisions on the Administration of Blockchain Information Services (Mainland China)", January 10, 2019 <https://www.leetsai.com/others/provisions-on-the-administration-of-blockchain-information-services-mainland-china>) (http://www.cac.gov.cn/2019-01/25/c_1124042599.htm [source document in Chinese]). The Provisions require blockchain service providers to register with the Cyberspace Administration of China and be subject to regular monitoring. Blockchain service providers must implement comprehensive measures, such as user registration and identity verification, and report to the government any new products, applications, or functions before launching them. <https://www.jonesday.com/jones-day-global-privacy--cybersecurity-update--vol-21-03-01-2019/> (citing http://www.cac.gov.cn/2019-01/25/c_1124042599.htm).

Relationship with the EU. Recent developments with Huawei highlight potential conflicts with European privacy regulations. European officials have stated that current guarantees for Europeans' data in China are not sufficient and current Chinese data regulation policies would not be sufficient for an "adequacy agreement." Since China's National Intelligence Law of 2017 requires companies to assist intelligence services, European officials have expressed concerns about a lack of safeguards, transparency, and democratic oversight. In an attempt to assuage Western fears about surveillance, Huawei's CEO has stated that he would not comply with a request from the Chinese government to hand over data, stating that he would "definitely refuse" such a request. Chinese officials also insist that companies like Huawei are private and not subject to oversight by the government. <https://www.politico.eu/article/european-union-eyes-privacy-clampdown-on-china-surveillance-huawei/>.

2. South Korea

Overview. South Korea's Personal Information Protection Act ("PIPA") (English translation available here: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=46731&lang=ENG) was promulgated in 2011 and has been subsequently amended. The South Korean Homeland and Security Ministry is tasked with the enforcement of PIPA. On November 15, 2018, amendments to PIPA were submitted to the South Korean National Assembly to grant enforcement power and functions to the Personal Information Protection Commission ("PIPC"). <https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-outlook-and-review-2019/>

Relationship with the EU. South Korea is changing its data privacy laws in a bid to secure an agreement with the EU to let South Korean digital communications providers move data out of the bloc, and the country is also preparing to try to win a broader adequacy decision from the EU by introducing proposed amendments to its Personal Information Protection Act. <https://news.bloomberglaw.com/privacy-and-data-security/south-korea-privacy-law-changes-may-help-eu-data-transfer-talks>. South Korea updated its Act on the Promotion of IT Network Use and Information Protection ("Network Act") in December 2018. As of March 19, 2019, the law requires digital communications providers who deal with South Korean data but who have no physical presence in the country to establish a domestic representative to deal with data protection

issues. South Korea has applied for a narrow adequacy decision for the digital communications industry by updating the sector-specific privacy law.

Lawsuits. A number of lawsuits have been brought by citizen watchdog groups in South Korea to address privacy breaches.

- **Lawsuit against e-commerce site Auction** (Supreme Court, 2013da43994, decided December 2, 2015). The server of the popular e-commerce site Auction was hacked in 2008, and a massive amount of user information was breached (including names, Resident Registration Numbers, account numbers, and addresses of the site's users). Information on over 10 million users was leaked and, among these users, approximately 146,600 users brought lawsuits against the company, claiming damages for negligence. The Supreme Court ruled that Auction did what was reasonably expected to be done to prevent the data breach and could not be held liable for negligence. See <https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL2-N7.pdf> at 14.
- **Lawsuit against E-Mart and Lotte Mart.** In February 2015, the YMCA, a core civil organization in Korea, sued major retail market leaders E-Mart and Lotte Mart (the first and the third largest local retail stores respectively) on suspicion of a breach of the Personal Information Protection Act in a complaint filed with the Seoul Central District Prosecutor's Office. YMCA argued that between 2012 and 2013 the two retail chains had collected personal information by holding sweepstakes and selling participants' information to insurance companies. Following investigation, prosecutors concluded that these incidents were the responsibility of the agents in charge of the sweepstakes procedure. It was revealed that the person who led the event at E-Mart illegally collected the information of 4.67 million customers and sold it to insurance companies for 7.2 billion won. A person related to Lotte Mart obtained 24 million customers' personal information through the events and earned 23 billion won by selling it to the insurance companies. See Song, D.H. & Son, C.Y. (2017). Mismanagement of personally identifiable information and the reaction of interested parties to safeguarding privacy in South Korea. *Information Research*, 22(4), paper 770. Retrieved June 9, 2019, from <http://InformationR.net/ir/22-4/paper770.html> (Archived by WebCite® at <http://www.webcitation.org/6vNxtks82>). This case explicitly exposed the loopholes in the management of personal data protection by employees of the retailers since the retailers argued that they were not involved in the events but only rented a “shop section” to insurance companies and advertising agencies.
- **Lawsuit against Homeplus.** A 2015 lawsuit was brought against Homeplus, South Korea's second-largest retailer, with more than 1,000 outlets across the country, for selling the personal information of its customers collected through a raffle event to an insurance company. Homeplus collected personal information of its customers through contest registration forms and membership registration materials. In addition to making internal use of the information, Homeplus bundled customer data and sold it to third-party insurance companies. Participating customers received written disclosure that their information could be sold to insurance companies, though the relevant disclosure was printed in one-millimeter characters. All three enforcement tools were applied against

Homeplus: the Korean Fair Trade Commission instigated an administrative proceeding, customers filed suit seeking civil remedies, and six Homeplus executives (including the CEO) were prosecuted for violations of privacy law.

- All six executives were acquitted, and Home Plus was found to be not guilty in January 2016 based on the rationale that their duty of disclosure had been met. On appeal, the higher court affirmed the lower court's decision based on the same rationale. <http://www.informationr.net/ir/22-4/paper770.html>. However, the Korean FTC assessed a fine against the company in the sum of 435 million Korean won (approximately 400,000 U.S. dollars). See <http://koreajoongangdaily.joins.com/news/article/Article.aspx?aid=3003608>.
- **Investigation of and fine imposed on Lotte Home Shopping.** In August 2016, the Korea Communications Commission, the Korean communications regulatory body, announced results of their investigation into illegal data trade by corporations. It found that Lotte Home Shopping, one of the big-five home shopping TV channels in Korea, had illegally sold 3.24 million won of their customers' information to insurance companies between 2009 and 2014. The Commission imposed a 180 million won fine.
 - Although Lotte Home Shopping illegally gained 3.73 billion won in exchange for personal information but were fined only 180 million won. This case revealed the limitation of the punishment compared to the crime. It consequently raised politicians' awareness of the need for punitive damages to punish the non-state actors' illegal trade in data and brought about the adoption of a strong compensation system for damages.
 - In response to the Lotte Home Shopping incident, the opposition People's Party made an official statement arguing that the current punishment for the illegal trading of data was too weak, reducing the incentive for effective data management. For this reason, it argued that "an adoption of a punitive damage system is imperative in order to prevent personal information leaking" (Jung, 2016, para. 8).
- **U.S. Lawsuit.** On May 10, 2019, Facebook filed a lawsuit against South Korean analytics firm Rankwave for abusing its developer platform's data and refusing to cooperate with a mandatory compliance audit and a request to delete data (*Facebook, Inc. v. Rankwave Co., Ltd.*, Case no. 19-CIV-02592 (CA Superior Ct., San Mateo, May 10, 2019) <https://techcrunch.com/wp-content/uploads/2019/05/TechCrunch-Facebook-Rankwave-Lawsuit.pdf>; see also <https://techcrunch.com/2019/05/10/facebook-rankwave-lawsuit/>). Facebook's lawsuit centers around Rankwave's offering to help businesses build a Facebook authorization step into their apps so they can pass all the user data to Rankwave, which then analyzes biographic and behavioral traits to supply user contact info and ad targeting assistance to the business. Rankwave also apparently misused data sucked in by its own consumer app for checking a user's social media "influencer score". See <https://techcrunch.com/2019/05/10/facebook-rankwave-lawsuit/>. It's unclear if the South Korean government also plans to act. Rankwave is a subsidiary of one of the largest

conglomerates in South Korea: CJ Group. See <http://www.businesskorea.co.kr/news/articleView.html?idxno=31759>.

3. Hong Kong

Overview. Hong Kong's Personal Data (Privacy) Ordinance ("PDPO") dates back to 1995. The Office of the Privacy Commissioner for Personal Data ("PCPD") is responsible for privacy and data enforcement.

PCPD Investigations. The PCPD has undertaken a number of investigations in response to various data and privacy breaches.

- **Investigation of Hong Kong Broadband Network Limited** (a Hong Kong telecom company). It was discovered on April 16, 2018, that the company's inactive-database leak exposed 380,000 customers' data including their names, email addresses, HKID card numbers, and some data from 43,000 credit cards. The PCPD published its report on February 21, 2019 and stated that the company must create a clear data-retention policy and erase consumers' personal data held longer than that policy allows – specifically, the company must write a clear data retention policy within 90 days that specifies how long it will retain personal data that is no longer necessary to accomplish the purpose for which it was collected. <https://news.bloomberglaw.com/privacy-and-data-security/hong-kong-telecom-company-told-to-create-clear-data-policies>. The Hong Kong Broadband Network must also devise a data security policy to make sure it regularly reviews user privileges and remote access security, and it must also create procedures to clarify the steps and time limits for deleting personal data in inactive databases after a system migration. https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/PCPD_Investigation_Report_R19-5759_Eng.pdf
- **Investigation of WWPKG (Travel Agent).** In November 2017, hackers infiltrated the database of the travel agency gaining access to client names, HKID cards, passport numbers, phone numbers, email addresses, credit card information, mailing addresses, and purchase history. See <https://www.scmp.com/news/hong-kong/economy/article/2118745/hack-attack-popular-hong-kong-travel-agent-wwpkg-puts>. It is unclear whether there has been an enforcement action against WWPKG (there is no compliance report published by the PCPD yet), but the police were involved in helping the agency arrest the hackers. <https://www.scmp.com/news/hong-kong/law-crime/article/2119251/hong-kong-police-unlock-wwpkg-travel-agency-customer-data>.
- **Investigation of Vtech (Toy Maker).** In November 2015, VTech collected digital data on children without parents' permission and failed to keep that information secure from hackers. Vtech paid \$650,000 to settle charges from the U.S. Federal Trade Commission. The PCPD also initiated a compliance check and stated that if Vtech were to fail to comply with an enforcement notice they would be liable to pay a fine of \$50,000 and a penalty of \$1,000. https://www.pcpd.org.hk/english/news_events/media_statements/press_20151201c.html.

- **Investigation of Hong Kong shopping mall membership programs.** On April 25, 2019, the PCPD published a report stating that it had found that Hong Kong malls had instituted good data practices for its collection of personal data and recommended generally that organizations incorporate good data governance practices for the future. https://www.pcpd.org.hk/english/enforcement/commissioners_findings/compliance_checks_reports/files/CCR_Shoppingmallonlinepromotion_E.pdf
- **Cathay Pacific 2018 Data Breach.** In 2018, over a 7-month period, Cathay Pacific leaked data about 9.4 million passengers, including their passport numbers, HKID numbers, and credit card numbers (403 expired credit card numbers and 27 credit card numbers with no CVV). The PCPD announced in October 2018 that it would initiate a compliance investigation. It appears that any result of this investigation is not yet published. <https://www.reuters.com/article/us-cathaypacific-cyber/cathay-pacific-faces-probe-over-massive-data-breach-idUSKCN1NB0JY>

4. Japan

Overview. In Japan, the Act on Protection of Personal Information (“PIPA”) currently in force was enacted on May 30, 2003 and came into effect in 2005. <https://www.alstonprivacy.com/may-30-fast-approaching-ready-compliance-amended-act-protection-personal-information-japan/>. The Act has been amended several times, and in January 2016, the Act was amended to establish the Personal Information Protection Commission (“PIPC”), Japan’s own version of a supervisory authority for data protection. The PIPC has the power to monitor compliance and to enforce the provisions of PIPA. The English translation of the enforcement rules is available here: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf.

PIPC’s website does not include information about any recent enforcement actions, and none seem to be available elsewhere online. This is relatively surprising since, on January 23, 2019, the European Commission adopted its decision finding that the level of data protection in the EU and Japan are equivalent. https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf.

Google “Right to be Forgotten” lawsuit. In 2017, the Japanese Supreme Court rejected a plaintiff’s demand that a Google web search bringing up reports of his arrest for child prostitution be removed, overturning the lower Tokyo district court’s order for Google to omit these search results. <https://www.wsj.com/articles/google-japan-case-raises-privacy-issues-1413981229> and <http://fortune.com/2017/02/01/googlepright-to-be-forgotten-japan/>.

5. The Philippines

Overview. The Philippines’ first comprehensive data protection law, the Data Privacy Act of 2012 (“DPA”), took effect in September 2012. In March 2016, the National Privacy Commission (“NPC”) the body responsible for enforcing and monitoring compliance with the DPA was formed. While the NPC has opened several investigations, it does not seem to have issued any fines or any injunctive relief.

NPC Investigations.

- **Hearings on Online Lending Operators Practices.** The NPC is presently (May 2019) handling a total of 485 complaints against operators of online lending applications that allegedly misused the borrower's information, including the disclosure of unpaid balances to other people. At least 235 cases were formally pursued by complainants and are now the subject of NPC hearings. Culpability has not yet been adjudicated, but the NPC has stated that the online lending entities may either be enjoined from operating or they may be required to pay damages to the affected individuals. <https://www.privacy.gov.ph/2019/05/npc-conducts-hearings-on-48-online-lending-apps-after-over-400-harassment-complaints/>.
- **Investigation of the Department of Foreign Affairs.** In January 2019, the NPC investigated whether the Department of Foreign Affairs had compromised personal passport data and allowed an unauthorized third party to obtain access to this data. Specifically, the NPC investigated whether a private contractor used by the Department of Foreign Affairs had caused this breach. The NPC preliminarily found that this data had not been compromised. <https://www.privacy.gov.ph/2019/01/npc-opens-passport-data-probe/>.