2-1-2016

To Discovery and Beyond: A Comprehensive Look at Argentina's Data Protection Laws

Sean McCleary

To Discovery and Beyond: A Comprehensive Look at Argentina's Data Protection Laws

Sean McCleary*

This article strives to shed light on the interplay between discovery practice under the Federal Rules of Civil Procedure, Argentina's data protection laws, and the ever-present possibility of discovery sanctions. For all intents and purposes, data protections laws serve as a double-edged sword that seek to protect an individual's privacy; however, data protection laws were not designed with litigation in mind. And because of that, it can be difficult for an Argentine company to comply with a discovery request that would implicate an individual's data privacy under Argentine law. In the end, it comes down to a balancing test. This article will explore the origins of data protections laws, the data protections laws in Argentina, discovery practice under the Federal Rules of Civil Procedure, and how Argentina's data protection laws can significantly impact discovery practice.

---

* Editor-in-Chief, Inter-American Law Review, 2014-2015. B.A., University of Florida 2011, J.D. *Cum Laude* University of Miami School of Law 2015. I want to thank my predecessor, Jamie Lynn Vanaria, and the 2015-2016 editorial staff for their tireless effort in helping this article come to publication. I am also deeply indebted to the Inter-American Law Review for providing me with a forum through which I could address these issues.

I. INTRODUCTION

The rise of cross-border transactions has been met with a rise in cross-border litigation. As American companies have increased business activity in Latin America and the European Union ("EU") they have also encountered data protection laws. When compared to other Latin American countries, Argentina presents a unique situation because it has comprehensive data protection laws that are similar to those in the EU[1] Additionally, Argentina and the U.S. have a trade relationship that is valued at $24.2 billion USD annually.[2] As globalization has accelerated in the past twenty years, it has become increasingly common for a U.S. party to file a domestic lawsuit against a foreign party.[3] The majority of these lawsuits are breach of contract actions. Almost inevitably, the involved parties will become immersed in pre-trial discovery.

---

[1] Aldo M. Leiva, *Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, 41 INT'L LAW NEWS 4, *available at* http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html.

[2] U.S. DEP'T. OF COMMERCE, *Doing Business in Argentina*, EXPORT.GOV (Oct. 23, 2015, 10:10 AM), http://export.gov/Argentina/doingbusinessinargentina/index.asp.

[3] *See* Lawyers for Civ. Justice et al., *Litigation Cost Survey of Major Companies*, 2010 Conference on Civil Litigation at Duke Law School (May 10-11, 2010), *available at* http://www.uscourts.gov/rules-policies/records-and-archives-rules-committees/special-projects-rules-committees/2010-civil

Pre-trial discovery is the "formal process of exchanging information between the parties about the witnesses and evidence [they will] present at trial."[4] Traditional discovery involved the exchange of hard-copy files and data. Today, discovery is increasingly conducted through the electronic exchange of information, a process known as e-discovery.[5] In many cases, pre-trial discovery may be outcome-determinative for either party.

Because many foreign jurisdictions have varying standards for the scope of pre-trial discovery, it is likely that many documents will be protected under either a blocking statute or a data privacy or data protection law.[6] The U.S. has permissive discovery standards compared not only to civil law regimes in the EU, but also to many Latin American countries such as Argentina.[7] What is largely considered standard pre-trial discovery in the U.S. is likely to be considered an invasion of privacy in the EU and Argentina. Many, if not most, EU members consider U.S. discovery standards to be invasive because EU members consider data privacy to be a fundamental right.[8] Paradoxically, although America has always placed a high value on privacy, its legal system encourages broad discovery procedures. Perhaps it is because pre-trial discovery is seen as an efficient way to

---

[4] AM. BAR ASS'N DIV. FOR PUB. EDUC., *How Courts Work*, AMERICANBAR.ORG, http://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/discovery.html (last visited Jan. 6, 2016).

[5] *Id.*

[6] Seth D. Rothman & Charles W. Cohen, *The Impact on U.S. Discovery of EU Data Protection and Discovery Blocking Statutes*, HUGHES HUBBARD (January 2013), http://www.hugheshubbard.com/Documents/Impact%20on%20U%20S%20%20Discovery%20of%20EU%20Data%20Protection%20and%20Discovery%20Blocking%20Statutes.pdf ("'Blocking Statutes' are statutes which prohibit the transfer of data for use in foreign proceedings unless the transfer complies with the Hague Evidence Convention.").

[7] William D. Wood & Brian C. Boyle, *Obtaining Foreign Discovery in U.S. Litigation*, 63 THE ADVOC. (Texas) 12 (2013).

[8] Council Directive No. 95/46/EC, O.J. L 281/31 (1995), *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. [hereinafter, EU Directive].

"encourage early disclosure and efficient settlement prior to trial."[9] Pre-trial discovery has even been vaunted as a means to provide "informational equity."[10] By contrast, in many civil law countries, discovery is a function that is best carried out by judges.[11] In their eyes, discovery is best carried out by the only person in the case whose duty is to be impartial.

This note has two aims: (1) to shed light on the labyrinth of discovery problems in Argentina and (2) to illustrate the impact that data protection laws have on U.S. entities conducting business in Argentina. For the purposes of highlighting the various discovery problems that may arise under Argentina's data protection laws, this note will explore the following hypothetical situations: (1) A lawsuit was filed in the U.S., thereby invoking U.S. discovery standards and (2) the Defendant was an Argentine party that has discoverable data in a physical or electronic form (electronically stored information or "ESI").

Part I of this note will provide a cursory understanding of the procedures for conducting cross-border discovery under U.S. discovery standards. In Part I, I will first examine the Hague Evidence Convention on the Taking of Evidence Abroad, as well as the problems associated with its interpretation. Part II of this note will discuss how data protection laws have impacted the ability of litigants to conduct discovery. Much of this discussion will center around the EU Directive (hereinafter, "Directive") and the Directive's influence on other nations to adopt data protection laws. Part III will specifically analyze the Directive's influence on Argentina's legislature, which prompted the country to create its own data protection

---

[9] *See* Marissa L. P. Caylor, *Modernizing the Hague Evidence Convention: A Proposed Solution to Cross-Border Discovery Conflicts During Civil and Commercial Litigation*, 28 B.U. INT'L L.J. 341, 363, 364-68 (2010), for further discussion on why pre-trial discovery in civil law countries is uncommon.

[10] *See generally* STEPHEN N. SUBRIN ET AL., CIVIL PROCEDURE: DOCTRINE, PRACTICE AND CONTEXT, 388-418 (3d ed. 2008) (explaining basic rules of discovery).

[11] Benjamin L. Klein, *Trust, Respect, and Cooperation May Keep Us Out of Jail: A Practical Guide to Navigating the European Union Privacy Directive's Restrictions on American Discovery Procedure*, 25 GEO. J. LEGAL ETHICS 623, 625 (2012) (See 625-28 for further discussion on the tensions between the U.S. and EU discovery dilemma.).

laws. Additionally, Part III will discuss the problems that Argentina's data protection laws present to U.S. litigators, which are similar to the problems that litigators face when dealing with European entities. Finally, Part IV will discuss some of the proposed solutions to resolve issues with cross-border discovery.

II. UNDERSTANDING THE GRAND SCHEME OF THINGS: U.S. DISCOVERY ABROAD

When domestic and foreign litigants enter pre-trial discovery in a U.S. jurisdiction, the court has options to mandate the foreign entity to either freeze or to produce discoverable materials. Under the Federal Rules of Civil Procedure (hereinafter, "FRCP"), a litigant may request unprivileged data that is "relevant to the claim or defense of any party."[12] In the past 15 years, e-discovery has been at the forefront of pre-trial discovery for civil litigation. Because we are moving further towards a paperless world, I will focus most of the discussion on e-discovery versus traditional discovery.

The following provides a brief understanding of e-discovery: a party transfers data to a vendor, which results in the creation of thousands, if not millions, of pages of information. In order to narrow the amount of relevant data, the information may be sorted and filtered by either a simple keyword search, "boolean search," or through "predictive coding."[13] Predictive coding is a computer-assisted search function that has only recently been permitted by courts.[14] It can be cost-effective because it can process large volumes of data with minimal input by those that are searching the data.[15]

---

[12] FED. R. CIV. P. 26(b)(1).

[13] Michael Lopresti, *What is Predictive Coding?: Including eDiscovery Applications*, KM WORLD (Jan. 14, 2013), http://www.kmworld.com/Articles/Editorial/What-Is- . . . /What-is-Predictive-Coding-Including-eDiscovery-Applications-87108.aspx.

[14] *See* Global Aerospace Inc., v. Landow Aviation, L.P., Case No. CL 61040 (Va. Cir. Ct. 2012).

[15] *See* Lopresti, *supra* note 13.

A. *Hague Evidence Convention and the U.S.'s Disdain for it*

Prior to 1987, U.S. litigants seeking to request evidence from a foreign entity were constrained by the Hague Evidence Convention on the Taking of Evidence Abroad (hereinafter, "Hague Convention").[16] The Hague Convention was established in order to "reconcile the differing legal philosophies of the Civil Law, Common Law, and other systems with regard to taking evidence."[17] The Hague Convention, which the U.S. and Argentina are both parties to, allows states seeking evidence to send a Letter of Request to the state in which the evidence is located.[18] Article 1 of the Hague Convention allows U.S. litigants to obtain evidence from foreign witnesses much to the same extent that the litigant would be able to obtain that evidence in the U.S.[19]

Soon after the Hague Convention was established, it began to unravel at the seams—in one fell swoop, the Convention allowed countries to opt-out of pre-trial discovery.[20] Per Article 23, the Hague Convention allowed signatory nations to sign a limiting reservation that would disallow the execution of Letters of Request for purposes of pre-trial discovery.[21] Argentina has exercised this right and it has disallowed pre-trial discovery under the Hague Convention, forcing litigants to search for an alternative means to make pre-trial discovery requests.[22] Despite its aspirational attempt to create a unified and global system for requesting evidence from abroad, many have argued that the Hague Convention has failed to achieve

---

[16] Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa, 482 U.S. 522, 541 (1987) [*hereinafter* Aerospatiale].

[17] *See* Caylor, *supra* note 9, at 344 (quoting Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522 (1987) (Blackmun, J., concurring)).

[18] Argentina was not an original party to the Convention, but it ratified the Convention on May 8, 1987. *See* The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, March 18, 1970, 23 U.S.T. 2555 T.I.A.S. 7444 [*hereinafter* Hague Convention].

[19] Caylor, *supra* note 9, at 344.

[20] *See id*. at 344-46 (noting that the addition of Limiting Reservations defeats the purpose of the Hague Convention).

[21] David W. Ogden & Sarah G. Rapawy, *Discovery in Transnational Litigation: Procedures and Procedural Issues*, ABA Business Law Section Spring Meeting, 2007, at 12, *available at* http://apps.americanbar.org/buslaw/newsletter/0058/materials/pp1.pdf.

[22] *Id.*

its goal.[23]Arguably, the Hague Convention failed because of its eagerness to please European constituents.

Realizing its lack of utility, U.S. courts needed a solution to circumvent the Hague Convention for a number of reasons. In addition to the execution of limiting reservations, other features of the Hague Convention also proved to be time-consuming. Letters of Request often take a considerable amount of time to process and, in many cases, they prove to be fruitless.[24] As a result, critics of the Hague Convention point out that it is poorly suited for the U.S.'s globalized economy.[25] The need for efficient discovery is ever-present in a world where cross-border litigation is commonplace.

The U.S. Supreme Court added the final nail in the Hague Convention's proverbial coffin by deeming its use discretionary.[26] In 1987, the U.S. Supreme Court ruled in *Societe Nationale Industrielle Aerospatiale* (hereinafter, "*Aerospatiale*") that the Hague Convention was not the exclusive means for gathering evidence abroad: the FRCP could be applied as well.[27] Here, litigants dissuaded by the Hague Convention's limiting reservations were offered an alternative avenue for making pre-trial discovery requests in countries

---

[23] *See* Caylor, *supra* note 9, at 372 ("The Hague Convention's inability to keep pace with globalization and its lengthy processing times have made it ineffective.").

[24] *See id.*

[25] *See* Moze Cowper & Amor Esteban, *E-Discovery, Privacy, and the Transfer of Data Across Borders: Proposed Solutions for Cutting the Gordian Knot*, 10 SEDONA CONF. J. 263, 272 (2009) (discussing why the Hague Convention on the taking evidence from abroad is anachronistic).

[26] This was a personal injury case stemming from a plane crash in Iowa. The French government owned the corporations that made the planes. The victims filed a lawsuit in the U.S. District Court for the Southern District of Iowa. The parties initially conducted discovery under the Federal Rules of Civil Procedure, but the defendants filed a motion for a protective order claiming that the Federal Rules are not applicable because the information sought was in France. The district court denied the motion. Upon appeal, the Eight Circuit affirmed. The case reached the Supreme Court with the question of to what extent to which a federal district court must employ the procedures set forth in the Hague Convention when litigants seek answers to interrogatories, the production of documents, and admissions from a French adversary over whom the court has personal jurisdiction. The Supreme Court ruled that the Hague Convention is not the exclusive means of obtaining evidence from a foreign litigant, and the Hague Convention does not need to be used first. *See* Aerospatiale, 482 U.S. at 541.

[27] *See id.*

that signed limiting reservations. The Court stated that the Hague Convention is "a permissive supplement, not a pre-emptive replacement, for other means of obtaining evidence abroad."[28] The Court concluded by establishing a five-factor balancing test for judges to use when determining whether it is appropriate to apply the FRCP. The factors to be weighed are as follows:

> (1) the importance to the . . . litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.[29]

Adding insult to injury, the Supreme Court stated that any mandatory application of the Hague Convention would undermine U.S. legal proceedings.[30] Just as the Hague Convention catered to the countries that wanted to avoid pre-trial discovery, the Supreme Court catered to U.S. litigants that needed to engage in it for purposes of developing their case. U.S. courts have also ruled that the FRCP can be applied in jurisdictional discovery.[31]

It is worth noting that, although the Hague Convention has been disfavored by U.S. courts, it is still widely used by other countries.[32] In defense of the Hague Convention, while it may be ineffective for pre-trial discovery and it may require a lengthy wait for a response, it does promote international cooperation.[33] Further, much of pre-trial discovery's purpose is to promote cooperation between oppos-

---

[28] *Id.* at 536.

[29] *Id.* at 544.

[30] *See* Caylor*, supra* note 9, at 346-48.

[31] *See* In re Vitamins Antitrust Litig., 120 F. Supp. 2d 45, 50 (D.D.C. 2000).

[32] James A.R. Nafziger, *Another Look at the Hague Evidence Convention After Aerospatiale*, 38 TEX. INT'L L.J. 103, 114 (2003).

[33] *See id.*

ing litigants. Additionally, the Convention has been useful for countries that have similar data privacy laws.[34] If two countries have signed limiting reservations under Article 23, then conducting cross-border discovery between the two countries should be fairly predictable because both countries have opted out of using Letters of Request in pre-trial discovery.

III. EU DIRECTIVE: A MODEL FOR DATA PROTECTION EVERYWHERE

In 1995, the European Commission adopted the EU Directive. The Directive was aimed at harmonizing divergent data protection regimes among EU member states in order to remove obstacles to the free flow of information and at "protect[ing] fundamental rights and freedoms, notably the right to privacy," by establishing minimum safeguards for the use of personal data.[35]

Prior to the Directive, the EU was scattered with varying data protection laws.[36] Data protection laws in some form or another have existed in Europe since at least 1970.[37] To help effectuate the goal of harmonization, the EU Directive creates obligations for data controllers[38] and data processors.[39] An example of the relationship between a data processor and data controller would be the relationship that exists between a corporation and the company that performs its payroll services.[40] The corporation is the data controller

---

[34] *Id.*

[35] EU Directive, *supra* note 8.

[36] Chuan Sun, *The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective*, 2 NW. J. TECH. & INTELL. PROP. 99, 100 (2003).

[37] Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1969 (2013).

[38] The EU Directive defines "controller" as "the person or entity that determines, alone or jointly with others, the purposes and the means of the processing of personal data." *See* EU Directive, *supra* note 8.

[39] *See id.*

[40] Bridget Treacy, *Working Party confirms 'controller' and 'processor' distinction*, HUNTON AND WILLIAMS, (Feb. 15, 2014), http://www.hunton.com/files/Publication/8fe272d1-d29c-4abd-85ae-17843d084da3/Presentation/PublicationAttachment/6d1be60b-be7d-413c-bd6f-6ee37c02c631/Treacy_controller-processor_distinctions.pdf.

because it is providing the scope to which its payroll company, its data processor, can process the corporation's data[41].

The EU Directive also acts to enforce individuals' rights.[42] Personal data is defined as "any information relating to an identified or identifiable natural person."[43] Put more simply, personal data can be information that relates to, among other characteristics, a person's physical, psychological, mental, or cultural traits.[44] The Directive's definition of personal data is extremely broad in scope. Due to the Directive's numerous data safeguards, the flow of information from EU states to the U.S. is greatly hindered—the Directive prohibits the transfer of data to a third country unless that country has adopted adequate data protection laws.[45]

Argentina is one of a few countries outside of the EU that has been deemed to have adequate data protection laws under the Directive's standard.[46] Because of its closely aligned data protection laws, one would expect that data transfers between the EU and an entity in Argentina would be easier than data transfers between entities with discordant data protection schemes, such as a transfer between the U.S. and Argentina.

A. *Data Transfers under the EU Directive*

The following represents three circumstances where data transfers are permitted under the EU Directive: (1) when there is consent by the data subject; (2) when it is necessary to meet a legal obligation; or (3) when it is necessary for the purposes of a legitimate interest.[47] However, these transfers are not intended for litigation purposes.

Consent can be required in many circumstances. For example, consent will likely be required when there is a request to retain data for longer than local laws allow.[48] Obtaining valid consent can be

---

41 *See id.*

42 *See* Chuan Sun, *supra* note 36, at 7.

43 EU Directive, *supra* note 8.

44 *See id.*

45 *See id.*

46 *See* Maxim Gakh, *Argentina's Protection of Personal Data: Initiation and Response*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 781, 782 (2006).

47 EU Directive, *supra* note 8.

48 *Id.*

challenging, particularly when dealing with a customer's information. For one, if the discovery request implicates the data of thousands of individuals, it is not reasonable for a company to request permission to process data from each customer, be it personal or sensitive. Of course, companies could request consent from customers as part of a business transaction—waivers are commonplace in modern business transactions. Under Argentina's data protection laws, consent is not necessary when it arises out of a contractual relationship.[49] In many cases, receiving consent is either too expensive or too time consuming. Because Argentina and EU members have a greater affinity for data privacy and protection, they will likely have lower expectation as to the quantity of potentially discoverable data.

Argentina is one of many countries outside of Europe that views data privacy as a fundamental right. As mentioned above, its data protection statutes have been deemed adequate, thereby meeting the EU Directive's standard.[50] This allows for data to flow more freely between Argentina and EU members.[51] In contrast, many foreign entities, particularly European countries, are hesitant to store data in the U.S. because of relatively permissive laws on data privacy.[52]

B. *Safe-Harbor Program*

After the EU directive was implemented, the Department of Commerce acted quickly to prevent a complete bulwark of data transfer between the EU and the U.S.[53] Realistically, neither the U.S.

---

[49] *See* PROTECCIÓN DE LOS DATOS PERSONALES [PERSONAL DATA PROTECTION ACT], Ley 25.326, Nov. 2, 2000 BOLETÍN OFICIAL [B.O.] 1 (Arg.) *available at* http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan044147.pdf (last visited Feb. 15, 2014) [hereinafter "PDPA"].

[50] *See* Gakh, *supra* note 46, at 781-82.

[51] *See id.* at 783.

[52] Following Edward Snowden's leak, details over the NSA's access to cloud computing sources has continued to deter non-U.S. companies from storing data in the U.S. *See* Andrea Peterson, *NSA Snooping Could Cost U.S. Tech Companies $35 Billion over Three Years*, WASHINGTON POST, (Feb. 12, 2014, 10:46 AM), http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/07/nsa-snooping-could-cost-u-s-tech-companies-35-billion-over-three-years/.

[53] U.S. DEP'T OF COMMERCE, *Safe Harbor*, EXPORT.GOV (Feb. 15, 2014), http://www.export.gov/safeharbor/.

nor the EU could survive in the absence of one another's economy.[54] In order to take initiative, the Department of Commerce established a Safe-Harbor program to help facilitate data transfers.[55] Under the Safe-Harbor program, which was approved by the EU in 2000, U.S. companies that maintained certain privacy policies would be deemed to have an adequate level of protection.[56] A downside to the Safe-Harbor program is that U.S. companies have had to cope with increased costs in maintaining adequate privacy policies.[57] The Safe-Harbor program was specifically designed and implemented in order to keep trade and commerce flowing—thus, it was not designed to aid litigants' discovery requests.[58] Initially, the program was unsuccessful.[59] Within a few years of its implementation, fewer than 500 companies had joined the program.[60] One significant reason for the program's lack of success was because of policy changes that followed its creation.[61] Contrary to what one might believe, following the attacks on September 11, 2001, the U.S. did not tighten data protection; instead, the U.S. legislature made it easier for the government to access data.[62] Meanwhile in the EU, data protection was getting stricter.[63] These diverging policies made it difficult for U.S. companies to comply with the program.

---

[54] *See* William H. Cooper, *EU-U.S. Economic Ties: Framework, Scope, and Magnitude*, CRS REPORT, (March 20, 2009).

[55] *Id.*

[56] Gakh, *supra* note 46, at 783-84.

[57] *See* Chuan Sun, *supra* note 36, at 100.

[58] *See id.* at 104 (discussing several ways that business can be disrupted between the EU and the U.S. in the absence of a data transfer scheme such as the Safe-Harbor Program).

[59] *See id.* at 110 (only twenty companies had joined the program within three months of its implementation).

[60] *See id.*

[61] *See id.* at 109.

[62] *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered titles of U.S.C.).

[63] *See* Chuan Sun, *supra* note 36, at 109; *see* Council Directive 2002/58, 2002 O.J. (L 201) 1 (EC).

IV. ARGENTINA'S PERSONAL DATA PROTECTION ACT

Argentina is a pioneer in the field of data protection by being the first country in Latin America to adopt comprehensive data protection laws.[64] Argentina took initiative by adopting data protection laws modeled after Spain's data protection laws.[65] Argentina's codification of data protection is the Personal Data Protection Act (hereinafter, "PDPA") No. 25.326.[66] The purpose of the PDPA is to implement Argentina's constitutional guarantees to data privacy.[67] Specifically, the Act reads as follows:

> The purpose of this Act is the full protection of personal information recorded in data files, registers, banks or other technical means of data-treatment, *either public or private for purposes of providing reports*, in order to guarantee the honor and intimacy of persons, as well as the access to the information that may be recorded about such persons, in accordance with the provisions of Section 43, Third Paragraph of the National Constitution.[68]

The PDPA guarantees individuals' rights and protections under the law and affords them access to their data.[69] As stated, the law applies to both public and private persons and legal entities that own databases.[70] In summary, the PDPA regulates data users' ability to process personal or sensitive data.[71]

There are striking similarities between the PDPA and the EU Directive. Specifically, Argentina and the EU share almost identical

---

[64] *See* Gakh, *supra* note 46, for a more comprehensive understanding of the differences in data protection between the U.S., Europe, and Latin America; Andrés Guadamuz, *Habeas Data: The Latin American Response to Data Protection*, 2001 J. INFO. L. & TECH. 3, https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz/ (last visited Aug. 29, 2006).

[65] John C. Eustice & Marc Alain Bohn, *Navigating the Gauntlet: A Survey of Data Privacy Laws in Three Key Latin American Countries*, 14 SEDONA CONF. J. 137, 138 (2013).

[66] *See* PDPA, *supra* note 49.

[67] *See id.* § 1.

[68] *Id.* (emphasis added).

[69] *See id.*

[70] *See id.* § 2.

[71] *See id.*

definitions of "data."[72] Under the PDPA, "personal data" is defined as "information of any kind referred to certain or ascertainable physical persons or legal entities."[73] Sensitive Data, which receives a higher degree of protection, is defined as "personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior."[74] The PDPA regulates "data users"[75] and "data owner[s]."[76] Under the PDPA, citizens are given wide latitude in accessing their own data.[77]

A. *Citizens' Right of Action: Habeas Data*

In some instances, the PDPA grants greater data privacy protection than the laws in Europe and, in particular, the U.S. Argentina has afforded its citizens a private right of action known as *Habeas Data*.[78] This cause of action falls into a category of constitutional rights known as "*amparo*."[79] The Argentine Constitution was amended in 1994 to add a provision dealing with privacy.[80] The relevant article of Argentina's Constitution reads as follows:

> Any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the

---

72 *Compare* PDPA, *supra* note 49*, with* EU Directive, *supra* note 8.

73 PDPA, *supra* note 49.

74 *Id.*

75 *Id.* ("Any person, either public or private, performing in its, his or her discretion the treatment of data contained in files, registers or banks, owned by such persons or to which they may have access through a connection.").

76 *Id.* ("Any physical person or legal entity having a legal domicile or local offices or branches in the country, whose data are subject to the treatment referred to in this Act.").

77 *See id.*

78 Guadamuz, *Habeas Data*, *supra* note 64 at 3, 3.2.4.

79 *See id.*

80 *See id.*

> sources of journalistic information shall not be impaired.[81]

Essentially, *Habeas Data* is a positive right that allows individuals to bring an action to protect their constitutional right to data privacy.[82] This right to access their information is codified in the PDPA as well.[83] *Habeas Data* can prove to be problematic when Argentine companies or entities are required to produce ESI that implicates the data privacy rights of countless individuals. On the other hand, the amount of people bringing these *Habeas Data* claims is rather low.[84]

B. *Enforcement and Oversight of the PDPA*

While evidence suggests that enforcement is rather lax, PDPA violations still carry severe penalties.[85] The Argentine Personal Data Protection Agency (hereinafter, "APDPA") is the agency that oversees the PDPA.[86] The agency has the power to review complaints and the power to initiate investigations on its own.[87] Upon finding a

---

[81] Art. 43, CONSTITUCIÓN NACIONAL [CONST. NAC.] (Arg.), *available at* http://pdba.georgetown.edu/Constitutions/Argentina/argen94_e.html.

[82] *See* Gakh, *supra* note 46, at 785.

[83] *See* PDPA, *supra* note 49 ("SECTION 33.- Legal Basis of a Complaint - The action for the protection of personal data or of *habeas data* shall be applicable: (a) to acquire knowledge of personal data stored in public or private data files, registers or banks intended for the provision of reports, as well as purposes thereof; (b) to those cases in which the falsehood, inaccuracy or outdating of the relevant information is presumed, and the treatment of such data whose registration is prohibited by this Act, in order to demand their suppression, rectification, confidentiality or updating.").

[84] *See* Gakh, *supra* note 46, at 789-91 (discussing the plaintiff's heightened pleading requirement, which can make it difficult for a plaintiff to assert his rights).

[85] Only 19 fines were issued between 2005 and mid-2012. It is believed that the lack of sanctions is a result of insufficient resources. *See* Eustice, *supra* note 65, at 141.

[86] Alec Christie, et al., *Argentina: Data Protection Laws of the World Handbook: Second Edition – Argentina*, MONDAQ (Feb. 13, 2014), http://www.mondaq.com/x/230846/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+Argentina.

[87] *Id.*

violation, the agency can impose fines or revoke the data controller's ability to maintain a database.[88] Civil fines include a "warning, suspension, or a fine ranging between [$1,000 to $100,000]."[89] Additionally, there are criminal sanctions for certain intentional acts, such as inserting false information into a database.[90] Criminal penalties can range from one month to multiple years of imprisonment.[91] These criminal penalties show how seriously the APDPA takes data privacy violations.

In order for an entity to keep data, its database must be registered with the APDPA.[92] Regardless of whether it is a public or private entity, so long as the entity is not using the data for personal use, it must be registered.[93] Consent is the key, in most instances, to a data controllers' ability to transfer and process data.[94] In some instances, consent is not required altogether.[95] When personal data is being collected, notice must be provided to those whose data is affected.[96] Entities must provide:

> (i) the purpose for which the data is being collected, (ii) who may receive the data, (iii) the existence of a database, the identity of the data collector and its mailing address; (iv) the consequences of providing the data, of refusing to do so or of providing inaccurate information; and (v) the data subject's access, rectification and suppression rights.[97]

---

88 *Id.*

89 *Id.*

90 *Id.*

91 PDPA, *supra* note 49, § 32.

92 *See* Christie, *supra* note 86.

93 *Id.*

94 *Id.*

95 *Id.* ("(i) the data is collected from a publicly accessible database, in the exercise of government duties, or as a result of a legal obligation, (ii) the database is limited to certain basic information, such as name, ID, tax ID, job, birthdate and address, (iii) the personal data derives from a scientific or professional contractual relationship and is used only in such context, or (iv) the information is provided by financial institutions, provided that they were required to do so by a court, the Central Bank or a tax authority").

96 *Id.*

97 *Id.*

Once the data is collected and stored in a database, it must be "truthful, adequate, pertinent, and not excessive, be used exclusively for the purpose for which it was legally obtained and be deleted on completion of that purpose."[98] Depending on the level of security that is required, the data controller may have a legal obligation to have someone appointed to maintain adequate security.[99] Regardless, data controllers must maintain an adequate system that notifies them of any breaches.[100]

In order for personal data to be transferred outside of Argentina, several conditions must be met.[101] Transferring personal data requires the data owner's consent as well as the presence of a legitimate interest between the transferring and the receiving parties.[102] Thus, international data transfers are only lawful in a few circumstances.[103] Under the PDPA, "[t]he treatment of personal data is unlawful when the data owner has not given his or her express consent, which must be given in writing, or through any other similar means, depending on the circumstances."[104] There are separate standards for the ability to transfer personal data and sensitive data. Not surprisingly, sensitive data is granted a greater level of protection.[105] Sensitive data can only be collected and utilized when there is a general interest authorized by law.[106] Examples of sensitive data can be

---

98 *See* Christie*, supra* note 86.

99 *See id.*

100 *See id.*

101 Eustice, *supra* note 65, at 140.

102 *See id.*

103 PDPA, *supra* note 49, at § 12 ("a) international judicial cooperation; b) exchange of medical information, when so required for the treatment of the party affected, or in case of an epidemiological survey, provided that it is conducted in pursuance of the terms of Paragraph e) of the foregoing Section; c) stock exchange or banking transfers, to the extent thereof, and in pursuance of the applicable laws; d) when the transfer is arranged within the framework of international treaties which the Argentine Republic is a signatory to; e) when the transfer is made for international cooperation purposes between intelligence agencies in the fight against organized crime, terrorism and drug-trafficking").

104 *Id*. §5.

105 Sensitive data can be collected and subjected to treatment only in case there exist circumstances of general interest authorized by law, or with statistical or scientific purposes provided data owners cannot be identified. *Id*. §7.

106 *Id.*

anything from information that details someone's racial background, to information detailing someone's sexual orientation.[107] Additionally, no person can be compelled to provide sensitive data.[108] Essentially, sensitive data can only be collected for public interest purposes.[109]

C. *Problems Facing Litigators and Entities under the PDPA*

Despite a seemingly rigid and aspirational data protection law scheme, many critics point to flaws in the PDPA.[110] Recently, Argentina's laws came under fire for three reasons: (1) the PDPA lacks any actual enforcement capability; (2) the language of the PDPA has not kept up with technological advances; and (3) the penalties for violating the law are not as serious as those within the EU[111] Combined, these issues have even caused some to critically examine Argentina's commitment to data protection.[112] In fact, some people do not feel that Argentina has adequate data protection as defined under the Directive.[113] Aside from the PDPA's technical problems, the law has also frustrated many litigators because it aspires to be much more than it is; the PDPA attempts to provide far-reaching and comprehensive data protection, but it does not provide enough transparency for litigators to predict whether they will be subject to sanctions.[114]

In theory, the PDPA, like the Directive, inevitably impedes the flow of information from Argentina to the U.S. Critics of the Directive claimed that strict enforcement of the Directive would hurt trans-Atlantic trade.[115] The same concerns would apply to trade between Argentina and any country with inadequate data protection.

---

107 *Id.* §2.

108 *Id.* §7.

109 PDPA, *supra* note 49, §7.

110 *See* Eustice, *supra* note 65, at 143.

111 *Id.*

112 *Id.* at 141-43; *see also* Enrique M. Stile, *The Current Importantce [sic] of Implementing Data Protection in Argentina*, EMPLOYMENT LAW ALLIANCE (Feb. 10, 2014), http://www.employmentlawalliance.com/firms/marvalar/articles /the-current-importance-of-implementing-data-protection-in-argentina.

113 *See* Eustice, *supra* note 65, at 141.

114 *See* Gakh, *supra* note 46; *see* Stile, *supra* note 112.

115 *See*, *e.g.*, Declan McCullagh, *U.S. Twitchy on EU Data Privacy*, WIRED NEWS (Oct. 16, 1998), http:// www.wired.com/news/business/0,1367,15671,00.h

Similar to the discovery problems that U.S. litigators face in the EU, Argentina's laws have posed countless issues to U.S. litigators as well. One particular problem area concerns the treatment of both personal and sensitive data with respect to work emails. In the U.S., work emails are not subject to the data protections standards present in the EU and Argentina.[116] Courts have gone as far as to say that the personal emails of company employees were discoverable in litigation.[117] Further, the U.S. Supreme Court has held that a company may monitor its employees' phone usage for work-related purposes.[118] Thus, in the U.S., work emails are not considered private, thereby making them accessible to the employer.[119] Therefore, U.S. employers would not face many problems when producing emails or text messages for discovery requests.[120] On the other hand, work emails are protected in Argentina.[121] If an email contains personal or sensitive data, the employer will likely face a roadblock in trying to comply with a U.S. discovery request. The data owner will generally not be forced to consent to its production in litigation.[122] In many fields of law, emails may form the foundation of a litigant's case. Embedded in an email may be information that is disserving to the defendant. In the absence of such emails, it may be difficult to establish key elements in a cause of action, making it fatal for a plaintiff's case. On the other hand, if the defendant fails to produce the emails, the U.S. court is not likely to respect the privacy rights of foreign individuals.[123] The court will instruct the jury that the defendant failed to produce documents; the inference that is drawn will certainly not be favorable to the defendant[124].

---

tml.

[116] European employees can deny consent to monitoring programs. *See generally* Lothar Determann & Robert Sprague*, Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States,* 26 BERKELEY TECH. L.J. 979, 1035 (2011).

[117] P.R. Tel. Co. v. San Juan Cable LLC, No. 11-2135 (GAG/BJM), 2013 U.S. Dist. LEXIS 146081, at *4-5 (D.P.R. Oct. 7, 2013) (finding that the company had a duty to preserve the personal emails of its former officers).

[118] City of Ontario v. Quon, 560 U.S. 746, 747 (2010).

[119] *Id.*

[120] *Id.*

[121] *See* PDPA, *supra* note 49.

[122] *See* Christie, *supra* note 86.

[123] *See* City of Ontario, 560 U.S. at 747.

[124] *See id.*

Under Argentine law, a party that violates the PDPA may be subject both to civil fines and criminal sanctions.[125] If the Argentine entity fails to produce documents after receiving a discovery request, the entity will likely face sanctions and other penalties for noncompliance. Argentine parties may be willing to produce documents if it only results in a small fine, but the risk of criminal sanctions is not likely compel someone to produce documents at the request of a U.S. court.[126] After all, how many litigators are willing to go to jail for their client? To that end, U.S. courts should be sensitive to the dilemma Argentine entities face, and should not be too quick to penalize a party who fails to produce documents for fear of criminal sanctions. U.S. courts have instructed the trier of fact to draw an adverse inference when the foreign entity fails to produce the documents requested during discovery.[127] By drawing an adverse inference, the trier of fact assumes that the non-producing party is hiding damaging information—completely ignoring the possibility that a conflict of laws could prevent the party from producing the information.

Once a U.S. litigant has made a discovery request in a U.S. court, the Argentine party has to choose between following the request or following Argentine law, which generally prohibits the transfer of data to countries with inadequate data laws.[128] The transfer of data out of Argentina will very likely infringe on the data privacy rights of individuals who are not a party to the lawsuit. Most likely, the data rights of employees and customers will be affected. This is where a fundamental conflict occurs. Courts must decide whether to order the production of data or to respect the domestic data privacy laws of the foreign country.

In a landmark case on foreign litigants' noncompliance with a court-ordered discovery request, the Supreme Court ruled that a foreign litigant could not be subject to the consequences of noncompliance as their noncompliance was the result of obeying the home

---

[125] *See* Eustice, *supra* note 65, at 141.

[126] PDPA, *supra* note 49, § 32.

[127] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442 (1987) [hereinafter, Restatement]; *see also* Cowper*, supra* note 17, at 264.

[128] PDPA, *supra* note 49, at § 12.

country's law.[129] Further to that end, Section 442 of the Restatement (Third) of Foreign Relations (hereinafter, "Restatement") requires that foreign litigants "make a good faith effort to secure permission from the foreign authorities to make the information available" whenever complying with a production order would subject them to civil or criminal penalties in their home country.[130] It has been aptly stated that both the Restatement and the Hague Convention are ill-suited in our ever-globalizing world.[131]

D. *Consequences of Noncompliance with U.S. Discovery Order.*

E-discovery has made cross-border discovery under the Restatement and the Hague Convention nearly impossible because of the amount of information that can be stored electronically. Modern technology has allowed entities to maintain vast troves of data.[132] The more information that is stored, the more likely that a great number of individuals' privacy rights will be affected. There is no doubt that pre-trial discovery can make or break many cases.[133] On one hand, pre-trial discovery often acts as an incentive for parties to settle.[134] When a company is faced with staggering discovery prices, it only seems logical that settlement may be less costly than litigation; however, if settlement is not an option and the foreign party is unable to comply with the discovery request, the Restatement suggests that sanctions should not be applied when a good faith effort

---

[129] *See* Societe Internationale Pour Participations Industrielles Et Commerciales, S. A. v. Rogers*,* 357 U.S. 197, 211 (1958) (finding that Swiss plaintiff's production of documents would have violated Swiss laws).

[130] *See* Restatement, *supra* note 127, § 442..

[131] *See* Caylor*, supra* note 9, at 264.

[132] Over half of the World's largest databases are owned and maintained by private multinational corporations. Amazon's database, for instance, stores the information of nearly 60 million customers, or 42 terabytes of data. *See Top 10 Largest Databases in the World*, COMPAREBUSINESSPRODUCTS.COM, http://www.comparebusinessproducts.com/fyi/10-largest-dat
abases-in-the-world (last visited Feb. 14, 2014).

[133] *See* Kevin J. Lynch*, When Staying Discovery Stays Justice: Analyzing Motions to Stay Discovery When a Motion to Dismiss is Pending*, 47 WAKE FOREST L. REV. 71, 71-72 (2012).

[134] *Id.*

has been made—but, courts can, and do, impose an adverse inference against the foreign party for noncompliance.[135] Although the Restatement tries to protect foreign parties, U.S. courts can and do use their discretion to draw adverse inferences in a wide array of domestic litigation.[136] An adverse inference can often be outcome-determinative. Because of this practice, it is clear that when a foreign entity files suit in the U.S. they will not be allowed to avail themselves of the data protection laws of their country. So, if an Argentine entity were to file a suit in the U.S. and hope for a favorable outcome, the entity is expected to produce discovery materials much to the same extent as it would be expected if it were located in the U.S.[137]

U.S. courts are not hesitant to issue adverse inferences. For example, the district court in *Lyondell Citgo Refining* issued an adverse inference despite claims by the defendant that it had made a good faith effort to produce certain requested materials.[138] Generally speaking, adverse inferences afford judges wide latitude in making decisions that certainly have a significant impact on a case's outcome. In fact, the standard of review for a judges' pre-trial discovery motion is "clearly erroneous."[139] Courts have posited that the adverse inference is "the necessary mechanism for restoring the evidentiary balance."[140] In understanding the underlying purpose of an adverse inference, it is important to understand that "[t]he inference is adverse to the destroyer not because of any finding of moral culpability, but because the risk that the evidence would have been detrimental rather than favorable should fall on the party responsible

---

135 *See* Restatement, *supra* note 127, § 442.

136 *See* Mali v. Federal Insurance Company, No. 11-5413, 2013 WL 2631369, slip op. (2d Cir. June 13, 2013).

137 *See* Reino de España v. Am. Bureau of Shipping, No. 03 Civ. 3573 LTS/RLE, 2006 WL 3208579, at *1 (S.D.N.Y. Nov. 3, 2006) (Spanish government brought suit in U.S. District Court, later objected to discovery remands on ground of Spanish Privacy law. Court ordered compliance, holding that plaintiff chose to sue in U.S. court and must follow U.S. procedures).

138 *See* Lyondell-Citgo Ref., LP v. Petroleos de Venez., S.A., No. 02 Civ. 0795(CBM), 2005 WL 1026461, at *1 (S.D.N.Y. May 2, 2005) (where the requested materials were corporate board minutes).

139 *Id.* at *3.

140 Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 75 (S.D.N.Y. 1991).

for its loss."[141] Foreign entities face the additional risk that if its lawyers comply with U.S. discovery demands in violation of their domestic laws, they may face criminal liability.[142] Foreign litigators are forced to balance the costs and benefits between complying with U.S. discovery requests and violating the PDPA. If they comply with the discovery request, then they may be subject to criminal liability and civil fines.[143] On the other hand, if they refuse to comply with the discovery request, then they face the imposition of an adverse inference, which may or may not be outcome-determinative to their case. Putting litigators in this case poses conflicting ethical obligations.[144] In some instances, where only a fine may be imposed for a violation, then it may be worth the cost to violate the PDPA. Unfortunately, these determinations are not so clear and easy to make. It has often been difficult to determine when the APDPA will or will not enforce the PDPA.[145]

V. POSSIBLE SOLUTIONS FOR EU-U.S. DISCOVERY PROBLEMS

Attempting to solve cross-border discovery problems in Argentina is no easy task. There are optimists that believe a solution is possible, only requiring some form of compromise,[146] while there are others who believe that a solution is far beyond reach.[147] Rather, they believe that only a series of protocols can help effectuate discovery requests.[148] It is unlikely that Argentina will ever fully comply with U.S. discovery requests because Argentina, like the EU, has

---

[141] *Id.*

[142] The French Supreme Court upheld the criminal conviction of a French lawyer who violated French data protection laws in an effort to comply with a U.S. discovery request. *See* Klein, *supra* note 11, at 624.

[143] PDPA, *supra* note 49, § 32.

[144] Advising a foreign client to break the law in Argentina by violating a data protection law would certainly conflict with most states' rules on professional responsibility. *See generally* MODEL RULES OF PROF'L CONDUCT (1992).

[145] *See* Eustice, *supra* note 65, at 141-42.

[146] *See generally* Nafziger, *supra* note 31; *see* Caylor, *supra* note 9, at 348.

[147] *See* Christian Zeunert & David Rosenthal, *Cross-Border Discovery-Practical Considerations and Solutions for Multinationals*, 12 SEDONA CONF. J. 145, 152 (2011) (claiming that it is unrealistic to think that an entity could fully comply with both foreign data protection laws and a U.S. discovery request).

[148] *See id.*

differing opinions on privacy and data protection.[149] With respect to discovery issues in the EU, many parties have tried to come up with a workable solution.

There are at least three solutions that may help to create cross-border discovery more predictable. One solution is to establish a committee that can determine specifically where the issues lie and then work with the legislature to reconcile them.[150] The second solution is to establish a series of procedures that entities can follow when faced with a U.S. discovery request.[151] A third solution is to update the Hague Evidence Convention.[152] It is worth mentioning that these solutions do not exist in a vacuum. Any one solution alone will not likely suffice.

A. *Establish a Working Party*

Following the implementation of the EU directive, the European Parliament established the Article 29 Data Protection Working Party ("Working Party").[153] While the Working Party is not a solution in and of itself, it is tasked with the duty of finding solutions to cross-border discovery obligations and has helped to highlight the issues.[154] Although discovery issues in the EU are slightly different than they are in Argentina, the Working Party's solutions still provide a great deal of guidance.

By finding solutions to cross-border discovery, the Working Party has to strike a balance between an individual's right to their data and the "free movement of such data."[155] The Working Party has been granted advisory status and acts independently of the European Parliament—essentially, it acts as an advisory committee.[156] In 2009, the Party released a paper titled, *Working Document on*

---

149 *See id.*

150 *Article 29 Working Party*, EUROPEAN COMMISSION (June 8, 2013), http://ec.europa.eu/justice/data-protection/article-29/index_en.htm ("Set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.").

151 *See* Zeunert, *supra* note 147.

152 *See* Klein, *supra* note 11, at 643-44.

153 *See Article 29 Working Party, supra* note 150.

154 *See id.*

155 *Id.*

156 *Id.*

Pre-trial Discovery for Cross-Border Civil Litigation.[157] The paper took notice of some of the struggles between the right to data privacy and the need to improve cross-border discovery.[158] Specifically, the paper addressed: "Pre-emptive document preservation in anticipation of proceedings before U.S. courts or in response to requests for litigation hold, known as 'freezing' [and] pre-trial discovery requests in U.S. civil litigation."[159]

Creating an organization similar to the Working Party would be a great starting point for solving the dilemma that currently affects the U.S. and Argentina. While there has been wide publication of sanctions imposed against U.S. companies operating in the EU, there has been little, if any, publication of companies being fined by the APDPA.[160] Because there is little case law regarding U.S.-Argentina discovery problems, an advisory committee could help bring light to specific issues that will prove to be problematic going forward. One suggestion by the Working Party is that "[o]nce personal data has been identified, the data controller would need to consider whether it is necessary for all of the personal data to be processed, or for example, could it be produced in an anonymous or redacted form."[161] This solution can be effective where the names of the data subjects are not specifically requested in pre-trial discovery, or where the names of the data subjects are not consequential to the discovery request.

In its paper, the Working Party established guidelines after they appropriately recognized that data protection obligations do not coexist well with foreign discovery requirements.[162] The Working

---

[157] *Working Document on Pre-trial Discovery for Cross-Border Civil Litigation,* EUROPEAN COMMISSION (Feb. 15, 2014), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf [hereinafter *Working Document*].

[158] *Id.* at 2, 7.

[159] *Id.* at 2-3.

[160] *See e.g.*, Aoife White, *Firms Face Fines as Much as 2% of Sales Under EU Privacy Law*, BLOOMBERG NEWS (Jan. 25, 2012, 10:22 AM), http://www.bloomberg.com/news/2012-01-25/companies-face-fines-as-much-as-2-of-sales-under-eu-privacy-law.html; *see also* Marianne Le Moullec, *The French Data Protection Authority Fines Google for Breach of French Privacy Laws*, PRIVACY LAW BLOG (Jan. 31, 2014), http://privacylaw.proskauer.com/2014/01/articles/online-privacy/the-french-data-protection-authority-fines-google-for-breach-of-french-privacy-laws/.

[161] *Working Document*, *supra* note 157, at 11.

[162] *Id.* at 7.

Party stated that because each level of discovery during litigation amounts to a processing of the data, there must be a justification at each stage.[163] The Directive does not allow arbitrary processing.[164] In Europe, like in Argentina, data controllers are not permitted to retain personal data indefinitely in the anticipation of future litigation.[165] This becomes problematic because the FRCP allows parties to send a discovery request to produce and permit the inspection of items in the responding party's possession, custody, or control.[166] The Working Party suggests that so long as data controllers freeze the documents that they currently have in their possession, then they cannot be faulted.[167] As long as data controllers retain information for short periods in abidance with local laws, they will not be violating any data protection laws, nor will they be violating any discovery requests.[168] Of course, this does not bode well for the party seeking the information because they will likely be seeking data from an earlier time; however, U.S. courts have held that the test to determine the production of documents is "control, not location."[169] Control is the "the legal right to obtain [the] documents on demand."[170]

If an entity receives a litigation hold, they are being asked to freeze the data. Essentially, the entity is being asked to process data, by retaining it longer than it otherwise would have.[171] Under the EU directive, retaining data in the anticipation of future litigation amounts to a "processing."[172] Holding data for the "mere unsubstantiated possibility" that a lawsuit will be filed is not enough to pass

---

[163] The stages are (1) retention, (2) disclosure, (3) onward transfer, and (4) secondary use. *Id*.

[164] *See id.*

[165] *Id.* at 7-8.

[166] FED. R. CIV. P. 34(a)(1).

[167] Data controllers need to hold or "freeze" what is currently in their database upon receiving a request to be in compliance with U.S. discovery requests. There is no FRCP requirement that companies constantly hold data in anticipation of litigation. *See Working Document*, *supra* note 157, at 7-8.

[168] *See id.*

[169] Marc Rich & Co. v. United States, 707 F.2d 663, 667 (1983).

[170] Flagg v. City of Detroit, 252, F.R.D. 346, 353 (E.D. Mich. 2008).

[171] Litigation holds act as a demand to suspend the company's retention and destruction practices. This asks them to freeze all the data that they currently have in possession. *See Working Document*, *supra* note 157, at 8.

[172] *See id.*

muster under EU laws.[173] There is no reason to suspect that this would be any different in Argentina. Under the FRCP, failure to preserve, in and of itself, opens a party up to sanctions.[174] In fact, the most common type of discovery sanction is the failure to preserve ESI.[175] Recognizing that Argentina's data privacy is comparable to that in the EU, the Working Party's resolution helps to provide guidance to Argentina-U.S. discovery issues. "The Working Party recognizes that the parties involved in litigation have a legitimate interest in accessing information that is necessary to make or defend a claim, but this must be balanced with the rights of the individual whose personal data is being sought."[176]

The Working Party makes many valid suggestions that can help entities embroiled in U.S. discovery comply with Argentina data protection laws without ignoring a discovery request. As previously mentioned, the Working Party is neither the solution, nor the endgame.

B. *The Sedona Conference*

The Sedona Conference Journal has been one of the foremost authorities on U.S. discovery practices and its conflict with European and Latin American data protection laws.[177] The Conference has published resources on a wide array of e-discovery issues. Among other significant publications, the Conference published several papers that address cross-border discovery. One paper in particular, published in June 2011, addressed the discovery issues that face multinational corporations.[178] The paper provided practical considerations and protocols.[179] By doing so, it focused on making multinationals prepared to handle the task of cross border discovery obligations.[180] Although the paper provides guidance in reference to multinationals, the guidance and solutions can be applied to nearly

---

173 *See id.*

174 Dan H. Willoughby, Jr. et. al., *Sanctions for E-Discovery Violations: By the Numbers*, 60 DUKE L.J. 789, 803 (2010).

175 *See id.*

176 *See Working Document*, *supra* note 157, at 2.

177 The Sedona Conference, https://thesedonaconference.org/publications.

178 *See* Zeunert, *supra* note 147, at 152.

179 *See id.*

180 *See generally id.*

any entity operating in Argentina that potentially faces U.S. discovery obligations.

The paper addresses four organizational challenges that multinationals face when dealing with cross-border discovery: (1) getting e-discovery experts on board early in the process; (2) educating and working together with opposing counsel; (3) the presence of additional time-consuming measures; and (4) fully complying with the discovery request.[181] Acknowledging these challenges before facing a discovery request may help, but it is ultimately self-defeating to think that one could satisfy both U.S. laws and Argentine laws.[182]

Multinational companies faced with the task of complying with U.S. discovery obligations would be wise to hire an e-discovery expert as soon as possible.[183] This is important because understanding where discoverable data is located and how to process it efficiently is absolutely necessary in order to comply with a discovery request promptly. It is suggested that multinationals would suffer if they relied solely on advice from U.S. trial lawyers when anticipating a discovery request.[184] By hiring in-house e-discovery experts, a multinational can maintain consistency in processing and addressing U.S. discovery requests.[185] For companies that are large enough, it may be cost-effective to create an e-discovery department.[186] An e-discovery team, it is suggested, can create a standardized process that is implemented company-wide.[187]

The second challenge requires that foreign entities educate their employees on the U.S. discovery requests and working with opposing counsel.[188] A simple solution to this challenge would be to meet and confer in the hopes that opposing counsel is receptive to the challenges that the defendant is facing.[189]

---

181 *See id.* at 147-152.

182 *Id.* at 151 (While handling the organizational challenges may be a matter of sheer effort and goodwill, it seems illusory (at first glance at least) to conduct an e-discovery in Europe expecting to fully satisfy U.S. law and European data protection legislation as well as other applicable legal requirements).

183 *Id.*

184 *See* Zeunert, *supra* note 147.

185 *Id.*

186 *Id.*

187 *Id.*

188 *See id.* at 149.

189 *See id*.

A solution to the third challenge, which is closely related to the second, requires that a discovery schedule is created so that both parties can understand the complexity of cross-border discovery in their respective situation.[190]

Lastly, the fourth challenge requires that multinationals keep in touch with the latest technical capabilities of filtering through discoverable data.[191] The benefits to this solution are twofold: multinationals can efficiently filter through personal and sensitive data, and they can do so in a timely manner.

Beyond the organizational challenges facing multinationals, the paper addresses conditions that must be met in order for multinationals to come to a solution with opposing counsel.[192] The first condition is that multinationals need to have the same willingness to comply with U.S. discovery requests as U.S.-based corporations do.[193] European and Latin American entities are not as accustomed to e-discovery and its staggering prices.[194] U.S. lawyers are more aware of the penalties for failure to follow U.S. discovery requests.[195] Entities in Europe or Latin American may need to acquire the same "willingness" in order for some solution to be found.[196] In order to encourage this elusive concept of "willingness," there will need to be more at stake than the fear of penalties or sanctions. Foreign litigators need to understand that U.S. discovery is, arguably, the most significant phase in litigation, and failure to cooperate with opposing counsel can result in an unfavorable outcome.

A workable solution for cross-border discovery is said to rest on three prerequisites: (1) parties must be willing to disclose all information allowed by applicable law; (2) foreign entities must be prepared if there is any risk at all of being called upon to produce materials; and (3) parties must familiarize themselves with their opponent.[197]

---

190 *See* Zeunert, *supra* note 147.
191 *Id.*
192 *Id.*
193 *Id.* at 152.
194 E-discovery prices can range from $500,000—$3 million. *Id.*
195 *Id.*
196 *See* Zeunert, *supra* note 147.
197 *See id.* at 152-154.

Two additional prerequisites can be added to this list. First, European and Latin American entities must have the ability to undertake a discovery request. E-discovery, being relatively new for some, requires a special level of expertise in handling, sourcing, and transferring data.[198] U.S. courts have come to expect that parties are capable of handling a request, especially if it is a larger entity.[199] It is possible that U.S. courts are willing to be more lenient with smaller foreign entities, but that is no certainty. Courts are unlikely to be lenient towards a smaller entity because it is too tedious to determine who is worthy of leniency. Consequently, this ad-hoc approach is impractical: it is both time-consuming and costly. When should a court decide to give leniency to a foreign entity? Should the court review the entity's financial statements in order to ascertain whether the entity is in a position to handle a cross-border discovery request? Thus, foreign entities should not expect to receive any judicial leeway once a discovery request is made.

The second additional prerequisite can be labeled "civility."[200] In this context, being civil requires that one understands the opposing party.[201] In the absence of civility, entities will either make ridiculous discovery demands or will refuse to cooperate at all. For there to be a workable solution in conducting discovery with foreign entities, both sides need to communicate regularly.[202] Even if both sides come to the realization that some data is not transferrable because it implicates a data protection law, a lack of civility will likely enrage the party seeking the data, making them more likely to seek a court-ordered discovery request. The violation of such a court order may result in sanctions or an adverse inference.

C. *Modernizing the Hague Evidence Convention*

The next solution focuses entirely on the Hague Evidence Convention. Perhaps we need to see if the Convention is salvageable. Modernizing the Convention would require that it be brought into the reality of a world dominated by ESI-centered discovery. In order

---

198 *See id.*
199 *See id.* at 152.
200 *See id.*
201 *See id.*
202 *See* Zeunert, *supra* note 147.

to modernize the Convention, there are at least four recommendations to put forward. The first is to create an amendment that will establish a clear meaning of pre-trial discovery.[203] The second is to establish a minimum data protection standard, modeled after the United Kingdom's Model Letter of Request.[204] The third and fourth recommendations are to allow bilateral treaties among countries and to place the burden of issuing Letters of Request on the Convention, rather than the countries in which evidence is requested.[205]

It is argued that because so many countries were unfamiliar with pre-trial discovery at the time the Convention was created, many of them blindly signed Article 23 limiting reservations.[206] It has been discovered that some countries that signed an Article 23 limiting reservation were under the impression that "pre-trial" discovery meant that discovery would take place before a claim was filed.[207] Perhaps those countries feared what they did not understand. It is suggested that civil law countries now have a better understanding of the scope of pre-trial discovery in the U.S.[208] It is possible that those countries that previously misunderstood pre-trial discovery may now be willing to rescind their Article 23 limiting reservation.

If pre-trial discovery is as efficient and effective as it is claimed to be, why would foreign countries not want to participate? One reason could be that even with foreign countries understanding what pre-trial discovery is, allowing foreign entities to engage in it will still result in the same potential data violations. Whether the data is provided early or late in the litigation, it is still being provided; however, if foreign countries, like Argentina and EU members, were to get a better understanding of pre-trial discovery, and if the U.S. established minimum data protection standards, then there may be a different outcome. Modernizing the Convention may take as much work as rewriting it.

---

203 *See* Caylor*, supra* note 9, at 374.

204 The U.K.'s model letter of request requires more specific descriptions of evidence requested than in civil law jurisdictions. *See id.*

205 *See id.*

206 *See id.* at 344.

207 *See id.* at 378.

208 *See id.* at 376.

D. *The Problem May Be Local Instead of Global.*

Globalization can only work if there is give and take, and it requires active and well-guided government action.[209] That is, to make globalization work efficiently, countries must accept certain active government involvement so that they can enjoy certain protectionist benefits.[210] Whether or not that is a perfect system is beyond the scope of this paper. In order for countries and multinational corporations to continue conducting business on a global scale, there needs to be a more unified system of cross-border discovery. Many of the previously mentioned solutions placed the focus on foreign countries. Is the U.S. to blame for these cross-border discovery dilemmas? It is possible that the problem does not lie within the EU or Argentina, but rather the problem lies within the U.S. One solution is that the U.S. should heighten its level of data protection and data privacy laws to that of the EU and Argentina.[211] Another solution is that U.S. courts need to be more cognizant of discovery under the PDPA and the EU Directive. Going one step further, courts may need to assess the value of a case-by-case basis in determining the merits of compelling discovery from a foreign entity. This last solution may assume that the judiciary must step in and reconcile the issue because it is unlikely that the U.S. legislature will heighten its data protection laws.

One could argue that U.S. pre-trial discovery requests are a cost of conducting business in the U.S. Should a foreign party produce documents and just pay fines if that means that they will not be subject to an adverse inference in a U.S. court? Essentially, the foreign party is forced to make a cost-benefit analysis.[212] Parties are forced to determine whether the costs of violating Argentine data protection laws are outweighed by the benefit that following a discovery request offers. Should it be in the policy of U.S. courts to incentivize entities to break foreign laws if that means benefiting a U.S. litigant

---

209 *See generally* David A. Moss, *Globalization and the Social Contract*, THE CENTENNIAL GLOBAL BUSINESS SUMMIT (Summer 2008), http://www.hbs.edu/centennial/businesssummit/business-society/globalization-and-the-social-contract.pdf.

210 *Id.*

211 *See* Nafziger, *supra* note 32.

212 *See* Caylor*, supra* note 9, at 368-69.

by allowing them to view the documents they requested? If the penalties for violating data protection laws in Argentina were nominal, then the choice to produce materials does not require any more discussion; however, because the penalties can be severe, it is not an easy choice. On the other hand, if the foreign party is availing itself of the protections and benefits of U.S. laws while conducting business, should it be allowed to shield itself under data protection laws of Argentina? U.S. courts have realized that some entities use the laws of foreign countries to protect themselves.[213] In *Columbia Pictures*, a California district court reiterated the position articulated in *Aerospatiale* and held that foreign statutes do not prevent a court from ordering a party to produce evidence.[214]

Quite possibly, the biggest impediment to the Hague Evidence Convention is *Aerospatiale*.[215] It has been suggested that perhaps in order to make the give-and-take system of globalization work, the U.S. should overturn *Aerospatiale* so that the Hague Evidence Convention is not wholly useless.[216] Would a gesture, such as overturning *Aerospatiale*, convince civil law countries that we are willing to compromise? Unlikely. If data privacy is as fundamental a right as it is claimed to be, then overturning *Aerospatiale* is enough to bring about change.

Conceptually, international treaties tend to take a one-size-fits-all approach to solving issues that affect scores of countries. This is problematic for obvious reasons. Every country—and every culture for that matter—has a unique view. Data privacy and cross-border discovery are no exception to this phenomenon. The fact that many countries have not signed limiting reservations to the Hague Evidence Convention shows that not all countries are opposed to the use of pre-trial discovery Letters of Request. Even if countries were unfamiliar with pre-trial discovery upon becoming a party to the Convention, they still may be disinclined to allow discovery requests. Again, to distinguish, common law countries and civil law

---

213 *See* Columbia Pictures v. Bunnell, 245 F.R.D. 443, 452 (C.D. Cal. 2007).

214 *See id.*

215 Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 541 (1987).

216 *See* Nafziger, *supra* note 32, at 104-06.

countries have different procedures for conducting discovery. In civil law countries, judges often conduct discovery.[217]

VI. CONCLUSION

Despite guidelines and protocols to cross-border discovery, any solution to the problem between the U.S. and Argentina will require some compromise between the two countries. After looking at the European model and the issues that are created by the EU directive, it seems clear that the U.S. and Argentina need to work together in finding a solution that is unique to each countries' needs. A one-size-fits-all approach is not likely to be helpful because each country's views on data privacy are as unique as an individual's fingerprint.

What makes cross-border discovery in Argentina especially difficult is that its data protection laws are almost unpredictable. In order to solve the discovery disputes between the U.S. and Argentina, at least three conditions must be met: (1) Argentine law makers must make violations of data protection law clearer; (2) U.S. courts needs to recognize that data privacy needs to be respected; and (3) U.S. courts should only apply sanctions and penalties in egregious situations. Argentine authorities need to clarify their willingness to comply with their own laws. If Argentine litigators are not fearful of being reprimanded for violating Argentine data protection laws, then the discussion does not need to go any further.

As the NSA's vast surveillance program has come to light recently, the EU has been increasingly reluctant to negotiate with the U.S. regarding trade.[218] U.S. courts need to be more accepting of the fact that data privacy is a fundamental right in Argentina, and that it is not a malleable concept that can be used for the benefit of U.S. litigants.

Lastly, U.S. courts should avoid using adverse inferences when foreign litigants are complying with foreign data privacy laws. Such sanctions should be reserved for egregious violations; for example,

---

[217] Klein, *supra* note 11, at 625.

[218] *NSA snooping: MEPs table proposals to protect EU citizens' privacy*, EUROPEAN PARLIAMENT NEWS (Feb. 12, 2014), http://www.europarl.europa.eu/news/en/news-room/content/20140210IPR35501/html/NSA-snooping-MEPs-table-proposals-to-protect-EU-citizens'-privacy.

when parties intentionally retain discoverable materials because of its damaging nature.