The Global Business Law Review

Volume 9 | Issue 1 Note

1-31-2021

Regulatory Responses to Data Privacy Crises and Their Ongoing Impact on E-Discovery

Teo Marzano
Cleveland-Marshall College of Law

REGULATORY RESPONSES TO DATA PRIVACY CRISES AND THEIR ONGOING IMPACT ON E-DISCOVERY

TEO MARZANO*

ABSTRACT

This note argues that advancements in technology and data analysis have reduced the efficacy of the legal data privacy framework in the United States. Furthermore, foreign law blocking statutes expose litigants and corporations to increased data liability. Indeed, not only do consumers lack adequate legal remedies, but litigants face uncertain legal liability and increased costs. Simply put, updated technology requires updated laws. Better data management protects consumers and data value. A legal framework with clear guidelines for protecting data is needed.

Still, data access is integral to litigation, and courts must balance the need for data against the need for data protection and privacy. An overhaul of how courts handle Discovery proportionality standards, and privacy in those standards, is necessary. Clarifying privacy's role in proportionality and quantifying when and how data should be limited in Discovery, would help accomplish this. It would also bring current Discovery practices and data management more in-line with foreign privacy law, and potentially reduce costs through standardization. Where costs are an issue,

* JD/MBA expected May 2022, Cleveland State University, Cleveland-Marshall College of Law, and Monte Ahuja College of Business; B.S. Case Western Reserve University. The author would like to thank Professor Brian Ray and Kristina Schiavone for their valuable input and guidance.

applying cost shifting standards for Discovery in a manner that promotes data security, and privacy law compliance, can encourage better privacy practices in E-Discovery as well.

I. INTRODUCTION

Electronic data is increasingly important for governments and corporations, representing an estimated $189 billion in revenue in 2019 alone.[1] Courts and governments also process significant data volume, making successful data management important for them as well.[2] Data is now a new dimension in our world with revenue potential, potential abuses, and unique data-centric regulatory issues surrounding data control, definitions, retention, and use.[3] In the United States, data exploitation and loss are a problem.[4] Lagging legislation, systemic security failures,[5] and widespread misuse of benign information erode public trust in corporations that store and process data.[6] Looking at only ten recent scandals, data for almost two billion users was "lost"

---

[1]Michael Shirer, *IDC Forecasts Revenues for Big Data and Business Analytics Solutions will Reach $189.1 Billion this Year with Double-Digit Annual Growth Through 2022*, IDC (Apr. 4, 2019), https://www.businesswire.com/news/home/20190404005662/en/IDC-Forecasts-Revenues-for-Big-Data-and-Business-Analytics-Solutions-Will-Reach-189.1-Billion-This-Year-with-Double-Digit-Annual-Growth-Through-2022 (finding one driving force to be increasing complexity of data solutions and the hardware required for effective data analytics and management).

[2] *See* Francesca El-Attrash, *The Importance of Data Storage & Management to Government*, BIG DATA (Jun. 12, 2017), https://www.govloop.com/resources/importance-data-storage-management-government/. "In the age of increasing data breaches, the ability to not only access but also manage data is critical to government's mission. Data is growing faster than ever. By the year 2020, about 1.7 megabytes of new information will be created every second for every human being on the planet."

[3] Social media companies like Facebook have been called out for misusing customer data. Kevin Granville, *Facebook and Cambridge Analytica: What you need to know as fallout widens*, NEW YORK TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[4] Naula O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, CFR (Jan. 1, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

[5] Calls for reform within the legal system have been widespread, and it is easy to see why; corporations handling data have consistently failed to prevent data breaches from occurring, and each breach exposes potentially millions of customers' data. *Id*.

[6] Equifax, Marriott, British Airways, Quest Diagnostics, USPS, and NHS have all lost personal data in data breaches within the past year alone, and this is by no means an exhaustive list. *Serial Data Breach Cases. When Corporations Know So Much About You. Why Don't they protect your information?*, SECLUDE, https://secude.com/serial-data-breach-cases/ (last visited Mar. 2, 2020). The fact that some of these companies are state run healthcare providers and respected financial institutions makes the matter especially troubling. *Id*

with little or no recourse for those people impacted.[7] These data breaches expose consumers to identity theft,[8] political manipulation, and more.[9] Some believe regulation can provide a privacy solution, maybe eliminate data breaches, but new regulations create conflicting regulatory compliance issues for data handlers without necessarily achieving better outcomes.[10]

The European Union's ("E.U.") regulatory response to the modern privacy crisis is the General Data Protection Regulation ("G.D.P.R.").[11] The expansive regulation, put into effect in 2018, has broad extraterritoriality provisions and impacts how firms must handle, process, store, and delete their data.[12] Additionally, California has rolled out similar legislation through the

---

[7] Seclude, *supra* note 7; *see also Big data, little recourse: Sorine's Story*, DIGITAL FUTURE SOCIETY (Apr. 2, 2019), https://digitalfuturesociety.com/big-data-little-recourse-sorine-story/ (stating customers' experiences can be "unethical and even traumatizing").

[8] *When information is lost or exposed*, FTC https://www.identitytheft.gov/info-lost-or-stolen, (last visited Feb. 18, 2020) (providing consumer resources for data loss victims including steps to prevent identity fraud).

[9] Data breaches are unauthorized access to stored confidential information that is gained either deliberately or accidentally. *What is a data breach?*, NORTON, https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html, (last visited Feb. 2, 2020) (finding system vulnerabilities, weak passwords, drive-by downloads, and targeted malware attacks to be the primary vectors for exploiters to gain access to corporate data). Dipayan Ghosh and Ben Scott, *Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You*, TIME (Mar. 19, 2018), https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/, (describing ongoing issue of data misuse for political aims, and as a means to disseminate misinformation).

[10] The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557, 561-571 (2018) (finding new regulations require data handlers to "develop protocols that address their production of information to government agencies within a reasonable timeframe and [mitigate privacy fallout.]"); *see also Regulation & the Economy*: *The Relationship and how to Improve it*, CED (Sept. 27, 2017), https://www.ced.org/reports/regulation-and-the-economy, (stating regulations do not always achieve their desired ends). "[T] hey do not always live up to public expectations or achieve their social goals. In other words, regulations in practice do not always make things better." *Id*.

[11] Mark Peasley, *It's Time for an American (Data Protection) Revolution*, 52 AKRON L. REV. 911, 913 (2018) (stating 40% increase in breaches from 2015 to 2016 underscores need for greater privacy regulation, and the GDPR contains guidelines that involve minimizing, and encrypting data properly to ensure security). Furthermore, the GDPR requires significantly greater data usage disclosures, provides users a right to deletion of their data at any time, and significantly expands penalties beyond previous standards. *Id*. at 931-37.

[12] W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AMERICAN BUSINESS LAW JOURNAL 287, 292-295 (finding transatlantic differences in how data privacy is regulated have created significantly different compliance standards in the E.U. and U.S. generally). U.S. privacy law has played more of a gap filler role; as broad privacy laws have been generally disfavored over narrower laws protecting only specific classes of data like medical records. *Id*. at 301-313. The FTC has passed a variety of

California Consumer Privacy Act[13], ("C.C.P.A."), and each new regulation brings new liabilities through increased avenues for violations and increased fines.[14]

Specifically, United States Electronic Discovery ("E-Discovery") can conflict with modern data handling and privacy standards,[15] and firms may require updated E-Discovery practices to remain compliant. Furthermore, there are competing compliance interests between disclosure in E-Discovery and privacy protection for relevant electronic data.[16] Litigants must prove their E-Discovery data needs outweigh the increased legal burdens that heightened privacy standards like the G.D.P.R. create.[17] Alternatively, parties seeking to block data disclosures may use privacy laws to shield their clients from Discovery.[18] Consequently, courts and corporations

---

acts protecting digital privacy; however, because of their fundamental differences, E.U. law has long considered U.S. privacy laws to be inadequate. *Id*. at 313-324.

[13] *California Consumer Privacy Act (CCPA)*, https://oag.ca.gov/privacy/ccpa, (last visited Feb. 2, 2020) (providing rights related to "access to, deletion of, and sharing of personal information that is collected by businesses"). The act also authorizes the Attorney General of CA to enact policies to further its aims. *Id.*

[14] *Id*. A right to deletion, while common in Europe, is not typical in U.S. law. *See also USA: Data Protection 2019*, ICLG (Mar. 7, 2019), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[15] The Sedona Conference, 19 SEDONA CONF. J. 557, 561-571 (2018), *supra* note 11 (finding competing interests between compliance with E-discovery and modern privacy law). Compliance with these standards requires significant understanding of the underlying definitions for data handlers, processors, etc., and firms advising corporations will have to ensure relevant protocols are in place for compliance with both E-discovery and privacy regulation. *Id*.

[16] *Id*. (stating legitimate governmental interests do not override "fundamental rights of Data subjects"). "Processing data when there are broad prohibitions against doing so is challenging, even when there appear to be exceptions that permit it." *Id*.

[17] Salt River Project Agric. Improvement & Power Dist. v. Trench Fr. SAS, 303 F. SUPP. 3D 1004, 1008 (D. Ariz. 2018) (arguing for plaintiff that "facially broad" request is specific to documents needed for the case). "SRP asserts that using Hague procedures will [delay litigation and increase expert costs]." *Id* at 1009 (finding availability of alternative means outweighed avoiding increased costs, and ruling in favor of Hague convention procedures).

[18] Giorgi Global Holdings, Inc. v. Smulski, E.D.Pa., No. 17-4416, U.S. Dist. LEXIS 89369 (May 21, 2020) (finding defendant did not prove production was barred by G.D.P.R). "Defendant . . . bears the burden of showing that the GDPR [bars production]." *Id*. at 6.

grapple with these new laws, and the new limits they create for disclosure and data liability in Discovery.

Increased regulatory fines, heightened compliance standards, and increases in data breach events mean firms face increasing risks for storing data, but data generates revenue.[19] More data means more money, as its value increases with volume.[20] However, data theft and data insurance are the tradeoffs.[21] These lucrative troves of data are also better targets for data breaches, which are now considered normal.[22] Appropriate data security reduces risk, but breaches are data security failures that show how inadequate current security is. Legislation may move slower than technology, but it is catching up in data security. [23] The G.D.P.R. increases liability for stored data – data breaches are damaging even absent these new regulations.[24] Breaches result in

[19] *Data as Currency: What Value Are You Getting?*, WHARTON UNIVERSITY, (Aug. 27, 2019), https://knowledge.wharton.upenn.edu/article/barrett-data-as-currency/ (stating data has an "absolute value" comparable to commodities like oil, and likening data handlers to bankers in their fiduciary obligations to manage data faithfully).

[20] *Id.*

[21] *Id.* (finding data gathering has externalities with exhaust like implications similar to automobile driving).

[22] Mark Peasley, *It's Time for an American (Data Protection) Revolution*, 52 AKRON L. REV. 911, 912 (2018) (stating number of people exposed by Equifax data breach is greater than the working population of the U.S). The patchwork of U.S. legislation regulating this industry has consistently proven inadequate for managing these firms, and for enforcing compliance. *Id.* at 916-926, 943.

[23] There has been very little broad legal and corporate reform within the U.S. with regards to privacy or data management in general. Paul Lambet, *Equifax Data Breach: 143 Million Only Tip of the Iceberg*, 1 INT'L J. DATA PROTECTION OFFICER, PRIVACY OFFICER & PRIVACY COUNS. 30, 33-34 (2017) (stating delayed responses, a lack of response, forced arbitration, and a general failure to adequately assess and address breaches present in the *Equifax* crisis show an overall need for data privacy reform).

[24] *Id.* (stating G.D.P.R. guidelines significantly increase required consent and disclosure standards for companies gathering and storing data).

substantial brand damage,[25] revenue loss,[26] legal and administrative fines,[27] and lawsuits. [28] Mitigating the risks data poses with proper data management[29] is arguably almost as important as getting the data, but continued data breaches highlight inadequate U.S. corporate and regulatory responses. In today's high-tech world, protecting data is essential to protecting corporate revenue streams; absent necessary precautions, data can become valueless as theft can destroy the intrinsic value of the data, or cost the corporation more than it is worth.[30]

If the E-Discovery process touches E.U. data, it triggers G.D.P.R. provisions placing litigants in a precarious position.[31] Furthermore, the data being requested need not come from the

---

[25] *No Place to Hide – The Effect of a Data Breach on Brand Value*, SGR: ATTORNEYS AT LAW: SGR BLOG, (Feb. 15, 2020), https://www.sgrlaw.com/no-place-to-hide-the-effect-of-a-data-breach-on-brand-value/. In addition to brand damage for both small and large firms, "data breaches can diminish the value of a company, impact stock performance, and can directly result in a lower purchase price for an acquisition." *Id*.

[26] Nearly a third of businesses suffering a breach lose revenue. *See Data Security Breach: 5 Consequences for Your Business*, THE AME GROUP, https://www.theamegroup.com/security-breach/, (last visited Feb. 15, 2020). Of those who lost revenue, "38% [lost] 20% or more." *Id*.

[27] *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FTC, (Jul. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions. This penalty is "one of the largest penalties ever assessed by the U.S. government for any violation." *Id*. The investigation and sanctions were in response to Facebook's third party sales of user information, frequently without any notification to those users that their data was being sold. *Id*.

[28] *See Data Breach Lawsuit*, CLASSACTION.COM, (Nov. 30 2018), https://www.classaction.com/data-breach/lawsuit/ (stating Marriott breach resulted in a class action suit). "When a company fails to exercise reasonable care in protecting customers' information, affected consumers may be able to file a class action lawsuit." *Id*.

[29] *See* Glen Rabie, *How to mitigate data risk in your organization*, https://www.yellowfinbi.com/blog/2019/07/how-to-mitigate-data-risk-in-your-organization, (last visited Feb. 15, 2020) (stating centralization, eliminating unnecessary copying, limiting access, and promoting "consistent business logic" all help reduce data risks). Data must be managed centrally to ensure risk minimization. *Id*.

[30] AMCA filed bankruptcy after more than $4.2 million in breach related costs not counting brand damage, client loss, and civil suits that followed the breach. *See From Data Breach to Bankruptcy – A Cautionary Tale for Those without Cyber Insurance*, PILLSBURY POLICYHOLDER PULSE BLOG, (Jul. 16, 2019), https://www.jdsupra.com/legalnews/from-data-breach-to-bankruptcy-a-17755/ (finding unnoticed breach lasting nearly a year allowed data for millions of individuals to be stolen, and resulted in the eventual bankruptcy of the parent corporation).

[31] "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or

E.U. to fall under the G.D.P.R.[32] Data handling procedures during and after litigation are also relevant in determining liability for privacy violations, and these costs must be considered before commencing litigation. Existing laws reward even attempted compliance through reduced sanctions, giving compliance an added financial benefit.[33] As data storage increases, the chance that a piece of it will fall under state or foreign government privacy regulations increases. Tailoring E-Discovery requests can prospectively reduce data risks without increasing costs, and work with proactive data management and privacy policies to limit data liability footprints. Therefore, firms should limit requests for private or sensitive data, and courts should encourage them when they fail in this regard.

The first two parts of this Note will address the differing legal approaches to privacy in the E.U. and the U.S., and the damage of inadequate data security.[34] The third part of this Note

---

to another international organization. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined." GDPR Ch5 art. 44.

Additionally, "In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available." GDPR Art. 46. Furthermore, the article specifies the manner and quality of the conditions and safeguards that must be in place for a transfer to occur. *Id.* It also incorporates the corporate rules of Article 47, and subjects the transfer and data handling to GDPR supervisory authority. *Id.*

[32] Todd Ehret, *Data Privacy and GDPR at One Year, a U.S. Prospective. Part One - Report* Card, REUTERS, (May 22 2019), https://www.reuters.com/article/bc-finreg-gdpr-one-year-report-card-part/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-one-report-card-idUSKCN1SS2K5. "GDPR applies to all online interactions with EU citizens no matter where in the world the business is taking place. It includes enhanced requirements regarding consent to use, and includes a "right to be forgotten" – or removed from the record — which is one of the more problematic challenges from a U.S. perspective." *Id.*

[33] The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557, 575 (2018) (finding internal privacy protections for data handling reduce breach damage and governmental sanctions).

[34] Natasha Lomas, *WTF is GDPR?*, TECH CRUNCH, (Jan. 20, 2018), https://techcrunch.com/2018/01/20/wtf-is-gdpr/. "A major point of note right off the bat is that GDPR does not merely apply to E.U. businesses; any entities processing the personal data of EU citizens need to comply. Facebook, for example — a US company that handles massive amounts of Europeans' personal data — is going to have to rework multiple business processes to comply with the new rules. Indeed, it's been working on this for a long time already." *Id.* This includes creating a new position at large data firms titled Data Protection Officers or DPOs. *Id.*

will discuss privacy as a proportionality factor in U.S. Discovery to be balanced alongside Discovery's need for open data disclosure. The fourth will show how courts have responded to the compliance requirements and compliance costs of the G.D.P.R. The fifth will argue why courts need to be more privacy conscious in setting data management guidelines, and in determining how to limit E-Discovery under existing proportionality standards. The sixth part will argue the U.S.'s current piecemeal approach to privacy requires clearer Federal guidance to increase its consistency.[35] Lastly, this Note will address Discovery cost shifting tools available to courts that can be used to encourage better privacy and data handling practices in litigation.

II. BACKGROUND

E.U. privacy law and policy differ substantially from U.S. law. However, both populations suffer when electronically stored data – sometimes referred to as ESI – is stolen or misappropriated, especially through data breaches. Ongoing tension between countries' differing approaches to data privacy – legal rights, handling and storage guidelines, and enforcement – create unique issues during U.S. Discovery in cross-border data transfers, or in data transfers involving foreign citizens' or foreign corporations' data. One goal of modern privacy law restrictions and standards on data transfers is to curtail electronic data abuses, and give citizens better protection and control over their stored data, including data sought for trials.

[35] Corporations can avoid unnecessary risks by applying a global standard to all data they process that meets GDPR minimums. *Id*. It is not just the comprehensiveness of the regulation that poses a problem for corporate data handlers, E.U. regulators have greater authority now to impose sanctions and fines on firms for violations. "Privacy experts suggest that the really big change here is around enforcement. Because while the E.U. has had long established data protection standards and rules — and treats privacy as a fundamental right — its regulators have lacked the teeth to command compliance." *Id*.

A. The E.U. Approach to Privacy

Because of their citizens' historical experience with governmental data abuse, the E.U. has robust privacy regulations.[36] Preventing data abuse is considered an essential governmental function, and E.U. citizens have "comprehensive privacy rights across all sectors."[37] The Charter of Fundamental Rights of the E.U. establishes that the "sanctity of these rights is essential to Europeans."[38] The G.D.P.R. is their regulatory response to rising global concerns over data misuse, data breaches, and the increasing importance of data protection.[39] Its extraterritoriality provisions provide better protection to E.U. citizens by enabling E.U. data officials, Data Protection Officers ("D.P.O.s"), to prosecute data handlers in violation of the regulation whether they are handling data in the E.U. or not.[40]

The G.D.P.R. is broader in defining personal data than the various U.S. laws for data management,[41] and the standards themselves are stringent.[42] Organizing and classifying data for

---

[36] Michael L. Rustad &Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 372-373 (2019) (stating much of EU privacy policy radiates from World War II data abuses perpetrated by the Nazis who exploited data for nefarious ends).

[37] *Id.*

[38] *Id.*

[39] Moreover, despite the obvious need for reform, lawmakers have failed to timely respond to the growing threat that unsecured data poses to consumers, and nearly all of the responsibility is on firms collecting data as these leaks are more frequently insider jobs. *See GDPR and the End of the Internet's Grand* Bargain, HARV. BUS. REV., (Apr. 9, 2018). "Until now, a fast-spreading epidemic of data misuse incidents has been largely overlooked by lawmakers, including breaches and data misuse at Yahoo, Facebook, Target, Equifax, and Under Armour. Though each incident generates its own round of hearings and regulatory fines, basic privacy law has remained unchanged." *Id*.

[40] *Id.*

[41] *EU General Data Protection Regulation (GDPR)* art. 4, 2016 O.J. L 119/1 Definitions (defining relevant terms, services, and impacted business sectors covered by the legislation). Covered data types include personal data, genetic data, biometric data, and health data. *Id*. The sweeping categorizations are a part of why the regulation is unprecedented.

[42] *EU General Data Protection Regulation (GDPR)* art. 5, 2016 O.J. L 119/1 Principles Relating to Processing of Personal Data. Many of the changes reflect the growing desire for transparency in data use, and the ability to have one's data deleted upon request. *Id*. Furthermore, data minimization is also advanced as it represents the best chance

G.D.P.R. compliance can be one of the largest regulatory expenses for a firm, and sanctions for breaches under the G.D.P.R. can amount to billions of dollars.[43] It also imposes burdens on companies to develop more sophisticated data management procedures for data storage, encryption, and deletion, and ignorance does not absolve non-compliance.[44] Furthermore, data handling under the G.D.P.R. is broadly defined, and compliance with local laws in no way protects handlers from foreign sanctions and fines.[45] For instance, the G.D.P.R.'s breach disclosure requirements represent a marked difference to other existing standards.[46]

Acknowledging modern technology, the G.D.P.R. places a 72-hour requirement on disclosing a data breach that is significantly less than any U.S. standards.[47] E.U. guidelines also impose transparency standards on data requests for the underlying need for the data, the data's relevance to the issue, the accuracy of the data, and the duration the data will be kept.[48] E.U. citizens also have a right to correct inaccurate electronic data, request its deletion, and to review

---

of preventing data misuse or loss. *Id*. (stating data use should be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed").

[43] Voss & Houser *supra* note 13 at 307-308 (stating California recently implemented a privacy regime similar to the GDPR; the California Consumer Privacy Act of 2018 broadly defines personal data, and subjects companies meeting certain threshold requirements to fines and sanctions for privacy violations).

[44] The Sedona Conference, *Commentary on Information Governance*, Second Edition, 20 SEDONA CONF. J. 95, 139-145 (2019) (finding better data management allows for better protection, retrieval, and compliance with regulatory systems).

[45] *Id.*; *see also* Craig D. Cannon, et al, *The Future of U.S. Pretrial Discovery Involving European Union Data after Salt River*, 27 ABA 1-4 (2019) (finding EU definition for data processing is "wholly different than it is elsewhere." *Id*. Furthermore, personal data is broadly defined to include many categories of information pertaining to a person's mental or physical attributes, as well as their "on-line" attributes like their IP address. *Id.*

[46] Aaron Tantleff, *Applying the GDPR Rules to the Equifax 143M Data Breach, 2 Int'l J. Data Protection Officer*, PRIVACY OFFICER & PRIVACY COUNS. 8-9 (2018).

[47] *Id.*

[48] Mark Austrian and Christopher Loeffler, *Cross-Border E-Discovery Meets Data Privacy Protection in the European Union*, 26 ABA 3-6 (2018) (stating the Sedona Conference advocates a tri-part structure to minimize conflict including a compliance plan, phased discovery, and protective orders extending special protections to EU citizens' data).

what data is being stored.[49] These requirements, and the way the E.U.'s D.P.O.s enforce them, will necessitate careful evaluation of ongoing privacy requirements, and coordination between litigants and experts to determine when they apply and how to meet them.[50]

Because of the broad definitions contained within it, the G.D.P.R. expands privacy liability significantly.[51] Data processing within it includes "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[52] Essentially, if relevant e-data is involved, the G.D.P.R imposes standards on how that data should be handled, and liability extends to storage and processing of data before and after litigation as well.[53]

[49] The G.D.P.R. grants individuals a right to be informed of data storage and use, including the right to see any automated profiling being conducted with their data. Information Commissioners Office, *Guide to the General Data Protection Regulation: Individual Rights*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/, (last visited Mar. 3, 2020) (stating data handlers to must also inform subjects of any new uses of their data). Data handlers must also provide contact information for the subjects Data Protection Officer, the purpose for processing their data, the legal authority for processing their data, the legitimate interest, the categories of data being processed, the potential recipients of the data, details concerning data transfers, the estimated retention period for data storage, and more. *Id*. Users also have a right to withdraw consent regarding their data storage, flag violations, and discover the source of the data being stored. *Id*.

[50] *Id*.

[51] *IP Addresses and the GDPR*, DBS, (Aug. 2, 2018), https://www.dbswebsite.com/blog/ip-addresses-gdpr/ (stating IP addresses fall under "personally-identifiable information," leading to conflicts with how businesses currently track users). While typically anonymized, IP address storage still presents an issue that the E.U. has yet to clarify. *Id*.

[52] The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 33 (2019) (finding E-discovery issues implicate the SCA as well, but overall focus is on "preservation and collection; relevance and proportionality; possession, custody, and control").

[53] Eric Schwarz, *Practical Considerations for Cross-Border Discover under the General Data Protection Regulation*, EYGM at 2-4, (2018).

The G.D.P.R.'s higher fines[54] make the underlying privacy issues in Discovery more relevant to litigants handling data for E.U. citizens, but U.S. privacy jurisprudence has long been incongruous with foreign views on data privacy rights and judicial access to data.[55]

B. The U.S. Approach to Privacy

Unlike the E.U., the U.S. approach to privacy lacks a unified enforcement body, varies by State, and does not protect personal information.[56] Constitutional support for the right to privacy is derived from the Fourth Amendment, and incorporated under the Fourteenth Amendment to apply to the states.[57] Courts have also held that reasonable expectations of privacy can sustain a tort claim.[58] U.S. privacy law, however, has played more of a gap filler role, as broad privacy

---

[54] Natasha Lomas, *WTF is GDPR?*, TECH CRUNCH, (Jan. 20, 2018), https://techcrunch.com/2018/01/20/wtf-is-gdpr/. "The maximum fine that organizations can be hit with for the most serious infringements of the regulation is 4% of their global annual turnover (or €20M, whichever is greater). Though data protection agencies will of course be able to impose smaller fines too. And, indeed, there's a tiered system of fines — with a lower level of penalties of up to 2% of global turnover (or €10M)." Because of the enormous revenue streams many tech companies have all over the world, the GDPR's fee structure is progressive. This ensures companies cannot accept fines as a cost of doing business without improving data policies." *Id*. *Cf* Sean J. Griffith, *Corporate Governance in an Era of Compliance*, 57 WM. & MARY L. REV. 2075 (2016) (finding corporations weigh competing costs to determine whether compliance or sanctions will be cheaper).

"It's not necessarily the case that individual EU Member States are getting stronger privacy laws as a consequence of GDPR (in some instances countries have arguably had higher standards in their domestic law). But the beefing up of enforcement that's baked into the new regime means there's a better opportunity for DPAs to start to bark and bite like proper watchdogs." *See Id.*

[55] Cannon, *et al*, 27 ABA 2019 *supra* note 46 (finding historical tension between pretrial discovery and E.U. privacy approach).

[56] Several States have enacted heightened privacy laws including California, New York, Maryland, Massachusetts, Hawaii, and North Dakota; however, even amongst these states there are differences in what rights are available to consumers. *See* Andy Green, *Complete Guide to Privacy Laws in the US*, INSIDE OUT SECURITY BLOG, (Mar. 29, 2020), https://www.varonis.com/blog/us-privacy-laws/ (stating only New York allows users a right to correct, while other States still offer other privacy protections such as the right to delete and right to access stored electronic data).

[57] *See* Voss & Houser *supra* note 13 at 296. *See also* Griswold v Connecticut, 381 U.S. 479, 494 (1965) (holding privacy is" a fundamental personal right emanating from" the Constitution). The Court found historical underpinnings for the right to privacy, as well support within the 4th, 5th, and 9th amendments of the Bill of Rights. *Id.*

[58] *See* Voss & Houser *supra* note 13.

laws have been disfavored over narrower laws protecting specific classes of data, like medical records.[59]

Moreover, a belief that lower regulatory standards foster corporate growth has prevailed in the U.S.[60] However, recent scandals like the 2017 Equifax data breach prove corporations are not adequately protecting data.[61] The U.S. regulatory enforcement for data loss events has simply not stopped this trend.[62] Typically, proceedings are private, and reforms are necessarily

[59] *Id*. at 301. The FTC, for instance, has passed a variety of acts protecting digital privacy; however, because of their fundamental differences, E.U. law has long considered U.S. privacy laws to be inadequate. *Id.* Currently, both nations have agreed to the E.U.-U.S. Privacy Shield ("Privacy Shield Agreement") for data transfers of personal information from the E.U. to the U.S to mitigate these concerns; there are still areas covered by the agreement that the E.U. has pointed out as potential problems. *Id*.

[60] Banking, energy, and airlines have all lobbied for deregulation to foster greater competitive advantage at one time or another. Kimberly Amadeo, *The Balance: Deregulation Pros, Cons, and Examples*, THE BALANCE, (Jan. 16 2020), https://www.thebalance.com/deregulation-definition-pros-cons-examples-3305921, (finding industry lobbying can promote deregulation, which may foster growth, but also produces negative externalities).

Furthermore, some U.S. commentators find the political pay-to-play environment in the U.S. to be responsive more to money than problem solving, CED REPORT *supra* note 11, https://www.ced.org/reports/regulation-and-the-economy. "Government decisions are more susceptible to bias through the influence of special-interest money and politics, whereas free market outcomes are impartial to all the different participants in the marketplace who clearly signal values through the prices they are willing to pay or receive." *Id*.

[61] The initial breach was relatively minor, but continued exploitation of the security weakness allowed hackers to continue to gather data. Lambet *supra* note 24 at 32 (finding general failure to address and assess breaches during Equifax crisis shows need for privacy and data management reforms in corporate setting, and provides teaching example for other data handlers). By the time the breach was caught, and security measures were improved, data for millions of U.S. citizens was lost to hackers. *Equifax Data Breach Settlement*, FCC, (Jan. 22, 2020), https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement (stating personal information for 147 million people was exposed in Equifax breach, and providing details for victim relief in the U.S. and U.S. territories).

[62] *See The Capital One Data Breach is Alarming, but These are the 5 Worst Corporate Hacks*, ABC NEWS, (Jul. 30, 2019), https://abcnews.go.com/Technology/marriotts-data-breach-large-largest-worst-corporate-hacks/story?id=59520391, (attributing top 2 worst data breaches to the same company, Yahoo, despite Federal Agency sanctions).

retroactive since the standards are not known in advance.[63] Variance in U.S. privacy law also extends data breach reporting up to two months in some jurisdictions.[64]

U.S. Federal privacy regulations for consumers are primarily handled by the Federal Trade Commission ("F.T.C."),[65] though other agencies like the Securities and Exchange Commission ("S.E.C.") play a role in regulating specific types of information like financial data.[66] Specific U.S. industries are subject to more stringent requirements than even the E.U.'s guidelines, but most are less regulated.[67] Lacking rulemaking authority,[68] the F.T.C. works

---

[63] *See generally* Daniel Goldberger; Nick Akerman; Joanna Levin; David Ray, *Fall 2016 Cross-Border Data Privacy Issues*, 25 CARDOZO J. INT'L & COMP. L. 379, 385 (2017) (stating FTC has brought enforcement actions against corporations for noncompliance with data management). The credit card industry has sued in such instances as well where the data losses create costs like card replacement and fraud prevention. *Id.*

[64] *See id.*

[65] "There is no single principle data protection legislation in the United States. Rather, a jumble of hundreds of laws enacted on both the federal and state levels serve to protect the personal data of U.S. residents." *USA: Data Protection 2019*, ICLG, (Mar. 7, 2019), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa. "At the federal level, the Federal Trade Commission Act (15 U.S.C. § 41 *et seq*.) broadly empowers the U.S. Federal Trade Commission (FTC) to bring enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy data protection regulations." *Id*.

[66] *Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies*, RISK ALERT, (Apr. 16, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf. "Regulation S-P, among other things, requires a registrant to: (1) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices generally no later than when it establishes a customer relationship ("Initial Privacy Notice"), (2) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship ("Annual Privacy Notice," and together with the Initial Privacy Notice, "Privacy Notices"), and (3) deliver a clear and conspicuous notice to its customers that accurately explains the right to opt out of some disclosures of non-public personal information about the customer to nonaffiliated third parties ("Opt-Out Notice")." *Id*.

[67] Rustad & Koenig, 71 FLA. L. REV. 365, *supra* note 37 at (2019). But areas not covered by the narrowly tailored regulations are without protection, thereby exposing US citizens' data. *Id.* at 381. The mixed legal classifications lead to widely varying privacy standards that ultimately make privacy compliance more difficult. *Id*. at 388-389.

[68] *A Guide to the Rulemaking Process*, OFFICE OF THE FEDERAL REGISTER, https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf , (last visited May 30, 2020) (stating rulemaking requires Congressional authorization for an agency to begin the pre-proposal process which culminates in the issuance of a final rule after a public notice and comment period). The Executive branch oversees the process, and gives guidance on the rule, which is also subject to Judicial review. *Id*. at 10-11 (stating rule is also subject to Congressional oversight through Congressional Review Act allowing Congress to veto rules). *See also* John Egerton, *FTC's Simons: We Need Rulemaking Authority*, (Nov. 27, 2018), https://www.broadcastingcable.com/news/ftcs-simons-we-need-rulemaking-authority (stating FTC chairman Simons requested rulemaking authority as part of an overhaul to better protect consumer privacy).

annually to reduce identity theft and data breaches in the U.S. through enforcement actions against corporations for exaggerating data security measures, inadequate customer support, data breach disclosure failures, failure to implement "physical, electronic, and managerial procedures to protect consumers' personal information," deceptive enrollment practices, and deceptive privacy policies in general.[69] The F.T.C. periodically issues comments on device and information security to "mitigate against privacy and security risks."[70]

Many of the programs the F.T.C. mandates for consumer privacy protection require data management protocols be enacted to help predict security weaknesses, and to develop adequate industry-specific protections based on the data being handled.[71] Consequently, organizations need to know which regulations apply in order to mitigate associated legal risks.[72] Various Federal requirements also criminalize noncompliance with respect to current breach disclosure standards,[73] so knowing what law applies is essential.

---

[69] *Privacy Data Security Update 2018*, Fed. Trade Comm'n, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf, (last visited Mar. 3, 2020). Settlements typically include monetary fines and compliance updates. *Id*. *See also* Fed. Trade Comm'n, *Equifax to Pay $575 Million as Part of Settlement with* FTC, https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related (concluding Equifax's violations required designating information security oversight employee, annual data risk assessments and technology review, certification on security compliance, continued testing and monitoring, and ensuring down-chain compliance with other data handlers) (July 22, 2019).

[70] FTC Privacy Update 2018 *supra note 70*. They have also called on Congress to pass privacy legislation for them to enforce as a Federal standard. *Id*. The continued absence of an overarching privacy standard has hindered the meaningful advancement of data privacy regulation in the U.S.

[71] *Id*. The FTC also hosts workshops to explain to various stakeholders and corporate insiders the importance of proper data management policies. *Id*. They also provide guidance to consumers and small business owners on cybersecurity issues. *Id*.

[72] *Id.*

[73] Privacy Act of 1974, 5 U.S.C. §552(a) (outlining methods for private individuals to control and monitor data). *See generally* Michael Bloom, *Protecting Personal Data: A Model Data Security and Breach Notification Statute*, 925 Johns. L. Rev. 977, 980-993 (2019) (stating current law is inadequate, and Federal standards should be implemented containing various state and federal law provisions already in place to create a more comprehensive standard for breach monitoring and reporting).

Legally, there is a view that data loss does not represent an actionable harm which precludes a finding of liability in the limited privacy tort claims available to citizens, and varying regional standards make this even less actionable.[74] Indeed, data protection laws have evolved in the U.S. courts to provide limited protection.[75]

a. Modern Privacy Laws Curtail Data Loss and Fallout

Data and privacy policy failures are managerial failures[76] that cost corporations and consumers alike.[77] Inadequate data security and privacy consideration cause significant losses of sensitive user data, costly and uncertain litigation, substantial brand damage, a loss of

[74]Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 659 (2019) (stating elimination of the "harm problem" in litigating privacy issues will provide plaintiffs better access to relief in court and in settlements). Laws necessarily interfere with contractual relationships between corporations and individuals; focusing properly on providing the correct remedy to individuals, and incentives to corporations, ensures the law is altering the appropriate aspects of these interactions to improve interactional outcomes for all parties. *Id.*

[75] *See generally* Roe v Wade, 410 U.S. 113, (1973) (stating broad meaning of liberty was meant to expand overtime, and includes a right to personal privacy contained within "penumbras of the Bill of Rights"). While the judicial concern in these cases was the right to privacy from the government, the same concerns apply to businesses uniquely positioned to exploit consumer data, like Equifax. *See also* Rustad & Koenig, *Towards A Global Data Privacy Standard*, 71 FLA. L. REV. 365, 372-373 (2019) (stating language in U.S. law is similar to that used by E.U. regulations)

[76] Jason Asbury, Maria McClelland, Kris Torgerson, India Vincent; Jennifer Boling, *Law and Business Technology: Cyber Security & Data Privacy Update*, 20 Tenn. J. Bus. L. 1065, 1088 (2019) (stressing importance of IT's role in explaining the importance of data privacy to management, and the need for better communication between leadership and IT). Ignorance is always an issue – either with regards to the underlying technology, or the protection of the information it stores. *Id*.

[77] Equifax was exposed to $575-$700 million in administrative fines and victim compensation funding in post-data breach actions. *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FTC, (Jul. 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related. , Shareholders and consumers ultimately foot the bill for data governance failures. *Id.*

The FTC required multiple compliance updates to Equifax's data handling and privacy practices as well; consequently, Equifax could have avoided a substantial percentage of its burden to the FTC by implementing reasonable data safeguards beforehand through a privacy-by-design approach. *See* Edith Ramirez, *Privacy By Design Conference*, FTC, (Jun. 13, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf (compelling institution of broad privacy compliance program for Facebook with employees responsible for protecting consumer privacy and conducting risk assessments with regards to data usage and permission)

stakeholder confidence, and increased administrative liability.[78] Consequently, a primary goal of modern privacy legislation is to curtail data mismanagement by expanding data rights and fines for violating them.[79] By granting citizens a right to access their data, review the data stored, and request its deletion, the G.D.P.R. permits a greater level of control over private data that can help curtail both data abuse and potential breach damage.[80] Proper data management is important, and not just because of recent personal data loss, breach events expose governments as well.[81] The

[78] Goldberger, *supra* note 64, at 395 (finding data breaches are typically a spur to new privacy laws).

[79] "GDPR stands for General Data Protection Regulation also referred to as Regulation (EU) 2016/679. GDPR replaces the existing protection directive that was introduced in 1995 and has been created by the European Parliament, the Council of the European Union and the European Commission to strengthen and unify data protection for all residents of the European Union." *What is GDPR? A Quick Reference Guide to the General Data Protection Regulation*, OUR IT DEPARTMENT, https://www.ouritdept.co.uk/what-is-gdpr/#3, (last visited Feb. 15, 2020). Goals include increasing data rights for E.U. citizens, helping citizens understand personal data usage, address exportation of E.U. citizens' data, increase regulatory authority over organizations breaching data protection regulations, simplify international regulatory standards for data, and require that all organizations handling E.U. data comply with new Privacy by Design rules. *Id*.

[80] Information Commissioners Office, *supra* note 50.

[81] Data can mean trade secrets, client information, or even State secrets. *See* Tim Shorrock, *Why does WikiLeaks keep publishing U.S. state secrets?*, Washington Post, (Apr. 16, 2017), https://www.washingtonpost.com/posteverything/wp/2017/03/16/the-reason-wikileaks-receives-so-many-u-s-state-secrets-private-contractors/ (stating governmental reliance on contractors to implement adequate data management policies has resulted in "catastrophic mistakes" including the Edward Snowden leaks). Furthermore, domestic and foreign operatives have stolen classified information in order to aid reverse engineering programs; ultimately, inherent flaws in the "privatized intelligence" industry have created substantial data risks that are unaddressed by existing standards. *Id.*

A data breach is "an unauthorized disclosure of personal information;" the Equifax data breach lost data belonging to 145 million users. Caitlin Kenny, Note, *The Equifax Data Breach and the Resulting Legal Recourse*, 13 Brook. J. Corp. Fin. & Com. L. 215-217 (2018) (stating 145 million users had sensitive data exposed including credit information). "The severity only increases when an agency that is given massive authority and access to millions of consumers' personal information is breached." *Id*. (stating technology available for black market hacking has increased and exacerbated the problem, and led to higher exposure of sensitive personal information).

Firms are frequently unaware that a breach has even occurred. Once they are aware, a process is undertaken to ascertain what data was lost, if that data was sensitive, who that data belonged to, where the company's ultimate liabilities lie, and whether or not any disclosure is required on their part to consumers, shareholders, government regulators, or the world at large. The knee-jerk reaction is to say every breach should be disclosed, but the information lost determines whether or not disclosure is necessary, not public opinion; therefore, some information can be lost without consumers ever knowing hackers have it for sale.

fact that data breaches have also increased over time, makes the underlying issues more relevant every day.[82, 83]

Traditional U.S. privacy violation sanctions are retrospective in nature, and the U.S. corporate response to privacy has been likewise reactive rather than proactive.[84] A wait-and-breach approach prevails in an area where proactivity is critical.[85] U.S. corporations, like Equifax, have failed to timely disclose breaches, materially misrepresented their security capabilities, and engaged in post-breach insider trading, all in violation of current S.E.C. and F.T.C. standards.[86] Yet, it is unclear what benefit if any can be derived from fining and sanctioning firms for non-compliance, as they continue to lose data despite them.[87] Costs

[82] From 2016 to 2017 alone there was a 29% increase in the number of data breaches tracked by the Identity Theft Resource Center and an almost 2% increase in breach size. *See* Kenny, *supra* note 75.

[83] Brian Barrett, *Security News this Week: Russia's SolarWinds Hack is a Historic Mess*, WIRED: SECURITY, (Dec. 19, 2020), https://www.wired.com/story/russia-solarwinds-hack-roundup/ (finding known software weakness in governmental agencies was exploited via malware that circumvented the US's "Einstein" cyber security detection system, which focuses exclusively on incoming threats). Not only did the government know as early as 2018 that this weakness existed, but they also chose to do nothing about it. *Id*; *see also* Sean Lyngaas, *Microsoft identifies second hacking group affecting SolarWinds software*, CYBERSCOOP: TECHNOLOGY, (Dec. 21, 2020), https://www.cyberscoop.com/microsoft-solar-winds-hackers-supernova-backdoor/ (stating second hack, unrelated to Russian hack, also compromised SolarWinds software, which is used broadly in corporate and governmental cyber security setups). The full extent and fallout from the SolarWinds hack will not be felt for years – but the message is still very clear: our data needs better protection.

[84] Voss & Houser, *supra* note 13.

[85] *Id.* at 341 (stating an ethical approach to data fosters good will as well).

See also Aaron Tantleff, PRIVACY OFFICER & PRIVACY COUNS. 8 *supra* note 47 (2018) (stating current U.S. laws are a patchwork of responsive mechanisms, and finding new EU regulatory scheme imposes significant breach response obligations on corporations handling relevant data).

[86] Equifax executives informed clients that their data security was top notch; furthermore, despite knowledge of the data breach, executives failed to disclose the information to relevant stock purchasers. In re Equifax Inc. Sec. Litig., 357 F. SUPP. 3D 1189, 1207 (N.D. Georg 2019) (finding material misrepresentation of stock value and data security standards by CEO "concerning a core business operation could be highly relevant to analysts evaluating Equifax's stock."). *See also* Tantleff, *supra* note 86.

[87] Tash Bottum, Note, *Material Breach & Disclosure*, 103 MINN. L. REV. 2095-2102 (2019) (finding continuing rise of breaches causes negative effects for corporate growth).

associated with data breaches are already astronomical.[88] However, delayed responses, a lack of response, forced arbitration, and a general failure to adequately assess and address breaches show an overall need for data handling and privacy reform in the U.S.[89] Overreliance on judicial and corporate discretion in U.S. data management has produced a fairly lax data environment—one that the G.D.P.R. seeks to curtail.[90]

C. Balancing Privacy and Data Needs in Discovery

Discovery of electronic data is an important step in U.S. litigation, and it has significant privacy implications as it involves data being transferred between companies and countries. U.S. pretrial Discovery, including E-Discovery, has no equivalent in most countries,[91] including the E.U. The open nature of U.S. Discovery requires litigating parties to disclose non-privileged information pertaining to relevant claims or defenses.[92] Discovery is broad, and may require disclosure of materials that are inadmissible as evidence.[93] However, parties can dispute the relevance of a Discovery request,[94] and can also limit disclosures on other grounds including

[88] *Id.* at 2124-25 (stating the bulk of costs associated with any class action suit will go towards litigating the issue, and will not provide an adequate financial remedy to damaged victims.)

[89] Lambet, *supra* note 24, at 34-35 (stating corporations need to engage data protection professionals who are aware of the issues and responsibilities imposed on them by the competing interests involved with big data; furthermore, preparing an adequate, timely response to any eventual breach is paramount to handling what is likely to be a very public inquiry into a data breach event).

[90] *O'Connor, supra* note 5.

[91] Birgit Kurtz, *U.S. Discovery: An Introduction*, 37 DAJV NEWSL. 6 (2012) (finding U.S. proceedings, especially discovery, very different from civil cases elsewhere).

[92] Fed. R. Civ. P. 26(b)(1) (stating disclosures include "existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter."). *See also* Kurtz, *supra* note 92, at 7 (stating purpose is to ensure both parties are "informed of all of the evidence of the other parties" prior to trial).

[93] Kurtz, *supra* note 92 (stating materials that may "arguably lead to the discovery of admissible evidence" must be included in discovery disclosures).

[94] *Id.* (stating parties resisting Discovery requests can assert privilege, or otherwise challenge a discovery request, and may seek a protective order to limit or block the disclosure of protected or irrelevant information).

privacy or foreign law conflicts.[95] Because of the burdens E-Discovery can impose on parties, it is already used as a tool to discourage litigation, and increasing costs makes it a more effective one.[96]

Courts do not typically involve themselves in the data management practices, or privacy rights issues, implicated by Discovery in general.[97] As a result—despite current legal safeguards—U.S. courts do not consistently protect data privacy rights.[98] A hands off approach prevails,[99] and litigants are encouraged to decide how to classify and handle information without judicial intervention.[100] The 2015 amendments to the Federal Rules of Civil Procedures ("Federal Rules") were aimed at reforming the U.S. Discovery process.[101] The Federal Rules aim

---

[95] Tarifa B. Laddon, *Navigating between U.S. Discovery and European Data - Protection Laws*, 38 LITIG. 10, 11 (2012) (stating litigants must address international data regulations during Discovery). Even where foreign laws permit a particular transfer, litigants can still argue production and protection of the data will place an undue burden, or a disproportionate burden, on their party. *Id.*

[96] Anna A. Ismer, *Bending the Rules: The Circuit Courts Inconsistent Application of the Federal Rules and Section 1920(4) in Cost Shifting and Taxing Electronic Discovery Costs*, 18 FLA. COASTAL L. REV. 129, 141-42 (2017)

[97] Ari Ezra Waldman, *Privacy's Law of Design*, 9 UC IRVINE L. REV. 1239 (2019) (stating legal focus is on consent and control over data with little emphasis on important privacy principles).

[98] K. Alex Khoury, *Electronic Discovery*, 68 MERCER L. REV. 976 (2017) (stating court compelled production of data in" native format"). Typical data protection measures alter the data, but the process is done to protect it. Compelling firms to provide it in a raw format reduces overall data security.

[99] *Data Protection Law*, LEGAL RESOURCES, https://www.hg.org/data-protection.html, (last visited Feb. 15, 2020). ("[H]as followed a policy geared toward allowing the private sector to lead the way in data protection.").

[100] *See* Khoury, *supra* note 99, at 971, 972 (stating process is cooperative in nature).

[101] Federal Rules of Civil Procedure 26(b)(1) (stating need for information requested must be "proportional to the needs of the case, considering the importance of issues at stake in the action, the amount in controversy, the parties' relative access to the relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit").

See also 2015 Amendments to the Federal Rules of Civil Procedure, PRACTICE POINTS, https://www.americanbar.org/groups/litigation/committees/products-liability/practice/2017/2015-amendments-to-frcp/, (last visited Feb. 15, 2020) (finding court now has greater discretion under Fed. Civ. Pro. Rule 26(c) to shift costs between parties based on discretionary factors). There is also increased liability under 37(e) for failing to properly maintain data relevant to litigation even if the data was lost before it began. *Id.*

was to increase cooperation between litigants, place more emphasis on proportionality in Discovery, and encourage more active management of the process by courts.[102]

The Supreme Court has provided greater prominence to proportionality in the update in order to increase judicial efficiency.[103] However, courts still place the burden on litigants to come to terms, and do not take an active approach.[104] They may, however, refuse to compel Discovery where parties have failed to adequately address it in their pretrial meetings, or force disclosure where one party seeks to block it.[105] Similarly, when faced with conflicts of law over data and disagreeing parties, the court will decide how data requests are handled by applying the Supreme Court's comity standards under *Aerospatiale.* [106]

With emphasis on international comity, these standards balance the proportional needs of the interested parties and nations.[107] Among other factors, the cost and burden of the production is weighed against the probable value of the data to the litigation.[108] Consequently, courts have discretion to use standard Discovery procedures despite foreign blocking statutes which seek to

---

[102] Khoury, *supra* note 99, at 973-975 (stating current standards require courts and attorneys alike to consider the proportionality of discovery to the case being litigated; finding cooperation is key to the process, and courts have refused to compel discovery in cases where parties have used it combatively or wastefully).

[103] Michael Thomas Murphy, *Occam's Phaser: Making Proportional Discovery (Finally) Work in Litigation by Requiring Phased Discovery*, 4 STAN. J. COMPLEX LITIG. 89, 96-101 (2016)

[104] *Id*.

[105] Khoury, *supra* note 99, at 972-973. Courts also require disclosure into data handling techniques, and the methods used to preserve and produce it. *Id*. at 974.

[106] *See also* Samantha Cutler, Note, *The Face-off between Data Privacy and Discovery: Why U. S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information*, 59 B.C. L. REV. 1513, 1527 (2018) (Stating appropriate test is "(1) the significance of the requested discovery in regard to the litigation; (2) the precision of the request; (3) whether the requested information was generated in the United States; (4) the availability of an alternate method for acquiring the discovery materials; and (5) the damage to the United States' or foreign nation's concerns if the discovery is not executed."); *see also* Cannon *et al*, 27 ABA 2019 *supra* note 41.

[107] *Id*.

[108] *Id*.

exert more control over data and how it is handled.[109] Congress has also passed legislation on coordinating Discovery with data in different nations.[110] Where parties disagree on how to proceed, courts will decide what standards apply, and may also decide who will pay for them.[111]

Proportionality is relevant in cost shifting as well. *Zubulake* and the 2006 amendments to the Federal Rules provide the current standard for cost shifting in Discovery.[112] Courts apply various balancing tests to determine whether cost shifting is appropriate, and can consider the value of the information, the willingness of either party to bear the costs, the ability of parties to resolve the issue between themselves, accessibility of the data, and the existence of "good cause" underlying the request for the data.[113] Because these costs are significant, conflict over proportionality and costs in discovery is likely to arise – courts have to decide the scope of Discovery, how it will be handled, and who will pay in light of each parties' conflicting

---

[109] *But see* Elvira Sihvola, Note, *Privacy and Political Integrity: How European Data Protection Laws May Limit the Regulation of Foreign Political Interference in U. S. Elections*, 25 COLUM. J. EUR. L. 135, 141-143 (2019) (stating in 2015 E.U. struck down U.S. framework allowing governmental interference with "fundamental rights of persons whose data . . . transferred from the EU to the US". finding the "generalized access" the court had to electronic data "violated the fundamental right to respect for private life."). The subsequently enacted Data Privacy Shield has replaced the former arrangement; however, neither the EU's nor the US's legal interests are completely satisfied by the replacement legislation. *Id.* EU activists as well as EU legislators remain unconvinced as to the efficacy of the Privacy Shield framework; furthermore, US foreign policy regulations may be hampered by provisions within the GDPR and Privacy Shield. *Id.* at 159-166.

[110] *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, Dep't of Justice, (last visited Feb. 2, 2020), www.justice.gov/cloudact (finding passage of the Clarifying Lawful Overseas Use of Data Act has two distinct parts: it authorizes the U.S. to use executive agreements with foreign nations to resolve data law conflicts, and it requires corporations to surrender pertinent investigative data regardless of where it is stored).

[111] Jonathan Remy Nash & Joanna Shepherd, *Aligning Incentives and Cost Allocation in Discovery*, 71 VAND. L. REV. 2015, 2020 (2018) (stating appropriate test is a seven-factor approach).

[112] I*d*. "(1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production compared to the amount in controversy; (4) the total cost of production compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issue at stake in the litigation and; (7) the relative benefits to the parties of obtaining the information." *Id*. at 2020 n.22 (2018).

[113] *Id*.

interests.[114] Approaches to proportionality vary because its impact on E-Discovery is still evolving.[115] Frequently, cooperation between parties is still the primary solution to both how data is handled, how compliance is achieved, and which party will pay for it.[116] Consequently, results in these situations can be hard to predict.

U.S. law allows the processing of personal information that is not protected by specific legislation, including data sought in E-Discovery.[117] However, this poses a problem for firms handling data covered by more restrictive foreign privacy laws.[118] Under the Federal Rules' current framework, firms may seek to curtail E-Discovery, or shift costs, where foreign laws place litigants at greater risk for subsequent suits, or where the costs of meeting those laws greatly increase data production costs.[119] The challenge here is getting U.S. courts to see that the costs are probative, or that the data is sufficiently private to warrant the heightened protections it may be owed under foreign standards. Conversely, the opposing challenge is to point out the value of the data, or to prove why it is not protected by foreign law.

---

[114] Murphy, *supra* note 103, at 104 (stating process of proportionality has a conflict driven element).

[115] Khoury, *supra* note 99, at 971, 980.

[116] Parties may even agree to cost-shifting arrangements beforehand. *See* Ismer, *supra* note 97, at 131-132.

[117] The Sedona Conference, *Commentary and Principles on Jurisdictional Conflict over Transfers of Personal Data Across Borders*, The Sedona Conference (2019 Public Comment Version) https://thesedonaconference.org/sites/default/files/publications/Jurisdictional%20Conflicts%20over%20Transfers%20of%20Personal%20Data%20%282019%29_0.pdf (finding general distinction between public and private data in U.S., rather than focus on personal data in EU law, allows processing of personal data not deemed private).

[118] *Id*. at 1 (stating data linked to a territory gives sovereign rights to that territory in determining how that data is used, transmitted, processed, disseminated, and stored).

[119] *Id.* at 32-38 (stating data localizing laws are used by foreign countries to control citizenry, protect citizens' data from exploitation, encourage appropriate international data prioritization, boost international data security, and limit foreign data extraction); *see generally*, Fed. R. Civ. P. 26(b)(1) (stating relative importance of data to litigation must be weighed against cost of production.

D. The G.D.P.R Seeks to Correct Inadequate Foreign Privacy Protection

The broad reach of the G.D.P.R., and the expansive standards within it, were designed to provide E.U. countries greater control over their data, and more consistency with how it is handled by corporations and courts alike. There exists a long history of tension between E.U. privacy laws and U.S. pretrial Discovery.[120] Transatlantic differences in how data privacy is regulated have created different compliance standards in the E.U. and U.S.[121] The G.D.P.R.'s new requirements make the mostly cooperative U.S. approach to Discovery less viable, as meeting relevant E.U. standards greatly increases costs,[122] making cooperation on what standard applies less likely. E.U. production standards under the G.D.P.R. weigh similar concerns to current U.S. Discovery laws, including proportionality and relevance,[123] but Discovery data requests for E.U. data are not permissible data transfers under the G.D.P.R.[124] Still, in conflict with G.D.P.R. data transfer guidelines, U.S. courts tend to favor disclosure of information under

---

[120] Cannon *et al., supra* note 46, at 1-4 (stating the *Salt River* decision shows a departure from the typical approach of compelling discovery regardless of so-called "blocking statutes").

[121] Voss & Houser, *supra* note 13.

See also Sean J. Griffith, *Corporate Governance in an Era of Compliance*, 57 Wm. & Mary L. Rev. 2075, 2116-2134 (2016) (finding compliance to current regulatory standards, that are the result of sanctions and legal actions instead of proactive regulations or prospective rules, has created compliance policies that are the result of mixed incentives; consequently, they are not policies espoused by shareholders or management, and do not necessarily represent the best interests of the corporation). Mixed incentives in decision making can be a result of extra firm involvement with intrafirm governance decisions. *See id*. at 2079. A compliance approach to privacy ignores agency costs, and fundamentally alters the typical corporate governance approach taken because it is normally a response to administrative action taken against peer corporations. *See also id*. at 2083-2092 (showing governmental use of "carrot-and-stick" in privacy compliance has resulted in heavy fines for corporations, and is used as tool to encourage reform).

[122] Elizabeth E. McGinn, Scott T. Sakiyama, & Brian W. Bartholomay, *Practical Considerations for Litigating Discovery Proportionality*, 64 Prac. Law. 15-17 (2018) (stating courts consistently uphold Discovery requests where the data sought is relevant to the case, notwithstanding the burdens faced by producing the data).

[123] Schwarz, *supra* note 54, at 3 (finding relevance of data and consequences to subjects pertinent).

[124] The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 Sedona Conf. J. 557, 566–67 (2018) (stating competing regulations create conflicts of interest in cross-border litigation due to differing standards present in U.S. E-Discovery and international privacy law).

Discovery laws over international standards by a significant margin.[125] However, G.D.P.R. Discovery compliance still increases the time expenditure and overall costs of litigation involving E.U. citizens' data, and mere cooperation cannot resolve this problem.[126] Additionally, the corporate response to the G.D.P.R. has been more pervasive than previous industry changes spurred by F.T.C. actions, showing its broad reach.[127] Though corporate compliance has not adequately protected consumers in the past, supporters now hope the G.D.P.R. can usher in an era of compliance that will.

The G.D.P.R. is not as generous with granting litigants' discretion.[128] Furthermore, its standards are frequently considered in privacy legislation updates,[129] and some similar provisions have been enacted at the state level.[130] This requires courts and litigants to regard competing legal interests and obligations in handling E-Discovery requests,[131] making data requests in

---

[125] Cannon et al., *supra* note 46 (finding need for specialized legal analysts to be a source of increased costs). *See also* Lambet, *supra* note 24, at 34, 35 (finding increased fines associated with heightened compliance standards).

[126] Cannon et al., *supra* note 46. *See generally also* Lambet, *supra* note 24, at 34, 35.

[127] When the GDPR was initially rolled out, some websites went entirely dark for a few days while legal teams sorted out liability and a response. *See generally* Ryan Browne, *US media websites down in Europe after a huge data law* shakeup, https://www.cnbc.com/2018/05/25/us-media-websites-down-in-europe-after-a-huge-data-law-shakeup.html, (May 25, 2018). Consent forms on some sites were used to subsequently restore access to affected consumers. *Id*. Many sites now have them for any users navigating their content.

[128] Mark Peasley, *It's Time for an American (Data Protection) Revolution*, 52 Akron L. Rev. 911 (2018) (subjecting any data handlers or processors to stringent management and reporting protocols).

[129] Dan Simmons, *12 Countries with GDPR-like Data Privacy Laws*, COMFORTE BLOG (Jan. 17, 2019), https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws (stating Brazil, New Zealand, and South Africa passed their own GDPR-like laws in 2020, while China and Canada are considering bills that also mirror the GDPR).

[130] California Consumer Privacy Act of 2018 (providing GDPR-like provisions for protecting sensitive personal data from governmental and corporate abuse).

[131] *See generally* The Sedona Conference, *supra* note 16, at 611 (stating corporations need to be proactive in notifying authorities of privacy issues in cross-border litigation). The *International Investigations Principles* proposes 8 general principles for managing data in cross border disputes; ultimately, proactive data management policies encourage cooperation between governments, increase faith in the process, and decrease the likelihood of a privacy breach. *id*. at 599-624 (stating principles include developing data identification and transfer protocols, consideration of the competing legal obligations data handlers are subject to as well as risks and costs arising from

cross-border disputes more difficult to resolve.[132] Additionally, the practical considerations of balancing privacy concerns against governmental interests in compelling data transfers through E-Discovery have not been adequately addressed by current E.U. guidance, leaving liability ambiguous.[133] Heightened data standards make expertise on data management more central to litigation as compliance becomes more technical, and costs become more significant and varied based on technical requirements.[134] Courts must understand the costs these new standards impose, evaluate new legal burdens on litigants, and develop consistent methods for handling both.

E. U.S. Courts Handle G.D.P.R. Issues and Costs Inconsistently in Discovery

Judicial application of new proportionality standards for Discovery in handling G.D.P.R. data conflicts produces mixed results for how the data is handled, how it is procured, and the assignation of production costs.[135] Even with clear standards in the G.D.P.R., courts still rely

investigations involving personal data, and early discussions of legal privacy implications and scope of investigation).

[132]*Id*. Any regulation necessarily creates a competing interest between parties' privacy rights and countries' rights to investigate cross-border disputes. *Id.* (stating a good faith, reasonableness standard should be applied to entities' compliance with E-discovery and privacy laws).

[133] Schwarz, *supra* note 54, at 4 (stating enforcement of data subjects' rights can cause conflicts with "needs of responding to either civil discovery or regulatory inquiries in the" [U.S.]).

[134] *See generally* The Sedona Conference, *Primer on Social Media*, 20 SEDONA CONF. J. 1, 21-24 (2019) (stating further that in requesting social media information parties should consider: which sources will likely contain relevant data, who controls the source, the date range associated with the data, relevancy of the data, value of data to the case generally, "dynamic nature" of "user-generated content," formatting of data for production and preservation, privacy concerns arising from data confidentiality). Because discovering the identity of anonymous users is expensive, and can be "difficult and lengthy," follow-up litigation can be even more costly and time consuming. *Id*. at 11-20, 40-45.

[135] *See generally Finjan, Inc. v. Zscaler, Inc.*, No. 17-cv-06946-JST (KAW), 2019 U.S. Dist. LEXIS 24570; *Corel Software, LLC v. Microsoft Corp.*, No. 2:15-cv-00528-JNP-PMW, 2018 U.S Dist. LEXIS 172875; *Microsoft Corp. v. United States* 829 F.3d 197 (2d Cir.2016).

overly on cooperation between parties during Discovery,[136] and fail to take proactive data protection measures through a "privacy by design" approach to Discovery and litigation generally.[137] Ongoing issues between conflicting legal spheres for investigations involving multinational data management and mergers and acquisitions between multinational firms, present multi-headed compliance problems,[138] made worse by a lack of direction. Adding to the issue, liability exists not only for inadequate safeguards on stored data, but also for failing to store data that is relevant to an investigation.[139]

---

[136] Khoury *supra* note 99 at 971-973 (finding instances of overly simplified and unnecessarily combative discovery proceedings present in the case law). Courts encourage the usage of e-experts, and the early discussion of E-discovery in litigation; however, the parties are encouraged towards particular policies, and guided by the rules. *Id.* at 974. There is a serious emphasis on cooperation, and the role of proportionality is evolving as courts look at various factors in deciding how to assign costs of discovery, whether or not to issue protective orders for sensitive information, document formatting for E-discovery, and other considerations. *Id.* at 975-976.

[137] Ezra *supra* note 98 at 1243 (advocating a privacy by design approach in statutory development in order to appropriately assign the costs of the legal burden of privacy. U.S. Federal courts have actively "put up barriers to privacy plaintiffs.") The design, technological, and structural steps necessary for compliance must be implemented before something goes wrong for corporations to mitigate liability under existing privacy and data management laws like the GDPR. *Id*.

A typical approach to privacy law conflicts can be seen in *In re Mercedes-Benz Emissions Litig.*, where the court found the Defendant's GDPR objections did not raise an issue sufficient to stay E-Discovery. *In re Mercedes-Benz Emissions Litig.*, No. 2:16-cv-881 (SDW)(JAD), 2019 U.S. Dist. LEXIS 193948, at *1 (D.N.J. Nov. 4, 2019). Furthermore, the court acknowledged that the GDPR potentially covered information in the litigation, but felt a lack of prior enforcement by EU authorities meant there was no reasonable objection here. *Id.* at 3 (stating defendant has not carried the burden of proving statute blocks production or burden of showing the sovereign nation has enforced the law). That is fundamentally inconsistent with both the GDPR and foreign privacy law in general.

See also Schwarz *supra* note 54 (stating corporate standards for handling data must ensure broad compliance with multiple regulatory schemes, including the GDPR). Here, we see a corporation attempting to comply with a U.S. E-Discovery request while still respecting GDPR guidelines, and the court has overruled their concerns, categorically determining there was no legitimate concern despite textual evidence to the contrary present in the GDPR. *Id*; *see also GDPR Article 47*. Corporations must disclose data responsibly or risk sanctions under international law, and that includes data disclosed pursuant to a U.S. court order; therefore, courts should respect these competing concerns, and adopt compliance protocols that ensure international interests in protecting citizens' data are adequately satisfied.

[138] The Sedona Conference, *supra* note 16, at 557 (2018). Firms are also obligated to not misuse resources while ensuring broad compliance and good public opinion. *Id*.

[139] However, internally implemented privacy protection programs can mitigate fines assessed for noncompliance in both regards. *Id.* (Corporations must develop policies for handling data generally within their IT departments, conducting internal investigations to ensure timely compliance with governmental requests for data including means for identifying data sources and satisfying production requests, initiating third-party data transfers, demonstrating

International comity requires regard for overlapping jurisdiction, yet U.S. courts have historically favored "U.S. Discovery by at least a four-to-one ratio, with two of those factors favoring U.S. Discovery by a ten-to-one ratio" – despite more stringent foreign data restrictions.[140] This propensity for overriding foreign privacy and data handling statutes continues despite the G.D.P.R. For example, in *Finjan v Zscaler,* the court applied existing proportionality standards under *Aerospatiale,* and found a protective order over the relevant data sufficient to address G.D.P.R. concerns that were raised.[141] The defendant sought to block an email Discovery request covered by the G.D.P.R., yet, despite granting the protective order, the *Finjan* court notably found all five *Aerospatiale* factors to weigh in favor of disclosure.[142]

In a similar case, *Corel Software v Microsoft,*[143] the court denied usage of a protective order facing similar G.D.P.R. concerns.[144] Microsoft resisted Discovery of telemetry data, the

---

good faith and reasonableness of withholding and disclosing data, handling data from and for differing jurisdictions, identifying relevant privacy and jurisdictional laws, and ensuring compliance to relevant protocols).

[140] *Cannon et al., supra* note 46 at 3.

[141] *Finjan, Inc. v. Zscaler, Inc.*, No. 17-cv-06946-JST (KAW), 2019 U.S. Dist. LEXIS 24570, at *2-4 (N.D.Cal. Feb. 14, 2019) (allowing E-Discovery of EU data despite GDPR constraints, but requiring a protective order over relevant data). Defendant argued the data would need to be anonymized and redacted. *See id*.

[142] *Id*. (finding anonymization unnecessary where protection order was in place).

[143] *Corel Software, LLC v. Microsoft Corp.*, No. 2:15-cv-00528-JNP-PMW, 2018 U.S Dist. LEXIS 172875 (D. Utah Oct. 5, 2018) (holding usage of data was both proportionate and relevant to the case, and that the cost of producing it under the GDPR was not over burdensome to Microsoft; subsequently, denying protective order request despite GDPR implications); *see also Uniloc 2017 LLC v. Microsoft Corp.*, C.D.Cal. No. 8:18-CV-02053-AG (JDEx), 2019 U.S. Dist. LEXIS 20933 (Feb. 5, 2019) (holding protective order over discovery materials was necessary under GDPR guidelines); *see also Strauch v. Comput. Sci. Corp.*, No. 3:14-cv-956 (JBA), 2019 U.S. Dist. LEXIS 133885 (D. Conn. May 31, 2019) (allowing Special Master to provide de-identified data in compliance with GDPR). Courts have refused protective orders for GDPR covered materials, granted them, and everything in between. Courts' analysis centers around the data's perceived relevance to the case, but generally glosses over the data rights' implications.

[144] Contrast the *Finjan* result with *Corel*; ultimately, the same concerns were raised, but the court in *Corel* declined to provide the same data protection put forth by the *Finjan* court. *Corel*, 2018 U.S Dist. LEXIS 172875.

In *Finjan* a careful analysis of each *Aerospatiale* factor was made. *Finjan*, 2019 U.S. Dist. LEXIS 24570. The *Corel* court made no reference to the *Aerospatiale* factors, ruled the information was proportional, and ruled further Microsoft had to disclose it. *Corel*, 2018 U.S Dist. LEXIS 172875, at *1-2. The court only applied the standards set forth in the Federal Rules. *Id*. These incongruous approaches to data blocking statutes are not anomalous.

retention of which placed them under tension with the G.D.P.R.[145] The court here also did not apply the *Aerospatiale* factors in dismissing the blocking statute concerns.[146] In yet another recent case, *In Re Hansainvest*, the court released G.D.P.R. governed data, but allowed the producing party to shift costs while disclaiming subsequent liability related to the production.[147] The issue arose when Hansainvest sought data from a foreign data processor, covered by E.U. law.[148] Again, the court here did not apply the *Aerospatiale* factors, even though they found the costs to be significant, the foreign law to be applicable, and the requested information to be fairly broad.[149]

Perhaps, not surprisingly, the courts did not apply the same standards in their analysis. In fact, two of the three courts ignored the Aerospatiale standards altogether .[150] The G.D.P.R. has also brought these issues to the Supreme Court.[151] Unfortunately, the Court was preempted by Congress in *United States v. Microsoft Corp.*, and there is continuing uncertainty in how courts should modify E-Discovery proceedings to give proper deference to the G.D.P.R.[152] Ultimately,

---

[145] *Id*. at 2-5 (stating obligations of G.D.P.R. were raised as an objection to Corel's data request).

[146] *Id*.

[147] *In re* Application of Hansainvest Hanseatische Investment-GmbH, 364 F. Supp. 3d 243, 252 (S.D.N.Y. 2018) (stating applicants must "assume costs of the document production," and "indemnify respondents against any potential breaches" of EU law).

[148] *Id.* at 247.

[149] *Id.* at 251-253 (finding objections to "end run" around German law, and status of respondent as only a potential litigant in case to be non-determinative). Furthermore, the court was not persuaded that the requests were made to circumvent German law, despite the locus of the information being Germany. *Id*.

[150] *Cf* Salt River (applying *Aerospatiale* and finding Hague procedures necessary).

[151] Microsoft had stored a U.S. citizen's data, requested by the government in litigation, on a server in Ireland. *Microsoft Corp. v. United States* 829 F.3d 197 (2d Cir.2016). Microsoft argued for not disclosing the data in order to avoid G.D.P.R. implications and possible sanctions. *Id.*

[152] *United States v. Microsoft Corp.*, 138 S. Ct. 1186, 200 L.Ed.2d 610 (2018) (holding relevant statutory changes had rendered issues presented moot; remanded for further proceedings); s*ee also* Cutler, *supra* note 107 at 1537 (stating U.S. courts create a "catch 22" when they do not give adequate regard to foreign privacy interests).

the U.S. Clarifying Lawful Overseas Use of Data Act[153] ("C.L.O.U.D. Act"), preempted the Court's decision, but the overriding nature of the act itself is evidence of a need to address the ongoing conflict between U.S. privacy views and the views held by other nations.

Costs are a concern, as E-Discovery firms have charged upwards of $100,000 for document production even without meeting G.D.P.R. requirements.[154] Consequently, attorneys must have technical knowledge in evaluating data value proportionality, as concerns over data, and data costs, must be addressed in advance for showing the data production is, or is not, unduly burdensome.[155] The current proportionality standards for E-Discovery allows parties to dispute who will pay for compliance with foreign laws, but there is significant variability in how these are handled.[156] Courts apply the Federal standards for cost shifting inconsistently, and the Supreme Court has not definitively weighed in on the matter.[157] Ambiguity clouds the issue, and circuits have not independently reached a consensus on how to apply the current standards in

[153] Department of Justice (CLOUD Act), *supra* note 111. The act aims to clarify existing standards for acquiring data subject to foreign data laws, which the U.S. Congress views as suitably high. *Id*. at 3.

[154] Michael Pasque, *Grasping E-Discovery*, 52 Tenn. B.J. 12 (2016); *see also* Ismer, 18 Fla. Coastal L. Rev. 129, *supra* note 97 (stating even taxes associated with E-discovery costs can balloon to over a million dollars in large litigation). Nearly 80% of litigation costs arise out of the Discovery process; additionally, most discovery is electronic. *Id.* Meta-data processing may also be necessary for proper data analysis, and will incur its own fees.

[155] Pasque, *supra* note 152 (stating data concerns may require employing specialty firms for data processing, and attorneys will have to monitor the exchange of information to ensure adherence to regulations, accuracy of the information, and attorney-client privilege where applicable).

[156] The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control*, 17 Sedona Conf. J. 467 (2016) (stating case-by-case analysis under current guidelines produces highly variable outcomes that fail to adequately address evolving international privacy laws).

[157] Ismer, 18 Fla. Coastal L. Rev. 129, *supra* note 97

light of the existing tensions.[158] Variable judicial standards in this area make the scope of liability imposed on firms unclear.[159]

Courts are aware that cost shifting is an issue, and proposed solutions vary from partially splitting costs to capping costs overall.[160] Each court applies its own view, though cooperation again figures prominently as a typical solution.[161] Some jurisdictions even take a loser-pays-all approach, and assign costs of Discovery on the losing party.[162] Other courts may split them after weighing several factors, which may include the overall cost itself.[163] Because of the case-by-case evaluation of proportionality, which is highly discretionary, cost-shifting approaches remain inconsistent.[164]

---

[158] *Id*.

[159] Bradley T. Tennis, *Cost-Shifting in Electronic Discovery*, 119 Yale L. J. 1113,1116 (2010) (stating a seven factor test is used to determine whether costs should be shifted in E-discovery: "(1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information.").

[160] Genevieve H. Harte, *Electronic Discovery in Civil Litigation: Avoiding Surprises in Cost Shifting Decisions*, 12 Seton Hall Cir. Rev. 267 (2016) (stating cooperation between the parties reduces and caps costs without imposing a regulatory scheme).

[161] *Id*. Proposals like phased discovery can provide a workable solution to the E-discovery dilemma, and may function better than the all-or-nothing approach. *Id*. Phasing allows specific costs to be shared or apportioned, and further limits access to data until it is determined the data is necessary. *Id*.

[162] Remy & Shepherd, *supra* note 112. Alternatively, producer-pays and requester-pays schemes have been applied, but both create negative incentives within the Discovery process. *Id.* (stating each Discovery pay-scheme can allow one party to unduly burden the other in a deliberate and systematic fashion.) Shifting costs where retrieved data has proven unhelpful to litigation, or a shared-cost approach, can potentially eliminate abuses within the current system. *Id*.

[163] Khoury, *supra* note 99, at 976-977.

[164] Remy & Shepherd, *supra* note 112. *See also* Tennis, 119 Yale L. J. 1113, *supra* note 159, at 1114 (stating existing doctrines have done little to standardize the approach).

III. STANDARDIZED DATA POLICIES PROMOTE PRIVACY RIGHTS AND REDUCE LIABILITY

Differing judicial emphasis on privacy as a proportionality factor in E-Discovery creates an uncertain legal environment, and does not accord privacy consistent consideration in litigation. Courts need clearer federal guidance on the current standards in order to produce more even results, and to ensure litigants' privacy rights are respected. Imposing financial burdens on parties that do not adequately protect data, or consider privacy in their data requests, can curtail the weaponization of Discovery and help reduce costs for all parties.

A. Judicial Emphasis on Privacy in Proportionality Can Curtail Discovery Costs

An absence of meaningful judicial guidance on data security and privacy creates a dangerous data environment in litigation that does not accord proper respect to protecting private data. However, open Discovery is essential to U.S. jurisprudence, and allowing regulations to unduly block data transfers undermines Discovery's role in deciding whether to proceed further with litigation or settle.[165] Therefore, updating underlying privacy views held by many U.S. courts can help limit overbroad Discovery, further respect for foreign interests in data, and ensure litigants are not using privacy to block reasonable U.S. E-Discovery requests.

The clear bias of U.S. courts favoring disclosure of private information over protection make even the requirements of the G.D.P.R. unlikely to curtail the lack of significance given to privacy by U.S. courts.[166] Even if they fail to completely prevent data loss, proactive data

[165] Kurtz *supra* note 92 (stating parties will evaluate relative strengths of case in order to ascertain "desirability of settling").

[166] Samantha Cutler, *The Face-off between Data Privacy and Discovery: Why U. S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information*, 59 B.C. L. REV. 1513, 1537 (2018) (stating foreign litigants are frequently caught in a "catch 22" when faced with US discovery requests regarding EU regulated data).

management policies can help to mitigate breaches and post-breach damage.[167] Therefore, U.S. courts should encourage them. Courts need to consider the value of privacy as a right, and place meaningful limits on E-Discovery to protect data from the outset.[168] While unguided disclosure between litigating parties is important, overreliance on it creates inconsistencies, and litigants can find themselves trapped by the competing needs of disclosing information and respecting personal privacy and data rights.[169] Proper application of privacy proportionality standards, with emphasis on data privacy rights, will curtail expansive Discovery, and reduce situations where the process is weaponized.[170] Overbroad governmental access to private information harms privacy rights,[171] and sends data handlers the wrong message. Reforming how courts handle privacy in Discovery will improve data management practices.

---

[167] Nando Delgado, *Using Cyber Security to Maximize Your Company Profits*, (May 10, 2019), https://dev.to/nandod1707/using-cyber-security-to-maximize-your-company-profits-280n

[168] Robert D. Keeling, *The Burden of Privacy in Discovery*, 20 SEDONA CONF. J. 415, 418 (2019) (stating discovery has always been a "cabined" procedure governed by various proportionality concerns balancing needs and burdens; additionally, giving proportionality equal standing with relevance in determining the extent of discovery is a trend in modern privacy law). Relative access to information is also considered. *Id*.

[169] The Sedona Conference, *Commentary on Defensible Disposition*, 20 SEDONA CONF. J. 179, 190-195 (2019) (Courts also distinguish between a party's legal obligation to maintain records and its obligation to the court for the pending litigation; consequently, failure to meet a statutory requirement in data management is not always dispositive of a corporation failing to reasonably comply with discovery requests). *Id*.

[170] Debbie Reynolds, *The Increasingly Complex Issues Involved in Data Breach Fallout*, 2 INT'L J. DATA PROTECTION OFFICER, PRIVACY OFFICER & PRIVACY COUNS. 13 (2018) (stating data breaches "can be one of the most devastating and disorienting types of business loss events . . . massive expenses, legal pressures to respond quickly, and vigilant efforts required to halt or prevent future breach events"). Furthermore, litigants should consider as threshold discovery issues the following when determining whether privacy should preclude a discovery request for social media accounts: likely relevancy of information from the source, possession/custody/control of source, "date range" of the information, what information is relevant to the case, the privacy value of the data compared to its legal value, the "dynamic nature of the social media and user-generated content;", data formatting, and the "confidentiality and privacy concerns related to parties and non-parties." *Id.*; *see also* The Sedona Conference, *Primer on Social Media supra* note 135.

[171] *See* Johnathan Greig, *How More Countries Plan to Pass Stringent Privacy Laws in 2019*, TECH REPUBLIC, (Jun. 25, 2019), https://www.techrepublic.com/article/how-more-countries-plan-to-pass-stringent-privacy-laws-in-2019/

Courts have an opportunity to improve data privacy practices by emphasizing important privacy principles, encouraging litigants to engage in proper data handling techniques, and promoting the implementation of better privacy safeguards.[172] Promoting better data practices does not necessarily mean less Discovery, but it does mean safer data in Discovery. U.S. courts have generally declined to expand consumer privacy rights through the common law – so U.S. citizens lack privacy rights already enjoyed in other parts of the world.[173] However, the E.U. is not the only country with stringent data privacy laws, and the continued legal interaction between the U.S. and other nations will require updated legal views of data privacy more in line with what may ultimately become a default global standard based on the most stringent data protection.[174] Consequently, improved data practices in Discovery will also ease conflicts over foreign data in E-Discovery.[175] In this way, better privacy practices ensure conflicting privacy laws do not hinder open Discovery in litigation. Furthermore, as States are moving to adopt updated privacy regulations, similar to California's C.C.P.A. and the G.D.P.R., the time is rapidly approaching when these conflicts will regularly occur at the state level as well.[176]

---

[172] Ari Ezra Waldman, *Privacy's Law of Design*, 9 UC IRVINE L. REV. 1239, 1258 (2019) (stating courts and U.S. law focus solely on consent and control). *Cf. Id.* Privacy has been consistently emphasized in European case law, and all data transfers subject to GDPR guidelines require specific privacy "safeguards" to ensure adequate consideration of citizens' privacy rights.

[173] Sihvola, *supra* note 110 at 160; *see also* Voss & Houser, *supra* note 13 (stating corporate shift towards general universal compliance standards can help to mitigate compliance costs while providing greater legal protections to non-EU citizens).

[174] TECH REPUBLIC, *supra* note 159 (finding many countries are passing new data management and privacy regulations since GDPR); *see also* COMFORTE, *supra* note 130 (finding broad passage and consideration of privacy laws around world including Brazil, China, and New Zealand).

[175] The Sedona Conference, *supra* note 34.

[176] Jeewon Kim Serrato, *US States Pass Data Protection Laws on the Heels of the GDPR*, DATA PROTECTION REPORT, (Jul. 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/ Alabama, Arizona, California, Colorado, Iowa, Louisiana, Nebraska, Oregon, South Carolina, South Dakota, Vermont, Virginia have updated breach notification and data security laws in the past two years, and others will follow.

Courts play a unique role in the E-Discovery data management chain. Their emphasis on proper data management and privacy practices encourages firms and litigants to engage in appropriate data practices. Giving data management more attention, and data privacy its proper weight in proportionality, will help streamline conflicts of law in Discovery and reduce data risks for all parties.[177]

B. Clearer Federal Proportionality Standards Are Needed

U.S. data management and privacy policies fail to meet existing international standards. For example, Congress's response to *Microsoft*, the C.L.O.U.D. Act, underscores fundamental flaws[178] in the U.S. approach to privacy and data. Clearer Federal guidance for proportionality, including emphasis on modern data management and the impact of foreign privacy legislation, will decrease tension with foreign laws in E-Discovery.[179] Courts require clarification in assessing and quantifying data burdens and needs as the current standards are not producing even results.[180] Limits for data ranges or procurement time,[181] and minimum standards for protection and deletion,[182] will provide more consistency in cases where cooperation fails. Lastly,

---

[177] The legal profession lags in protecting data and privacy. Daniel Goldberger; Nick Akerman; Joanna Levin; David Ray, *Fall 2016 Cross-Border Data Privacy Issues*, 25 CARDOZO J. INT'L & COMP. L. 379, 384 (2017) (discussing how data management is a problem in firms because "People walk out with thumb drives all the time.")

[178] Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L. J. 1, 9 (2018) (Finding U.S. legal privacy standards to be "deeply flawed" and "unlikely to change [soon]"). U.S. legal framework is outdated and outmoded; consequently, advancements in technology have led to continued privacy failures, and legal standards that do not allow consumers adequate control over their data. *Id.* U.S. regulators rely on our underlying apathy to updating privacy law, and privacy law in the U.S. has stagnated and worsened over time. *Id*. at 31-33.

[179] *See* The Sedona Conference *supra* note 34.

[180] McGinn & Sakiyama & Bartholomay, 64 PRAC. LAW. 15-17, *supra* note 123.

[181] *Id*. (stating court found no burden where 100 hours of data procurement was acceptable for restoring data).

[182] *Id*. (finding increased costs caused by excessive deletion was greater than value of litigation and still acceptable).

clarifying privacy's role in Federal proportionality standards will promote better data policies for domestic data handlers, just as the G.D.P.R. has for global data handlers.[183] Litigants will also profit from a more standardized approach to weighing data procurement burdens and privacy in proportionality, as the existing case by case analysis is overly discretionary, and does not address modern technological advances in data handling and use.[184]

Federal standards need to provide clarity on protecting foreign data interests, weighing data costs, and determining when and how to limit data access to produce more consistent results. Currently, court Circuits have handled privacy issues arising under current Federal regulations differently, and inconsistencies abound.[185] Analysis under the current guidelines produces highly variable outcomes. It also fails to adequately consider cross-border privacy laws, and produces an uneven application of E-document procurement and privacy laws alike.[186] Inconsistencies in applying the various balancing factors for deciding whether or not electronic data should be subject to E-Discovery, with or without a protective order, highlight the need for greater clarity in data management and foreign privacy compliance.[187]

---

[183] Rustad & Koenig, 71 FLA. L. REV. 365, *supra* note 76 (stating Microsoft has touted universal compliance to the G.D.P.R. for all its data clients as a competitive advantage it has over other data handlers).

[184] McGinn & Sakiyama & Bartholomay, 64 PRAC. LAW. 15-17, *supra* note 123 (stating court has found data recreation not overly burdensome despite significant expense). The need for this recreation was an email system that did not store emails beyond several days. *Cf Id.* However, deletion is an important part of data protection.

[185] Voss & Houser, *supra* note 13 at 385. Notably, personal data definitions vary, and courts do not agree on what privacy issues give rise to cognizable harms. *Id.* at 414.

[186] The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control*, 17 SEDONA CONF. J. 467 (2016) (finding modified E-Discovery and data management procedures can reduce costs of litigation and promote greater consistency across legal forums).

[187] The Sedona Conference, *supra* note 118; *see also* Finjan *supra* note 141 and Corel, *supra* note 143.

In *Finjan*, the Northern District Court of California found anonymization unnecessary despite G.D.P.R. restrictions,[188] while other districts have required it or more.[189] Importantly, an Arizona district court found the potential burden imposed by the foreign blocking statute, and France's interest in protecting data to weigh in favor using Hague proceedings.[190] Differences in the standards courts use in analyzing blocking statutes, and differences in how they apply those standards, do not produce consistent results for G.D.P.R. governed data.[191] Furthermore, the Supreme Court has not addressed these issues or inconsistencies.[192] Presented with similar G.D.P.R. conflicts, courts continue to arrive at competing conclusions, and as more privacy laws enter the legal arena, parties' liabilities under them will become more confusing.

The structure of the G.D.P.R. is such that compliance typically obviates the need for additional privacy policies, but courts do not take the blanket adherence approach that corporations have found to be cost saving.[193] Instead, courts have relied on litigative negotiations

---

[188] Finjan, Inc. v. Zscaler, Inc., LEXIS 24570, 9 (N.D.Cal. 2019) (finding protective order in standard discovery adequate, and anonymization unnecessary). The court did not accept that the data was possibly redundant, and found the defendant's U.S. based location to also weigh in favor of discovery. *Id* at 2-3. Notably, the court also found redacted data would not be equivalent. *Id*. They also noted the unlikelihood of enforcement under the G.D.P.R. *Id*. at 3-4 (stating value to U.K. was low, and that it was unclear production was even barred). *Cf* Salt River, *supra* note 18 (finding Hague convention guidelines necessary for G.D.P.R. protected data).

Salt River, *supra* note 18 at 5-8 (emphasizing the optional nature of applying The Hague convention guidelines in-lieu of standard discovery procedures). The court gave additional weight to Trench-France's assertion that the data was likely to be redundant, and not crucial to the outcome of the case at this time. *Id*. Additionally, the court considered the fact that Trench-France was seeking to block standard discovery while Trench-Canada was complying with discovery. *Id*. at 11-12. They also found the request overbroad, the company's foreign location, and the likelihood of compliance with Hague procedures to weigh in favor of using Hague procedures. *Id* at 13-14.

[190] *Id*. at 3-4 (finding minimum of 60 added days, and likelihood of rapid compliance after, to also weigh in favor of Hague procedures).

[191] Two of four courts applied *Aerospatiale*, one of four courts found Hague proceedings necessary, one of four found a protective order necessary, one of four shifted costs onto the requesting party, and one of four indemnified the producing party. *See generally* Finjan, Inc. v. Zscaler, Salt River, IN RE HANSAINVEST, and Corel v. Microsoft, *supra*.

[192] *See United States v. Microsoft Corp.*, 138 S.Ct. 1186 *supra* note 152.

[193] Reynolds, *supra* note 170.

between parties and protective orders to meet G.D.P.R. data management requirements.[194] Consequently, the Discovery process still relies more on litigants' cooperation than it does on oversight by the court,[195] which means data management and privacy compliance in E-Discovery are met through each jurisdictions regionalized interpretations..[196]

Vague regulatory standards increase costs of litigation, discourage appropriate suits, and "undermine the rule of law."[197] U.S. courts need clearer guidance on creating judicial privacy standards that are responsive to modern technological advances and updated laws.[198] In *Corel*, Microsoft argued the production of telemetry data would be unduly burdensome because of the anonymization of the data required by the G.D.P.R.[199] Glossing over the technical tension and G.D.P.R. requirements, the court found the data value outweighed the data costs,[200] but the

---

[194] *Id*. The issue becomes how seriously, or not seriously, the court may perceive relevant privacy concerns to be. *Id*; *see also In re* Facebook, Inc. Secs. Litigation, LEXIS 166027 (U.S. Dist.2019) (Sep. 25, 2019) (finding absence of scienter despite a "business model [that] depends on users freely sharing their information and thus incentivizes misuse of data").

[195] Keeling, *supra* note 168.

[196] Houser *supra* note 13. Data privacy violations by various US corporations have resulted in multimillion dollar fines, and the implementation of various compliance programs; however, the regionalized nature of enforcement prevents a comprehensive compliance standard. *Id*. EU regulators believe the extraterritorial application of the GDPR will eliminate the unfair advantage deregulated US corporations have in the tech market. *Id*.

[197] Ezra, *supra* note 98 at 1257-1259; *see also* Corel Software, LLC v. Microsoft Corp., LEXIS 172875 (D.Utah 2018) (denying protective order despite GDPR restrictions on requested telemetry data). Furthermore, the court ordered Microsoft to produce the telemetry data despite Microsoft's objections that production violated GDPR provisions governing telemetry data of EU citizens. *Id*. International comity requires a balancing of competing legal concerns; here, the court's minimalist approach to analyzing the GDPR related concerns is typical of the disregard U.S. courts have traditionally given international data and privacy laws. *Id*.

[198] Marija Boban, *Digital Single Market and EU Data Protection Reform with Regard to the Processing of Personal Data as the Challenge of the Modern World*, 16 ECONOMIC AND SOCIAL DEVELOPMENT, 16TH INTERNATIONAL SCIENTIFIC CONFERENCE ON ECONOMIC AND SOCIAL DEVELOPMENT: THE LEGAL CHALLENGES OF MODERN WORLD 191 (2016) (stating rapid technological changes have resulted in private and public deficiencies in data handling.) The growth in the "knowledge-based economy" in the past decade has led to revisions in economic and social theory; legal revisions have lagged. *Id*.

[199] Corel Software, LLC v. Microsoft Corp., LEXIS 172875 (D.Utah 2018) (stating tension with G.D.P.R. makes production of effected data by Microsoft unduly burdensome).

[200] *Id*. at 2 (stating also Microsoft has sufficient resources to carry financial burden).

standard on when costs are overly burdensome is not clear.[201] Microsoft also sought to block further retention of the data for trial, as it potentially violated G.D.P.R. deletion standards, and was denied.[202] The court did so without examining Microsoft's obligations under the G.D.P.R. for data storage.[203]

Where costs are not an issue, data liability may be. As in the *Hansainvest* case, fines under the G.D.P.R. lead some firms to require indemnity from the data they produce,[204] and that courts allow this shows they do not understand the potential liability litigants face from data production and retention. Clarifying how to handle the G.D.P.R.'s new legal burdens, and promoting better data management in E-Discovery, ensures broader compliance to privacy laws, and streamlines issues already arising between disclosure and the protection of private information.[205] Furthermore, requiring greater data protection can eliminate potential liability without reducing the availability of data in Discovery.

Just as the G.D.P.R. has forced global corporations to adopt compliance programs for meeting evolving privacy standards, emphasis on privacy's role in proportionality also encourages broader respect for privacy.[206] The increased scope of modern privacy laws is

---

[201] McGinn & Sakiyama & Bartholomay *supra*, note 123 at 16-17 (finding even financially unbalanced parties may still be compelled to produce data despite higher burdens landing on one party).

[202] *Corel Software, LLC*, LEXIS 172875 (D.Utah 2018) (stating further retention of the data raised significant G.D.P.R. concerns and costs). The court ordered Microsoft to produce the data, and to continue to retain the data, finding their concerns unsupported. *Id* at 1-2.

[203] ICO, *supra* note 50 (stating data storage should be minimized, and subject to a standard retention/deletion period). The data must also be properly protected, limited in use by consent, and necessary for a specific purpose. *Id*.

[204] *In re* Application of Hansainvest Hanseatische Investment-GMBH, 364 F. Supp.3d 243, 252 (S.D.N.Y. 2018).

[205]The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557 (2018). Corporate privacy protection requires an interactive approach, as concerns are ongoing and evolving constantly; regulations impose a structure for compliance that allows corporations to meet a minimum standard without properly considering their underlying policies on privacy and data generally. *Id*.

[206] Voss & Houser *supra* note 13; *see also* W. Gregory Voss, *GDPR: The End of Google and Facebook Or a New Paradigm in Data Privacy*, 25 RICH. J.L. & TECH. 1 (2018) (stating the US lacks an "overarching federal privacy

relevant in E-Discovery proceedings, and a better framework for handling privacy law conflicts and costs is needed.[207] Standards for weighing data production costs that consider modern privacy retention, deletion, and data management safeguards, help to mitigate unforeseen data liabilities.[208] Additionally, clarifying privacy's role in E-Discovery will help curtail overbroad Discovery, and eliminate data management conflicts with the G.D.P.R. that many critics believe are still present in the new Data Privacy Shield Agreement as well.[209] Disregarding privacy in E-Discovery is out-of-step with Global privacy standards, and encourages overbroad Discovery. Clarifying how to handle privacy burdens and restrictions in Federal proportionality standards

---

statute," relying instead on a regional approach.) Significant differences in their approaches to privacy have resulted in strikingly different legal responses to privacy violations. *Id*. The FTC has brought only a handful of actions against corporations for violating data privacy rights, the proceedings are largely confidential, and fines tend to be nominal in nature. *Id.* EU Data Privacy Authorities, DPAs, have brought hundreds of actions against various U.S. Corporations for privacy statute violations. *Id*. The extraterritoriality of the GDPR is considered an important aspect of its legal force; ultimately, data privacy rights are a "global social and economic issue." *Id*. The U.S. Congress's hearings with Facebook CEO Mark Zuckerberg showed a fundamental lack of understanding regarding modern technological advances in metadata processing, and underscored a need for understanding underlying security and technology necessary for proper data management. *Id*.

[207] *Id*.

[208] *See* The Sedona Conference *supra* note 34.

[209] *Annexes E.U. U.S. Privacy Shield*, FTC, (Dec 7, 2016), https://www.ftc.gov/system/files/documents/plain-language/annexes_eu-us_privacy_shield_en1.pdf (stating new compliance department will keep E.U. apprised of new data rights laws in U.S.) The new framework was proposed by the U.S. to meet GDPR data requirements, and ensure continued transfer of data between the two countries. *Id*. at 11.

promotes foreign data interests,[210] encourages proactive data management policies, provides consistency to litigants,[211] and can decrease litigation costs.[212]

C. Cost Shifting as a Tool to Promote Privacy in E-Discovery

Because E-Discovery costs and penalties for violating data handling laws are growing, courts should consider litigants' data management and privacy policies when assigning data compliance costs. Firms with better data policies should be rewarded, as their practices will reduce costs overall by meeting compliance minimums without additional action from the court.

The current variable standards of cost shifting for E-Discovery neither encourage better Discovery practices nor produce consistent results for litigants.[213] Because new data regulations stand to substantially increase compliance costs, a means of allocating those costs definitively gives litigants better directions on how to approach G.D.P.R. costs.[214] Irregular or arbitrary

---

[210] Cannon *et al*, 27 ABA 2019 *supra* note 41 at 2. "Violations of blocking statutes can lead to the imposition of civil and criminal penalties, including fines and imprisonment. The fears motivating the enactment of blocking statutes appear to be well founded as . . . U.S. courts have routinely asserted the power to demand evidence held by foreign entities through" Federal procedure, including E-Discovery. *Id*.

But see Salt River Project Agricultural Improvement & Power Dist. v. Trench Fr. SAS, 303 F. SUPP. 3D 1004 (D.Ariz.2018) (holding French corporation's statement that Hague convention standards would result in the document production without protestation weighed in favor of a Hague standard approach instead of standard E-Discovery). The court also found the France had "an emphatic sovereign interest in controlling foreign access to information within its borders, and in protecting its citizens from foreign discovery practices" contrary to their privacy views. *Id*. In this particularly anomalous case, the court weighed the factors heavily in favor of The Hague standard over typical E-Discovery. *Id*.

[211] The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control, supra* note 182 (stating Current e-document procurement guidance is inadequate for courts and litigants alike).

[212] Ezra, *supra* note 98.

[213] *Ismer*, 18 FLA. COASTAL L. REV. 129, *supra* note 97 (stating cost of Discovery is becoming a bigger issue as Discovery costs grow. *See also* Henry *supra* note 153 (stating GDPR requirements will increase E-Discovery costs to higher levels for compliance with mixed standards).

[214] *In re* Hansainvest Hanseatische Invest. -GMBH, 364 F. SUPP. 3D 243 (S.D.N.Y.2018) (holding costs related to GDPR will be borne by party requesting documents) Here, the court allowed E-Discovery to continue, but required that the Applicant pay for the document production, and indemnify the Respondent against any liability arising from the data transfer. *Id*. Assigning the greater costs to one party because the data underlying those costs pertains to EU citizens seems arbitrary at best; however, the court did also acknowledge that selective E-Discovery requests, limited in scope, could reduce the overall costs, and stated the parties should proceed accordingly. *Id*. U.S. Soccer Fed Inc. v. Silvia Int'l Invs., LEXIS 75350 (S.D. Fla. 2019) (requesting GDPR costs be shifted to plaintiff where

shifting of G.D.P.R. costs onto one party can discourage litigants. Application of a phased approach has merits, as does requiring each side to share the burdens of the costs, but there is also something to be said for rewards-based systems that encourage good litigative practices, including privacy right protection.[215]

Cost assignation based on each parties' privacy and data practices in E-Discovery could serve as a benchmark standard for assigning compliance costs. E-Discovery already requires a good cause showing for document production,[216] inclusion of privacy standards as a metric for cost assignation would ensure each side has considered the privacy implications of the information they are requesting.[217] Both sides already know extensive E-Discovery will be expensive, and knowing privacy failures will assign those costs to [your] side will encourage litigants to implement better data and privacy policies, potentially reducing conflicts with international privacy and data management laws as well.[218]

Additionally, the added emphasis on privacy as a factor for cost shifting can encourage firms to adopt heightened data standards overall. Broader data compliance will allow law firms to catch up to other industries, as they are generally considered deficient in data security.[219] Protecting sensitive information, including incidental private information obtained during E-

---

discovery touched on data belonging to EU citizens because of extra "costs and fees" related to GDPR data handling compliance). The court ultimately transferred the case to another court more familiar with the matter, but GDPR-costs are rapidly becoming an issue in Federal litigation. *Id*.

[215] Murphy *supra* note 103; *see also* Ismer, 18 FLA. COASTAL L. REV. 129, *supra* note 97.

[216] Tennis, *supra* note 159.

[217] Nash *supra* note 112.

[218] *See generally* Goldberger *supra* note 64 (stating litigation can result in confiscation of personal devices only linked to work email). The scattered U.S. approach, from a lack of Congressional regulation on protecting personal data, is not helpful. *Id*. Security is a "moving target," requiring constant updates as do laws on data security; consequently, any laws implemented need room to be updated in interpretation. *Id*. One way courts can revise their enforcement of privacy rights, is through cost assignation, because it is currently a discretionary matter.

[219] *Id*.

Discovery, is important, and most firms do not have adequate policies in place.[220] A financial incentive to become more privacy conscious will spur essential changes in data management policies,[221] and encourage broader compliance with data handling laws. Ultimately, the most essential change that needs to occur is the way we all view personal privacy, and the laws already in place are telling us we should. Consequently, deciding not to consider data management and privacy in litigation could result in financial consequences even without a cost shifting scheme that considers them.

IV. CONCLUSION

The importance of privacy in E-Discovery increases as rapid advancements in technological methods for obtaining, processing, and using electronic data increase. As global privacy standards unify, U.S. courts will need to re-evaluate their data privacy policies and procedures – that includes weighing privacy more in granting certain Discovery requests. This problem will only increase as data storage grows,[222] and the law must adapt. Data is the lifeblood of our digital society – there are no corrective responses to data loss events. An absence of data security creates many of the problems we see in unvaccinated populations. Proactivity is the only solution as exploits that are not caught quickly can be used to target connected data servers or

[220] *See* Goldberg *supra* note 64.

[221] Bottum *supra* note 88.

Document retention and deletion are pivotal to data privacy because attention to what is being stored, how long it is stored, and whether or not it needs to be stored are the first line of defense in stopping data loss. Deleting old – or unneeded – data, minimizes data exposure. Therefore, it also minimizes data risk, while furthering privacy interests. Ignorance is also an issue here – implementing a compliance department for ESI, electronic data, automatically improves outcomes. Even in the event of a breach, having an action plan, and staff committed to monitoring server storage, updates/downloads, and ensuring unnecessary data is deleted on a regular cycle, will limit material damages arising from a breach.

[222] *Id*. 2020 data production is predicted to be 44x higher than data production was only a decade ago. *Id*.

higher value targets.[223] Data security is about universal preparedness. Protecting a nation's data requires partner nations to cooperate with data standards by enacting policies that ensure data transferred out of the country is still protected. Sensitive data requires policies that will ensure one weak link does not allow a breakdown in the data chain, and that includes data gathered for litigation through Discovery.[224]

Varying regional standards do not give consistent regard to data management and privacy, and discretion and cooperation can only go so far. Clearer Federal standards for weighing privacy in proportionality for E-Discovery disputes – updated for the modern realities of data handling and privacy rights – will provide litigating parties with clarity and can reduce compliance costs overall. Furthermore, courts can reward parties by shifting compliance costs to parties that do not adequately address these concerns in Discovery. Respecting data rights during E-Discovery, by tailoring data requests to minimize sensitive data exposure, minimizes data handling risks. Therefore, respect for privacy can reduce liability, and is also a practice that pays for itself.

[223] *Id.* One 2009 breach targeting credit card payment processors is considered the largest theft of credit card information in finance history. *Id*. *See also* Barrett *supra* note 84.

[224] *Id*. The vast majority of data breaches are from a lack of appropriate data security. *Id*. Still, some data loss is the result of insiders, random accidents, and theft. *Id*. One data loss incident was the result of a USPS truck delivering sensitive files to the wrong business. *Id*.

Incidents like this underscore the need for more standardized policies that put an impetus on all data handlers to take the current data situation seriously, and respond accordingly with procedures that help prevent data loss events.