Data Privacy Laws and Blocking Statutes: Five Practical Strategies for Counsel

By David Yerich (United Health Group), Christopher Wall (HaystackID) and Ashish Prasad (HaystackID)

It's not an exaggeration to say data privacy has become one of the biggest and most controversial issues in the digital era, and the laws enacted—which are constantly in flux—are something for legal counsel to keep a watchful eye on. While the United States is generally regarded as trailing Europe and other parts of the world when it comes to privacy and data protection regulation, corporations and their counsel need keep up with the developing corpus of data privacy laws worldwide. The steady advance of these laws all around the world has a material impact on how counsel handles litigation or regulatory discovery in international cases. In this article, we discuss the effect of data privacy laws and corresponding blocking statutes on U.S.-based corporations and offer some practical strategies for counsel when dealing with international investigations and litigation.

Data Privacy Laws

Data privacy laws prohibit misuse or disclosure of private individuals' data. At least 89 countries have enacted data privacy laws, and more countries are expected to enact their own data privacy laws in coming years.

With the General Data Protection Regulation (GDPR), the European Union (EU) has arguably played a leading role in data protection regulation. A brief overview of how the EU developed that leading role is instructive. Europe has a fraught history with use of personal information, and in particular the use of information about race, religion, and personal and real property ownership. After World War II, that general mistrust for large data aggregations continued, and in 1950 the right to privacy was included in the European Convention on Human Rights. In the mid-1970s, Germany and France established some of the first privacy laws in Europe, and with the establishment of the EU came a greater effort to harmonize

the laws of EU member states, including laws protecting individuals' rights to their personal information. To that end, in 1995 the EU implemented the Data Protection Directive 95/46/EC, which required every member state to adapt the Directive's privacy framework to their national regulations.

Responding to the reported desire of more than 90% of Europeans to harmonize data protection rights across the EU,[1] in January 2012 the European Commission proposed data protection reform, including changes to Directive 95/46/EC. The changes were intended to further harmonize the various data protection laws currently in place in the EU member states, protect personal data "[i]n today's new, challenging digital environment,"[2] and "make Europe fit for the digital age."[3] The GDPR (Regulation 2016/679) entered into force on May 24, 2016; however, the regulation did not fully take effect until May 25, 2018. The two-year implementation period was intended to give businesses and regulators sufficient time to put into place the steps necessary to comply with new obligations under the broad and far-reaching regulation.[4]

The GDPR was certainly groundbreaking for the EU, but the regulation has had an equally profound effect on data protection in other jurisdictions around the world. Some of those countries that have passed GDPR-like data protection laws include Argentina, Bahrain, Brazil, Israel, Japan, Kenya, Mauritius, New Zealand, Nigeria, South Africa, South Korea, Qatar, Switzerland, Turkey, Uganda, the UK and Uruguay.[5] In the US, 3 days after the GDPR took effect, the State of California passed the California

---

[1] *Protection of Personal Data*, EUROPEAN COMM'N, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en (last visited Nov. 25, 2022).

[2] European Comm'n, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM (2012) 09 final (Jan. 25, 2012), *available at* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF.

[3] *Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market*, EUROPEAN COMM'N (Dec. 15, 2015), https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6321.

[4] *Id.*

[5] In 2000, Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA). While PIPEDA pre-dates passage of the GDPR, its protections have been deemed "adequate" (with some exceptions) by EU standards for import into Canada of EU-residents' personal information.

Consumer Privacy Act (CCPA), which took effect on January 1, 2020, and granted California residents many rights similar to those granted EU residents under the GDPR.

An important consideration under the GDPR (and GDPR-like laws in other parts of the world) involves cross-border data transfers. The GDPR permits transfers of European residents' personal data to countries that are deemed to have "adequate" data protections in place, and only permits transfers to inadequate countries if specific transfer mechanisms are used to effect the transfer.[6] The EU currently includes the U.S. among those countries that do *not* have adequate safeguards in place for protecting individuals' data. Thus, where U.S. discovery (or discovery in any other inadequate jurisdiction) potentially involves data from a GDPR-regulated jurisdiction, lawyers need to look to one of the EU-sanctioned transfer mechanisms to transfer the protected data.

A Safe Harbor and a Privacy Shield

Practically speaking, a country deemed to provide "adequate data protections" acts as an extension of European territory so far as data protection is concerned. One innovative approach to a finding of adequacy, especially given the importance of the free flow of information between the U.S. and Europe, was to establish a legal framework to regulate exchanges of personal data for commercial purposes between the EU and the U.S.

The first attempt at creating such a framework was crafted between 1998 and 2000 and would become known as the Safe Harbor. Under the Safe Harbor, U.S. companies could self-certify that they adhered to EU data protection requirements and thus transfer data freely between the EU and U.S. at

[6] As of December 17, 2021, the European Commission recognizes Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, and Uruguay as offering adequate levels of data protection. *Adequacy Decisions*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Nov. 25, 2022).

least among those commercial organizations that had put the protections in place to allow for safe and compliant transfers of personal information under Directive (95/46/EC) and had self-certified to that effect.[7] Unfortunately, a 2015 decision in the Court of Justice of the European Union (CJEU) closed that safe harbor.

In *Maximillian Schrems v. Data Protection Commissioner* (commonly known as *"Schrems I*"), the court invalidated the Safe Harbor self-certification framework that U.S. companies had been using to conduct data transfers from the EU to the United States.[8] Almost immediately after the court issued the *Schrems* decision, the European Commission and the U.S. Government began work on a new framework. On February 2, 2016, they reached agreement[9] and five months later the EU member states approved,[10] and the Commission adopted, what became known as the EU-U.S. Privacy Shield.[11]

Like the Safe Harbor, the Privacy Shield was a self-certification framework for data transfers between two commercial entities and required that companies submit to and demonstrate robust compliance with Privacy Shield principles, including limiting the collection of personal information, adhering to tightened conditions for onward data transfers, and ensuring compliance with handling, processing and other requirements established by European Data Protection Authorities. But also like the Safe Harbor, the Privacy Shield fell under legal challenge. In *Data Protection Commissioner v. Facebook*

---

[7] *U.S.-EU Safe Harbor Framework Documents*, LIBRARY OF CONG. WEB ARCHIVES (Apr. 5, 2015), http://webarchive.loc.gov/all/20150405033356/http://export.gov/safeharbor/eu/eg_main_018493.asp

[8] C-362/14, *Maximillian Schrems v. Data Prot. Comm'r*, ECLI:EU:C:2015:650.

[9] *EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield*, EUROPEAN COMM'N (Feb. 2, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216.

[10] *Statement by Vice-President Ansip and Commissioner Jourová on the Occasion of the Adoption by Member States of the EU-U.S. Privacy Shield*, EUROPEAN COMM'N (July 8, 2016), https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_2443.

[11] *European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows*, EUROPEAN COMM'N (July 12, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461.

Ireland (known as *Schrems II*),[12] the CJEU determined that the protections afforded by the Privacy Shield were inadequate and thus invalidated the EU-U.S. Privacy Shield.[13]

As of this writing, the EU and U.S. have not agreed upon a new framework to replace the Safe Harbor or Privacy Shield; however, in March 2022 U.S. President Biden and EU Commission President von der Leyen announced an agreement in principle on a "Trans-Atlantic Data Privacy Framework" that will potentially again allow data to flow across borders in a GDPR-compliant manner.[14] On December 13, 2022, the European Commission moved toward adopting an adequacy decision for a new EU-U.S. Data Privacy Framework, specifically crafted to address the concerns raised by the Court in its July 2020 Schrems II decision.[15] The draft adequacy decision still needs to be reviewed by the European Data Protection Board (EDPB), and then approved by the individual EU Member States and the European Parliament. Assuming the draft survives that scrutiny, the Commission adopt and put into effect the final adequacy decision. At that point, US companies will again be able to self-certify compliance with GDPR privacy obligations and join the EU-U.S. Data Privacy Framework.

Binding Corporate Rules

Until a new privacy framework becomes reality, lawyers seeking to move data across borders will need another mechanism to do so. In some circumstances, binding corporate rules (BCRs) can meet the need. BCRs are sets of data protection policies that EU companies establish to permit personal data

[12] C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd.*, ECLI:EU:C:2020:559.
[13] Press Release No 91/20, Court of Justice of the European Union, *The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU-US Data Protection Shield* (July 16, 2020), https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.
[14] *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, THE WHITE HOUSE (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.
[15] Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US (December 13, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631

transfers outside the EU, but within a company or family of companies.[16] The rules must "include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data."[17] While that may not sound too different from the self-certification requirements under the Privacy Shield, the practical differences are significant. It is important to note that BCRs only cover intra-company transfers, and do not address transfers outside of the organization, as might be required during discovery.

Typically, the use of BCRs is limited to "large companies with wide-ranging data transfer obligations."[18] That is because the process of implementing BCRs can be complex and can take years to complete. Companies must submit binding corporate rules for approval from the data protection authority or authorities in the member states in which the company does business. The data protection authorities communicate their review of the submitted rules to the European Data Protection Board (EDPB), which then issues its opinion on whether the proposed binding corporate rules are sufficient. Only once the BCRs have been approved by the EDPB will the relevant member state data protection authorities approve the BCRs so that the company can use them as a mechanism for intra-company transfers.

Standard Contractual Clauses

With the demise of the Privacy Shield and the unwieldiness of BCRs, standard contractual clauses (SCCs) have become the go-to mechanism for cross-border data transfers. SCCs are standard contractual

[16] Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, Recital 110, *available at* https://gdpr.eu/recital-110-binding-corporate-rules/.

[17] *Id.*

[18] Duane C. Pozza & Joan Stewart, *Cross-Border Data Transfer Mechanisms in Flux as Court of Justice for the European Union Invalidates Privacy Shield*, WILEY REIN LLP (July 16, 2020), https://www.wiley.law/alert-Cross-Border-Data-Transfer-Mechanisms-in-Flux-as-Court-of-Justice-for-the-European-Union-Invalidates-Privacy-Shield.

terms and conditions that both the data exporter and the data importer agree to, and effectively bind both parties to provide adequate safeguards to the data subject to transfer. The SCCs themselves are approved by the European Commission, and for the SCCs to remain effective the clauses themselves must not be altered. It is now common, however, for the SCCs to be incorporated into a Data Processing Agreement or other contract, which can add additional data protection safeguards so long as those additional safeguards do not contravene the SCCs or diminish the data protection rights of the individuals the SCCs were designed to protect.

While *Schrems II* did not invalidate the use of SCCs, it did give EU regulators pause, and in June 2021 the European Commission issued updated SCCs which replaced the old SCCs that were adopted under the Data Protection Directive, with the goal of ensuring—post *Schrems II*—that the rights and freedoms of EU individuals are upheld.[19] The new SCCs include provisions to provide transparency and notification controls, and address the potential for government requests for access to transferred data. To that end, for every transfer, the new SCCs require both the exporter and the importer to conduct and document a Transfer Impact Assessment (TIA). The basis for these TIAs comes from the European Court of Justice. In *Schrems II*, the court stated that, even where the transfer mechanism is SCCs and the parties to the transfer have contractually obligated themselves to abide by data protection principles, it still falls to those parties "to verify, on a case-by-case basis and, where appropriate, . . . whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguard to those offered by those clauses."[20] There is no "standard" TIA issued by the Commission for use in assessing the risk of a transfer; nor is there an acceptable "score" one must receive on a TIA in order to conduct a

[19] *European Commission Adopts New Tools for Safe Exchanges of Personal Data*, EUROPEAN COMM'N (June 4, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.
[20] *Schrems II*, ECLI:EU:C:2020:559, ¶ 134.

transfer. The requirement is that a TIA be completed, and that in doing that assessment the transferring party identifies the risks and any mitigations to those risks associated with the proposed transfer.

As of this writing, in most cases SCCs provide the most convenient mechanism for data transfer for purposes of US discovery and provide a standard of data protection for data moved from countries that have "adequate" protections in place to those, like the U.S., that do not, and with the TIA can help ensure that personal data is protected to a level that is acceptable under the GDPR.

Finally, lawyers seeking to transfer data from the EU or from other jurisdictions with GDPR-like data protection laws should note that the GDPR does not prohibit more stringent data protection regulations for topics such as the age of consent, data protection officer designation, employment-related data protection, and breach notification obligations. Similarly, other countries that have enacted GDPR-like privacy laws have adjusted their regulations to meet their specific needs. Those localized protections can add another wrinkle to lawyers' efforts to move data from such jurisdictions to the US for purposes of discovery.

Blocking Statutes

When it comes to data transfers for purposes of U.S. discovery, the GDPR and its transfer restrictions are not the only hurdle. Another way that individual countries have adapted data protection laws to their own needs is through implementation of blocking statutes, largely in response to broad American discovery requirements. Broadly speaking, a blocking statute is a law in one jurisdiction intended to prevent application in that jurisdiction of a law of a second jurisdiction.

In the data protection context, blocking statutes vary in their scope and enforcement, but all have the underlying goal of preventing non-U.S. nationals' acquiescence to U.S. discovery requests that may

otherwise result in those foreign nationals' personal information being brought to the U.S.[21] While data privacy laws aim to protect individuals' data privacy, blocking statutes are intended to protect the sovereignty of the state and its citizens from foreign litigation.[22]

Foreign nationals often cite a blocking statute to avoid complying with a U.S. discovery request or to avoid sanctions for failing to comply.[23]

France's blocking statue, oft cited as a prime example of the blocking statue conflict, requires the use of the cooperation mechanisms provided for by the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (the Hague Evidence Convention) before anyone can engage in discovery under a foreign judicial system, including that in the U.S. Together with France's data protection laws, the French blocking statute presents a very real challenge for transferring potentially relevant data to the United States for purposes of litigation discovery.[24]

***Aérospatiale* Case Leads to Balancing Test for U.S. Courts**

Blocking statutes do not always excuse foreign nationals from having to comply with a U.S. discovery order, and these statutes often have limited effect helping foreign nationals avoid producing documents. The U.S. Supreme Court has weighed in on blocking statutes generally. In *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, ("*Aérospatiale*"), the U.S. Supreme Court addressed blocking statutes, and laid out a balancing test for courts to use in determining

[21] *Compagnie Francaise d'Assurance Pour le Commerce Exterieur v. Phillips Petroleum Co.*, 105 F.R.D. 16, 30 (S.D.N.Y. 1984).
[22] M.J. Hoda, *The* Aérospatiale *Dilemma: Why U.S. Courts Ignore Blocking Statutes and What Foreign States Can Do About It*, 106 CAL. L. REV. 231, 238 (2018).
[23] 71 Am. Jur. Trials 1 (Originally published in 1999) § 43 (Sept. 2022 update).

[24] Thomas Rouhette & Ela Barda, *The French Blocking Statute and Cross-Border Discovery*, 84 DEF. COUNS. J. 1 (July 2017), *available at* https://www.iadclaw.org/defensecounseljournal/the-french-blocking-statute-and-cross-border-discovery/; Constantin Achillas, et al., *The French Blocking Statute: Effective Protection Against Cross-Border Discovery?*, BRYAN CAVE LLP (June 2014), https://www.bclplaw.com/a/web/2180/ComLit-Alert-ENG-6.19.pdf.

whether to order cross-border discovery.[25] (The factors in this balancing test are also articulated in the Restatement (Third) of Foreign Relations Law § 442(c) (1987)). The Court noted that the Hague Evidence Convention dictated the procedures that must be followed for pre-trial discovery, and emphasized that not following those procedures would hurt both domestic and foreign litigants. Nonetheless, with respect to the blocking statute the Court found that "such statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence, even though the act of production may violate that statute."[26] In determining how to strike the correct balance between competing laws, the court looked to the comity analysis as outlined in the Restatement of Foreign Relations Law. That analysis includes several factors:

> (1) the importance to the . . . litigation of the documents or other information requested;
>
> (2) the degree of the 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 interests of the United States, or compliance with the request would undermine interests of the state where the information is located.[27]

In the decades since *Aérospatiale,* courts have often applied the factors outlined there, and have usually, but not always, found that the U.S. discovery interests outweigh the foreign interests inherent in the blocking statute. U.S. courts have noted that blocking statutes have not been regularly enforced, but in at least one case the defendant was ordered to produce documents which resulted in a French lawyer being convicted and fined €10,000 for violating the blocking statute.[28]

---

[25] *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for the S Dist. of Iowa*, 482 U.S. 522, 544 n.28 (1987).
[26] *Id.* at 544 n.29.
[27] *Id*. at 544, n. 28.
[28] *Strauss v. Credit Lyonnais, S.A.*, 242 F.R.D 199 (E.D.N.Y 2007); Article 29 Working Party, *Working Doc. 1/2009 on Pre-trial Discovery for Cross Border Civil Litigation*, p.5, n.3, Doc. No. 000339/09/EN WP 158 (Feb. 11, 2009).

Practical Strategies for Counsel

Confronting data privacy laws and blocking statutes during discovery can be daunting to both newcomers and seasoned practitioners. Below are some strategies for counsel to follow when confronted with data privacy laws and blocking statutes.

1. **Be cognizant of the data privacy laws specific to the country or countries you are dealing with.** Online data privacy maps can help lawyers compare different countries' approaches to data protection and identify where data transfers issue may lie and what steps to take to address them.[29] Where significant hurdles to data transfers arise, it is always sound strategy to engage local counsel to navigate the privacy landscape.[30]
2. **Consider the Sedona Conference practice pointers for conducting cross-border discovery.** The Sedona Conference is a nonprofit research and educational institute dedicated to moving the law forward "in a reasoned and just way."[31] The Sedona Conference offers several useful practice points for cross-border discovery, geared specifically to in-house counsel, but instructive to outside counsel as well. Its pointers include the following.
    a) Balancing the need for urgency in preserving information with the need to proceed deliberately in countries with comprehensive data protection laws.
    b) Identifying and defining privacy issues with opposing parties or regulators through outside counsel where possible.

[29] *See, e.g.*, *Data Protection Laws of the World*, DLA PIPER, http://dlapiperdataprotection.com/#handbook/law-section/c1_EG; *Data Protection Around the World*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, https://www.cnil.fr/en/data-protection-around-the-world.
[30] The Sedona Conference, *The Sedona Conference Practical In-house Approaches for Cross-border Discovery & Data Protection*, 17 SEDONA CONF. J. 397, 424 (2016), *available at* https://thesedonaconference.org/sites/default/files/publications/Practical%20In-House%20Approaches%20for%20Cross-Border%20Discovery%20%26%20Data%20Protection.17TSCJ397.pdf .
[31] *Homepage*, THE SEDONA CONF., https://thesedonaconference.org/ (last visited Nov. 25, 2022).

c) Setting up transparency "checkpoints," beginning with preservation and continuing through the life of the matter, to avoid revocation of consent.

d) Planning a successful in-country collection with detailed surveys of appropriate systems well in advance of any discovery deadlines.

e) Using the processing stage of discovery as an opportunity to balance compliance with both discovery and data protection laws.

f) Considering ways to limit the production of protected data; when production of protected data is necessary, safeguards can be established to demonstrate due respect for both discovery and data protection laws.[32]

3. **Consider seeking support of the foreign embassy or consulate and look for alternative solutions that can accommodate both the importing and exporting jurisdictions.** A foreign party from which discovery has been requested may seek the assistance of that country's consulate or embassy to support the position that there is a "national interest" in keeping the information confidential. In addition, the party should look for alternative solutions that can accommodate the discovery laws of both jurisdictions, such as the Hague Evidence Convention.[33]

4. **Know the data: Where it is, what it is, and how important it is to the finder of fact.** In a slight variation to the best evidence rule, before making an international discovery request, counsel should make sure that the foreign evidence in question is not available somewhere in-country. Counsel should also determine how important the evidence is to the case: is it worth the time, effort, risk and expense of complying with data protection and privacy laws and blocking statutes?

[32] The Sedona Conference, *supra* note 31, at 461–62.
[33] 3 Bus. & Com. Litig. Fed. Cts. § 29.21 (5th ed.).

5. **Be aware of the impact of and developments following the *Schrems* decisions.** The *Schrems* decisions changed the analysis counsel must undertake when considering cross-border data transfers for discovery.[34] The Safe Harbor is no longer safe and the Privacy Shield won't protect you. SCCs typically present the safest and most streamlined mechanism for data transfers from GDPR and GDPR-like jurisdictions. Counsel must be certain to use the latest SCCs available on the EU's website[35] and conduct the appropriate data transfer impact assessment prior to each transfer. Counsel attempting to transfer data from the EU to the U.S. should be fully aware of the ramifications of the *Schrems* decisions, and keep abreast of developments, challenges and decisions related the adequacy of the various transfer mechanisms for data.

Conclusion

Navigating data privacy laws and blocking statutes requires a methodical, informed approach. The timing and content implications of privacy laws and blocking statutes can have a significant impact on litigation that involves cross-border discovery.

[34] *See generally Schrems I*; *Schrems II*.
[35] *Standard Contractual Clauses for International Transfers*, EUROPEAN COMM'N (June 4, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.