CO-OPTING PRIVACY

Neil Richards[*]

Washington University School of Law

Preliminary Conference Draft – Not to be cited or quoted without permission

November 1, 2021

As privacy and data protection law have expanded across the world over the past few decades, companies have found ways to turn the rules to their own advantage.[1] At a macro level, Julie Cohen demonstrates how companies shape the structures of information law to serve their own purposes.[2] At a more granular level, Ari Waldman's careful ethnographic work illustrates the way companies use privacy compliance structures to further their own ends and frustrate the goals behind privacy rules.[3] Other scholars have started to consider the pretextual use of privacy rules and justifications. Thus, Rory van Loo has shown how companies have been using privacy rules to their own advantage to avoid competition and accountability.[4] In a slightly different context, Susan Hazeldean has argued that opponents of LGBT rights have offered pretextual privacy arguments in disputes over access to gendered toilets in accord with a person's gender identity.[5] The story of how powerful entities co-opt privacy is thus growing, but the picture remains incomplete. This paper offers an additional example of corporate shaping of privacy

[*] Koch Distinguished Professor in Law and Director, Cordell Institute, Washington University in St. Louis. I am grateful to Ryan Calo, Julie Cohen, Danielle Citron, Rory Van Loo, Ari Waldman, and Woody Hartzog and to the participants at the Pound Civil Justice Institute and U.C. Hastings Center for Litigation and the Courts conference on "The Internet and the Law: Legal Challenges in the New Digital Age" for their helpful suggestions and comments on earlier drafts. I am also grateful to Nathan Hall for his excellent research assistance. Finally, I should disclose that while I developed some of the arguments advanced in this paper while involved as an expert witness in some of the federal district court cases cited in the paper, all of the opinions and arguments I advance here are my own independent conclusions as a scholar as this paper, like the Symposium of which it is a part, is intended in the spirit of combining the insights of scholarship and practice.

[1] For an excellent overview of the development of privacy and data protection policy since the 1970s, see Priscilla M. Regan, *Fifty-plus years of information privacy policy-making: The more things change, the more they stay the same*, RESEARCH HANDBOOK ON INFORMATION POLICY (Alistair S. Duff ed. 2021).

[2] E.g., JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2020).

[3] E.g., ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (Cambridge 2021).

[4] See, e.g., Rory Van Loo, *Digital Market Perfection*, 117 MICH. L. REV. 815, 836-39 (2019); Van Loo, [not-yet citeable draft on file with author].

[5] Susan Hazeldean, *Privacy as Pretext*, 104 CORNELL L. REV. 1719 (2019).

rules at the level of geopolitics: the use of the General Data Protection Regulation (GDPR) in Europe to frustrate ordinary discovery requests by U.S. plaintiffs in transnational litigation. [6] In so doing, it attempts to further refine our understanding of how privacy rights and privacy rhetoric can be used to co-opt the values they were intended to protect.

In a series of cases, European defendants have argued that the GDPR requires them to redact all names from otherwise valid discovery requests for relevant evidence produced under a protective order, thereby turning the GDPR from a rule designed to protect the fundamental data protection rights of EU citizens into a corporate litigation tool to frustrate and delay the production of evidence of alleged wrongdoing. This example is significant for two reasons. First, it represents what is in effect a complementary opposite to Waldman's examples of strategic privacy dilution through compliance mechanisms – the equally strategic broadening of privacy rules through compliance to serve corporate rather than individual ends. Second, this example points the way toward a broader phenomenon of the sort Cohen and Van Loo articulate – the use of privacy as pretext to serve powerful institutional interests more generally. Privacy pretexts of the sort exemplified by the GDPR case represent a different kind of challenge to privacy law, and they warrant further study by privacy scholars.

This paper thus seeks to make three contributions to the privacy literature. First, at the most basic level, it identifies the practice of defendants attempting strategically to co-opt the GDPR to serve their own purposes. Second, it offers an explanation of precisely why and how this practice represents not merely an incorrect reading of the GDPR, but more broadly a significant departure from its purposes – to safeguard the fundamental right of data protection secured by European constitutional and regulatory law. Third, it places the problem of privacy pretexts and the GDPR in the broader context of the co-option of privacy rules more generally, offers a framework for thinking about such efforts, and argues that this problem is only likely to deepen as privacy and data protection rules thicken through the ongoing processes of reform.

Reflecting these contributions, the paper's argument also proceeds in three parts. To ground the analysis which follows, Part I offers a brief overview of the goals and mechanisms of the GDPR. It explains how the GDPR is in essence an implementation of EU human rights law intended to empower individuals by protecting personal information about them that is held by companies and other institutional entities. Part II describes the ways in which companies have sought to co-opt the GDPR for their own purposes, using it defensively and pretextually in

[6] Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018 [hereinafter *GDPR*].

trans-national lawsuits to pervert the individual human rights goals of the GDPR. Part III suggests that the GDPR example sheds light on privacy pretexts more generally. It offers a definition of privacy pretexts as the co-option of privacy rules to serve institutional rather than individual interests; suggests that the phenomenon of privacy pretexts is more common than the existing privacy literature and discourse has appreciated; and situates the notion of privacy pretexts as a complementary addition alongside the privacy-on-the-ground work of Waldman, the competition scholarship of Van Loo, and the historical and theory work of Cohen. It concludes by arguing that what Hazeldean calls "Privacy Pretexts" might well represent a battle for the soul of privacy law. This means not only that the co-option of privacy rights demands further study at both the theoretical and practical levels, but that regulators creating and courts interpreting new privacy rules must be careful to ensure that those rules are not co-opted pretextually, turning intended protections for individuals into further tools for their exploitation by powerful entities.

I. THE PURPOSE AND CONTEXT OF THE GDPR

The GDPR became the law of the European Union ("EU") in May of 2018.[7] While it is the most recent general European privacy statute, it is certainly not the first. The GDPR is the successor to the EU Data Protection Directive of 1995.[8] While the GDPR has some significant differences from the Data Protection Directive, it follows largely the same conceptual and legal model—one that can be traced back all the way to a 1973 Report of the United States Department of Health, Education and Welfare that established the "Fair Information Practice Principles" or FIPS, which have become the basic building block of data protection laws in the United States and around the world.[9] Thus, while the GDPR is certainly the leading and most influential privacy law in the world at the moment, it continues the traditions of EU data protection law, rather than starting them anew in a radical (and radically more protective) direction.[10] It is thus, as one group of international privacy scholars have concluded, "an evolution, not a revolution."[11]

Many of the GDPR's evolutions, however, were intended to fill perceived gaps in EU data protection law and to update that law for the digital practices of the

---

[7] Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018 [hereinafter *GDPR*].
[8] European Union Data Protection Directive, O.J. L 281 , 23/11/1995 P. 0031 – 0050 [hereinafter *EU Data Protection Directive*].
[9] See Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1699-1705 (2020).
[10] See, e.g., Anupam Chander, Margot Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733 (2021); Paul Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U L. REV. 771, 810 (2019).
[11] *Id.* at 6.

2020s. As such it was opposed at the drafting stage by business interests who preferred the looser data protection requirements of the status quo.[12] It is thus quite an irony (though perhaps an expected one) that now it is in effect businesses have sought to turn it to their own interests, both within internal compliance structures[13] and by taking litigation positions that at least facially use the pretext of privacy protection.[14] My observation here is not intended to discredit the GDPR itself. The GDPR marks a huge step in protecting the privacy interests of people around the world against institutions seeking to use the data in ways that exceed the expectations or that menace basic notions of data protection. It has influenced the development of U.S. law at the state level by inspiring a new generation of state data protection laws[15] and at the federal level by stimulating a renewed debate about federal privacy reform and the prospect of a "U.S. GDPR."[16] However, as I will explain below, those same strong protections have offered an opportunity for them to be cop-opted for other ends. Yet in order to understand how the GDPR's

[12] See, e.g., Regan, supra note x, at 167.
[13] See WALDMAN, supra note x, at y.
[14] *See*, *e.g.*, Corel Software, LLC v. Microsoft Corp., No. 2:15-cv-00528-JNP-PMW, 2018 WL 4855268, (D. Ut. Oct. 5, 2018) (ordering the production of relevant personal data by defendant over a GDPR objection); In re Farm-Raised Salmon & Salmon Prods. Antitrust Litig., No. 19-21551-CIV-ALTONAGA/Louis, (S.D. Fla., June 3, 2020) (holding that the GDPR does not mandate redaction of relevant documents produced subject to a protective order); Uniloc 2017 LLC v. Microsoft Corp., 8:18-CV-02053, 2019 WL 451345, *1 (C.D. Cal. Feb. 5, 2019) (amended stipulated protective order allowing the production of GDPR-covered data); Vancouver Alumni Asset Holdings, Inc. v. Daimler AG et al., No. 2:16-cv-02942-DSF-KS (C.D. Cal. Apr. 16, 2016) (Dkt. No. 237) ("IT IS HEREBY ORDERED that Defendant shall produce unredacted documents in response to Lead Plaintiff's First RFPs, subject to the protection of the Stipulated Protective Order and the parties' Confidentiality Agreement. Nothing in this Order is intended as, nor shall be construed as, a waiver of any objections, other than those based on the GDPR and/or the BDSG, that Defendants may have to the scope of Lead Plaintiff's First RFPs."); Finjan, Inc. v. Zscaler, Inc., No. 17-cv-06946-JST, 2019 WL 618554, at *1 (N.D. Cal. Feb. 14, 2019) (holding that the GDPR does not preclude Defendant from producing relevant e-mails in un-redacted form subject to a protective order after applying international comity balancing test, and noting that production of relevant emails "would appear to not violate the GDPR."); Giorgi Global Holdings, Inc. v. Smulski, No. 17-4416, 2020 WL 2571177, at *1 (E.D. Pa. May 21, 2020) (finding that the GDPR does not bar Defendant's production of relevant documents subject to a protective order after applying international comity balancing test). These rulings are consistent with federal court rulings on pre-GDPR European data protection rules under the Directive and implementing statutes such as the British Data Protection Act and the German Federal Data Protection Act. See, e.g., Laydon v. Mizuho Bank, Ltd., 183 F.Supp.3d 409 (S.D.N.Y. 2016) (allowing production subject to a protective order of unredacted documents in a fraud case against an EU data protection objection under the precursor to the GDPR); Knight Capital Partners Corp. v. Henkel AG & Co., 290 F.Supp.3d 681 (E.D. Mich. 2017) (finding the production of relevant unredacted "ordinary-course-of-business communications" and emails to be "necessary" to the establishment of civil tort claims under a protective order).
[15] Cite CCPA, Colorado, Virginia Laws, NYT Magazine Article on linkage between GDPR and CCPA.
[16] *See* Press Release, Senator Markey Introduces Resolution to Apply European Privacy Protections to Americans, *Ed Markey: News*, (May 24, 2018). https://www.markey.senate.gov/news/press-releases/senator-markey-introduces-resolution-to-apply-european-privacy-protections-to-americans.

purposes might be co-opted, it is first necessary to understand what those intended purposes were intended to be.

This Part offers a brief overview of the goals and context of the GDPR for an American legal audience. This is an important first step because to the uninitiated, the GDPR can be bewildering, a dense thicket of 99 substantive Articles, 170 interpretive Recitals, and a growing mountain of guidance, reports, and judgments from a variety of EU administrative agencies and courts at the member state and transnational levels. It is easy for an American lawyer or judge to get lost in this mass of dense European legal materials, and easy even for an expert to lose a sense of the big picture.

In order to make sense of the GDPR, then, it is useful to highlight three broad interpretive principles: (1) the GDPR is best understood as regulating data flows rather than restricting them; (2) the general approach of European law in this area is characterized by its commitment to balance and rather than absolutism; and (3) the protections of the GDPR are generally committed to reasonableness under the circumstances rather than unyielding strictness.

A. Regulation Rather than Restriction

There is a tension at the very core of the GDPR's stated purposes of data protection. While it intends to protect the data protection rights of EU citizens, the purpose of the GDPR is not to stop data flows within the EU, or even across national borders. Instead, the GDPR recognizes that personal information flow is one of the foundations of both the EU economy and the international economy and ensures that the fundamental right of data protection is respected by regulating the inevitable flow of personal data in reasonable, responsible, and ethical ways.[17] Thus, GDPR fits better under the English-language concept of a *regulation* of flows of personal information, rather than a *restriction*. After all, the GDPR is itself titled as a General Data Protection *Regulation*.

This conclusion is supported by recent scholarship by American and European data protection scholars interpreting the GDPR. These scholars describe the most important implications of the GDPR, the first three of which are particularly relevant here. First, they explain that the "GDPR can be seen as a data governance framework. The GDPR encourages companies to think carefully about data and have a plan for the collection, use, and destruction of the data. The GDPR compliance process may cause some businesses to increase the use of data in their activities, especially if the companies are not data-intensive, but the GDPR causes them to realize the utility of data. Other businesses will use GDPR as an

[17] GDPR Art. 1.

opportunity to view data as a strategic asset, on the same level as companies view their patent portfolio or copyrights."[18]

Second, they explain that "the GDPR attempts to put privacy on par with the laws that companies take seriously—antitrust and foreign corrupt practices law. … Since the adoption of the GDPR, privacy and personal data are being discussed at the highest levels in companies. Many companies have revised their data practices, and take, for the first time, a professional approach to handling personal data."[19]

Third, "the GDPR requires protections to follow data," particularly in the context of commercial transfers to service providers and other vendors with whom the data is shared.[20] Thus, the GDPR is not a blunt or inflexible restriction on the use or transfer of personal data by companies, but rather a requirement that companies take data governance seriously like other regulatory obligations, in a way that facilitates the ethical usage and transfer of personal data.

The GDPR does not talk in terms of *strict* or *absolute minimum* necessity. Instead, it talks about proportionality, reasonableness, and balancing, with the overarching goal of ensuring that data protection rights are protected, but not at the expense of other important interests. Reflecting this basic structure, the GDPR has numerous and broad exceptions and derogations, including, for example, consent, performance of a contract, legitimate interests, journalistic exceptions, and exceptions required by legal obligations, among others.[21]

B. Balance rather than Absolutism

The GDPR, like the Data Protection Directive before it, implements the European rights of privacy and data protection. These rights are enshrined in the EU Charter of Fundamental Rights, which was proclaimed in 2000[22] and took full effect after the Treaty of Lisbon in 2009.[23] In this respect, there is a close analogy between the relationship in EU law between the Charter and the GDPR and the relationship in US law between the Fourth Amendment and the Electronic Communications Act ("ECPA").[24] Both the Charter and the Fourth Amendment establish fundamental rights of privacy that are protected and implemented by the GDPR (applying to data processing in general) and ECPA (applying to wiretapping

---

[18] Chris Jay Hoofnagle et al., The European Union General Data Protection Regulation: What It Is And What It Means (September 24, 2018), at 4. UC Berkeley Public Law Research Paper. Available at SSRN: https://ssrn.com/abstract=3254511.
[19] *Id.*
[20] *Id.*
[21] *See GDPR*, art. 6.
[22] Charter of Fundamental Rights of the European Union, OJ C 364/01, 18.12.2000 [hereinafter *EU Charter*].
[23] Treaty of Lisbon, OJ C 306, 17.12.2007.
[24] Electronic Communications Act of 1986, codified at 18 U.S.C. § 2511 et seq.

and government access to communications records). In both cases a legislative act implements a regime balancing privacy interests against other interests, providing detailed procedures that operate on top of a constitutional baseline of rights protection.

Article 7 of the EU Charter provides "Respect for private and family life. Everyone has the right to respect for his or her private and family life, home and communications."[25] Article 8 of the Charter provides "Protection of personal data[]. Everyone has the right to the protection of personal data concerning him or her."[26] These rights are related, but distinct in the sense that "[d]ata protection focuses on whether data is used fairly and with due process while privacy preserves the Athenian ideal of private life."[27] The GDPR is intended to give detail to these rights in ways that are reasonable, and that also respect other interests and other fundamental rights.

Constitutional rights in European law operate differently from the way constitutional rights operate in American law. First, there are far more constitutional rights in Europe than in the U.S. For example, while the U.S. Bill of Rights,[28] the three Civil War Amendments,[29] and the Nineteenth Amendment[30] represent 14 fundamental rights articles, the EU Charter has over 50 articles protecting a wide variety of rights as diverse as a prohibition on torture,[31] human trafficking,[32] and child labor.[33] At the same time, unlike the U.S. Constitution, which largely protects only negative rights ("freedom from" various problematic government actions), the EU Charter protects many affirmative rights ("freedom to" perform certain human activities). Thus, the Charter also provides fundamental rights and freedoms including rights to dignity,[34] life,[35] marriage,[36] academic and scientific freedom,[37] education,[38] choosing an occupation,[39] conducting a business,[40]

[25] *EU Charter*, art. 7.
[26] *EU Charter*, art. 8.
[27] Hoofnagle, *supra* note 9, at 6 (citation omitted).
[28] U.S. CONST. amends. I-X.
[29] U.S. CONST. amends. XIII-XV.
[30] U.S. CONST. amend. XIX.
[31] *EU Charter*, art. 4.
[32] *EU Charter*, art. 5.
[33] *EU Charter*, art. 32.
[34] *EU Charter*, art. 1.
[35] *EU Charter*, art. 2.
[36] *EU Charter*, art. 9.
[37] *EU Charter*, art. 13.
[38] *EU Charter*, art. 14.
[39] *EU Charter*, art. 15.
[40] *EU Charter*, art. 16.

cultural, religious, and linguistic diversity,[41] rights of children and the elderly,[42] collective bargaining,[43] social security and health,[44] consumer protection,[45] and access to documents.[46] Important to this case, the Charter also grants a right to a fair trial, including that "Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal[.]"[47]

With so many broad positive and negative rights guaranteed in the EU, conflict between fundamental rights is inevitable. This brings up a second way in which European fundamental rights differ from American ones. Central to EU fundamental rights law the concept of "proportionality," the idea that rights are not absolute and that they must be tailored to circumstances, such as conflicts among rights or conflicts between rights and legitimate state objectives.[48] In this respect, and in my experience, the European use of the word "fundamental" is used in the sense of "foundational" rather than "absolute." To use examples from American usage, it is used more like the "fundamentals" of contract law (i.e., the basics) than "fundamentalism."

By contrast, fundamental rights in the United States are often more absolute where they apply. For example, it would be highly unlikely for an American court to require Google to stop displaying search results to an old newspaper article that indicated that a man had become bankrupt in the past. Yet this is exactly what the European Court of Justice did in the *Google Spain* case, using EU fundamental rights principles to balance between free expression and data protection rights (and using proportionality analysis to require Google to stop the search results but not requiring the newspaper's website to take them down).[49] The EU approach here was characteristically one of proportionality and balancing rather than absolutist. By contrast, in the United States, if the First Amendment were held to apply, it would be very unlikely for the government to insist on a strong form of such a "right to be forgotten."[50]

---

[41] *EU Charter*, art. 22.
[42] *EU Charter*, arts. 25-26.
[43] *EU Charter*, art. 28.
[44] *EU Charter*, arts. 34-35.
[45] *EU Charter*, art. 38.
[46] *EU Charter*, art. 42.
[47] *EU Charter*, art. 47.
[48] Paul M. Schwartz & Karl-Niklaus Peifer, *Transatlantic Data Privacy*, 106 Geo. L. J. 115, 131 (2017).
[49] *Google Spain & Google Inc. v. AEPD* (ECJ, 13/5/2014, C-131/12), paras 63-88.
[50] Neil Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age 90-92 (2005); Jeffrey Rosen, Response: The Right to Be Forgotten, 64 Stan. L. Rev. Online 88 (2012).

The GDPR applies the idea that proportionality and balance surround 'fundamental rights' in the context of data protection.[51] In addition to its official text, the GDPR includes 173 Recitals, explanatory notes intended to provide interpretive context.[52] In the first Recital, the GDPR announces that "The protection of natural persons in relation to the processing of personal data is a fundamental right" and that European law "provide[s] that everyone has the right to the protection of personal data concerning him or her."[53] But then in the fourth Recital, the GDPR announces that:

> The processing of personal data should be designed to serve mankind. The right to the protection of personal data *is not an absolute right*; *it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*. This Regulation respects all fundamental rights and observes the freedoms and principles recognized in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, *the right to an effective remedy and to a fair trial*, and cultural, religious and linguistic diversity.[54]

Thus, the GDPR interprets the privacy rights it is protecting at the outset as ones that must be balanced in general against and accommodated to other rights and interests, and explicitly includes the right to an effective remedy and a fair trial as one of those rights.

Along with expressly noting the need to balance data protection rights against other fundamental rights (including what we would call due process rights in the U.S.), the GDPR also expressly balances the data protection right against the free flow of personal data.[55] A major goal of European data protection law over the past two decades has been to ensure that personal information flows freely throughout the EU (and, where appropriate, outside the EU), but that data protection rights are respected at the same time. This is recognized in Article 1 of the GDPR, which provides that "[t]he free movement of personal information within the Union shall be neither restricted nor prohibited for reasons connected with the

---

[51] See also Paul M. Schwartz & Karl-Niklaus Peifer, Transatlantic Data Privacy, 106 Geo. L. J. 115, 131 (2017) ("When these other interests conflict with data protection, EU courts undertake a proportionality analysis.").
[52] *GDPR*
[53] *GDPR*, Recital 1.
[54] *GDPR*, Recital 4 (emphasis added).
[55] *See GDPR*, Recital 3.

protection of natural persons with regard to the processing of personal data."[56] Recital 6 explains further that

> Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further *facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data*.[57]

Illustrating this tension, in a recent article two leading privacy law scholars – one American and one German – concurred that:

> EU law safeguards not only privacy and data protection, but also the free flow of information. It does so as part of its goal of establishing an internal market for personal data in which there is 'free movement of goods, persons, services and capital,' as the Data Protection Directive expressed in 1995. The twin goals, then, are to ensure both a free flow of personal data from one member state to another and high standards of data protection to protect 'the fundamental rights of individuals.'[58]

The scholars continue by noting that EU law recognizes the importance of international flows of information as well, and that EU law balances these and other conflicts through "proportionality analysis."[59]

C. Reasonableness over Unyielding Strictness

The GDPR requires that the processing (essentially, the collection, storage, use, or disclosure) of personal data in the EU take place under a "lawful basis."[60] Article 5(1)(c) of the GDPR sets out some principles relating to the processing of personal data, including that data be "*adequate*, *relevant* and limited to what is necessary in relation to the purposes for which they are processed."[61]

---

[56] *GDPR*, art. 1.
[57] *GPDR*, Recital 6 (emphasis added).
[58] Paul M. Schwartz & Karl-Niklaus Peifer, Transatlantic Data Privacy, 106 Geo. L. J. 115, 130-31 (2017) (citation omitted).
[59] *Id.*
[60] *See GPDR*, arts. 5-6.
[61] *GDPR*, art. 5(1)(c).

Article 5(1) of the GDPR thus continues in the familiar EU vein of reasonableness and proportionality, rather than talking in terms of absolute or strict necessity. The text of the GDPR occasionally uses the word "necessary," but it does not do so in a way that evokes strict or absolute necessity.[62] Thus, Article 5 requires not strict necessity, but that processing be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[63] "Adequacy" and "relevance" are expansive concepts rather than limiting or absolutist ones, and the section itself provides context that the word "necessary" should be interpreted not by some external notion of strictness but in "relation to the purposes for which the[data] is processed."[64] Requiring data to be both "adequate" and "relevant" while limited to what is not "necessary" in the context of a discovery request is a far cry from strict or absolute necessity.

The GDPR does not talk in terms of "necessity," but rather states that data processing be "necessary" under the circumstances. This is an important distinction because the word "necessary" has a broad range of meanings that include reasonable appropriateness under the circumstances. The U.S. Constitution, for example, gives Congress the power "to make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or any Department or Officer thereof."[65] As all American lawyers know, in the landmark case of *McCulloch v. Maryland*,[66] the state of Maryland challenged the federal government's chartering of a bank as beyond its powers (i.e., that it was not "necessary" to regulate Commerce). Writing for the Supreme Court, the great Chief Justice John Marshall rejected this argument, explaining (as relevant here) that "necessary" in that context meant not strict necessity, but instead a broader notion of reasonable appropriateness.[67]

Another area in which U.S. and EU law are harmonious is the importance of proportionality in discovery. Federal Rule of Civil Procedure 26, for example, relies on the principle of proportionality as its touchstone:

> Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues,

[62] *See GDPR*, art. 5(1).
[63] *Id.*
[64] *GDPR*, art. 5(1)(c).
[65] U.S. Const. Art. I § 8.
[66] 17 U.S. (4 Wheat.) 316 (1819).
[67] *Id.* at 413-19.

> and whether the burden or expense of the proposed discovery outweighs its likely benefit.[68]

That being said, the definition of "necessary" in the GDPR is not so broad as to impose no limitation. Rather, the limitation is significantly less strict than one of strict necessity – that only the absolute minimum necessary personal data can be processed or transferred to the U.S. as part of a protected discovery request. It is more appropriate to read the word "necessary" in context with the other words in the text of the GDPR, which require data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[69] These are terms of reasonableness, appropriateness, and proportionality, which are consonant with similar norms of U.S. discovery.

Finally, even Article 9 of the GDPR, which addresses sensitive data (such as health or religious beliefs), provides that the heightened protections for sensitive data "shall not apply" when "processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity."[70] The relevant recital to this provision further provides that "[a] derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure."[71] Even given the importance of protecting sensitive data, the importance of the proper function of the justice system is an interest so compelling as to win out when balanced against data privacy.

***

Taking a step back, the GDPR is a complex enactment that seeks to balance a variety of often competing interests – data protection, other fundamental rights, practicality, state interests in governance, and private interests such as contractual rights and the "legitimate interests" of individuals and businesses. It should thus not be a surprise that with so many interests to balance, the GDPR is characterized by flexibility and the hallmarks of proportionality that we see elsewhere in EU fundamental rights law. Yet, at bottom, it bears repeating, the GDPR seeks to balance the data protection rights of humans in the EU with the reality that flows of personal data have become a hallmark of the European economy and society.

II. CO-OPTING THE GDPR

[68] FRCP 26(b)(1). See also *The Sedona Conference, International Principles on Discovery, Disclosure & Data Protection in Civil Litigation* (Transitional Edition), at 12-13 (Jan. 2017).
[69] *GDPR*, art. 5(1)(c).
[70] *GDPR*, art. 9(2)(f).
[71] *GDPR*, Recital 52.

The necessary flexibility of the GDPR that allows it to be applied to virtually all processing of personal data in the EU also creates risks of co-option. In a series of recent cases brought by U.S.-based plaintiffs, EU-based defendants have tried to resist ordinary discovery requests by attempting to have all personal information redacted from their discovery responses. In a case where, for example, U.S. plaintiffs might sue a German automaker for false statements made about a car's emissions standards, plaintiffs would make what would be (under U.S. law at least) ordinary discovery requests to produce emails, organization charts, test results, and other responsive documents. It would hardly require a seasoned civil litigator to recognize that civil discovery without actual names would not only make litigation more difficult, but it would also place a substantial burden on plaintiffs in their ability to uncover (for example) either ordinary civil fraud or a conspiracy to circumvent environmental and consumer protection laws. But in such cases, the reason offered for such a limited response to the discovery requests is often couched in GDPR terms – the idea that a defendants' employees had fundamental rights in data protection that would be infringed by the ordinary civil process, even where the documents would be disclosed under a protective order of the sort typically used to protect confidential information disclosed in civil discovery.

Although many might think that stonewalling of this sort would be facially unreasonable, the complexity of the GDPR has allowed a series of defendants to argue (ostensibly with a straight face) that while civil discovery containing real names in the US might be unobjectionable, European fundamental rights law prohibits it. Moreover, when cases of this sort are litigated in federal court by federal district or magistrate judges with limited experience and training in European fundamental rights law, there is a significant opportunity for mischief by defendants advancing a privacy pretext of this sort.

This Part explains why a civil discovery response seeking anonymous or pseudonymous discovery is not required by law, and in so doing illustrates the ways in which technical data protection rules created for the purpose of limiting corporate power in the context of personal data can actually be co-opted to advance it. After a brief explanation of the basic legal methodology used by U.S. courts to resolve discovery disputes of this sort, it explains why both the governing text and official guidance given by EU regulators illustrates how GDPR-mandated pseudonymous discovery is being asserted in an attempt to co-opt the GDPR's data protection rules.

Under current U.S. law, a court facing a claim that an otherwise relevant and responsive discovery request containing real names would violate the GDPR must analyze the issue under a three-step analysis. First, the court must determine whether civil discovery responses represent a lawful basis for processing under the

GDPR. Second, it must determine whether, lawful basis notwithstanding, the GDPR would allow the transfer of the personal data in the discovery response outside the EU to the United States. Third, even if EU law might prevent the discovery request, the court would have to apply the test in the *Aeropostale* case to conduct an international comity analysis about whether the discovery order might nonetheless be valid and enforceable in a U.S. court.

1. Lawful Basis. The GDPR's basic approach, common to data protection regimes, is that all processing of personal data must have a lawful basis if it is going to be carried out. At the outset, disclosure of civil discovery requests would undoubtedly fall within the GDPR's broad definition of processing, so there would have to be a lawful basis for it to be carried out. Article 6(1) of the GDPR offers six separate grounds for the lawful processing of data – (1) the consent of the "data subject" (the person to whom the data relates), (2) processing pursuant to the performance of a contract, (3) processing that "necessary for compliance with a legal obligation to which the controller is subject," (4) processing that is necessary to protect the vital interests of a natural person, (5) processing necessary for a task carried out in the public interest, and (6) processing that is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[72] Additionally, for all processing that is not carried out with the consent of the data subject, GDPR Article 6(4) requires a further balancing test involving the relationship between the processing and the reason the data was collected in the first place, the context and nature of the relationship between the data subject and the entity processing the data, the kind of data being processed, possible consequences to the data subject of the processing, and the existence of "appropriate safeguards, which may include encryption or pseudonymization."[73]

Notwithstanding the GDPR's many articles regulating personal information, responding to lawful discovery requests undoubtedly constitutes a "legitimate interest" under Article 6(1) of the GDPR, and this includes the transfer of personal information to the United States "if it is necessary for the establishment, exercise, or defence of legal claims."[74] Article 6(1) does not include a specific derogation for processing the data in the same way that Article 49(1)(e) provides. This had led some commentators to conclude that the problem with transnational discovery takes place not at the transfer stage, governed by Article 49(1)(e), but rather at the

[72] GDPR art. 6(1).
[73] GDPR art. 6(4).
[74] *See GPDR*, art. 49(1)(e).

processing stage.[75] However, their understanding of the word "necessary" is in stark contrast to the legal principles explained previously in this paper.[76] If necessary is taken in the context of the other articles of the GDPR[77] and the spirit of European human rights law, then it clearly leads to a balancing of important legal interests. It follows that "necessary" under the GDPR is harmonious with U.S. discovery procedure,[78] and U.S. litigation and discovery is a legitimate interest under Article 6(1). Moreover, given the GDPR's strong preference for data flows within the EU compared to its relative reluctance to allow data to flow outside the EU, it would be absurd for it to be read to allow data transfer overseas to countries with lesser levels of data protection, but not allow that data to be processed within the EU.

2. International Transfer. Consistent both with prior practice under the Directive and with its twin goals of allowing data flow and ensuring data protection, the GDPR restricts data flows outside of Europe, requiring a separate legal justification if data is to be exported outside the EU. Ideally, this would be to a country that has received an "adequacy" determination by the European Commission, certifying that its domestic data protection regime has been deemed as essentially equivalent in its protections to that of the GDPR.[79] In such a case, the foreign country would become functionally part of the EU for purposes of the limitations on data export. To date, while a number of countries around the world have been held to be adequate, the United States is not one of them. Other grounds that can be used to justify cross-border data flows include model contracts, binding corporate rules, and approved codes of conduct.[80]

Beyond these principal grounds for cross-border transfer, Article 49 of the GDPR contains a series "derogations" or exceptions for specific situations. These include consent by the data subject, transfers necessary for the performance of certain contracts, reasons of important public interest, the "vital interests" of natural persons, and (of special importance here) litigation. Thus, article 49(1) of the GDPR explicitly allows for emails containing personal data to be transferred to the United States if they are "necessary for the establishment, exercise, or defense of legal claims."[81] This text is supplemented by its corresponding Recital, which makes clear that

---

[75] Gary Weingarden & Matthias Artzt, "Stuck in the middle with you: When US discovery orders hit GDPR," *IAPP* (Jan. 26, 2021). https://iapp.org/news/a/stuck-in-the-middle-with-you-when-u-s-discovery-orders-hit-the-gdpr/.
[76] *See Id. See also supra* notes 52-62.
[77] *See supra* notes 53-54 and 61-62.
[78] *See supra* note 59 and accompanying text.
[79] GDPR art. 45.
[80] GDPR art. 46.
[81] *GDPR*, art. 49(1).

> Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, *where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies.* Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.[82]

Considering these requirements in the context of cross-border discovery requests, it is notable that Recital 111 authorizes transfers that are "occasional and necessary in relation to a contract or a legal claim."[83] Discovery responses to relevant requests for production should fall within the plain terms of this standard: relevant and proportional discovery requests are both "occasional" and "necessary." Discovery requests are "occasional" in that they are infrequent, and are different from, for instance, the constant processing of data in the U.S. by a company like Google or Facebook to serve smartphone applications installed by their EU customers (i.e., search requests or Newsfeed stories). Relevant and proportional discovery requests are also "necessary" to vindicate legal claims, not only under the plain meaning of the term, but also because of principles of due process (itself a fundamental right in both Europe and the U.S.).[84] The exception for legal production not only includes court proceedings at its core, but its breadth also encompasses a wide variety of tribunals such as regulatory bodies.[85] The anticipated discovery requests in this case would thus be within the heart of the derogation rather than at the periphery. Thus, any balancing of the legitimate interest in the production of a reasonable set of relevant business documents to establish a legal claim pursuant to a well-crafted protective order would cut in favor of the discovery of such documents.

Further, outside the context of litigation discovery, Recital 111 contemplates "transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register

---

[82] *GDPR*, Recital 111 (emphasis added).
[83] *Id.*
[84] *See* U.S. Const., amend. V *and GDPR*, Recital 4, *and EU Charter*, art. 47.
[85] *GDPR*, Recital 111.

established by law and intended for consultation by the public or persons having a legitimate interest."[86] The Recital explains that in this "latter case" (but presumably not in the case of litigation discovery):

> such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.[87]

This Recital would consider discovery responses to relevant requests for production as less threatening to the values of data protection than this other category of "register transfer" data, particularly where the documents are to be produced subject to a protective order. Article 49 and Recital 111 strengthen the view that notions of reasonableness and proportionality run throughout the GDPR's approach to data protection, specifically in the context of the production of a defined set of relevant evidence subject to a protective order.

Beyond the text and recitals of the GDPR, advisory materials from official EU data protection bodies also shed light on the availability of the Article 49(1) derogation for cross-border litigation. The European Data Protection Board ("EDPB") is an independent European Body composed of the EU's national data protection commissioners, with the responsibility of ensuring a consistent interpretation of the GDPR throughout Europe.[88] It has the authority to adopt general guidance to interpret the GDPR and to issue decisions that bind individual EU data protection authorities to ensure a consistent administrative interpretation of EU law. That said, it is not a court, and its interpretations of EU law are not final.[89] Nevertheless, the EDPB and its Data Protection Directive-era precursor, the

---

[86] *Id.*
[87] *Id.*
[88] *See* European Commission, What is the European Data Protection Board (EDPB)?, available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en.
[89] *Id. accord* Chris Jay Hoofnagle et al., The European Union General Data Protection Regulation: What It Is And What It Means (September 24, 2018), at 8. UC Berkeley Public Law Research Paper. Available at SSRN: https://ssrn.com/abstract=3254511 ("Now that the GDPR is enforceable, its interpretation is entrusted to the courts, combined with persuasive, albeit non-binding, interpretation by the newly created European Data Protection Board.").

Article 29 Working Party,[90] are composed of knowledgeable EU government regulators, and their reports are entitled to due consideration.

The EDPB guidance of most significant relevance to this case is the "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679" (hereinafter "The Guidelines")[91] As the title of this document suggests, this relatively short, 17-page report offers guidance on the provisions of GDPR Article 49 that permit transfer of personal data to "third countries," including the United States, in the context of pretrial discovery.[92]

The Guidelines explain that, in general, for transfers of European personal data to the U.S., it is necessary to satisfy both the general requirements of the GDPR for processing as well as the specific requirements of Article 49 for transfer.[93] The EDPB explains at the outset that "the WP29, as predecessor of the EDPB, has long advocated as best practice a layered approach to transfers," involving a consideration of whether the "third country has an adequate level of data protection and ensuring that the exported data will be safeguarded in the third country."[94] As a note, the EDPB expressly terms its "layered approach" a "best practice," rather than a practice mandated by the GDPR, as Defendants suggest, for neither the GDPR's text nor its recitals explicitly require such an approach. The EDPB, as an association of national data protection enforcement officers, itself acts in an advocacy or advisory capacity here, rather than being an authoritative interpreter of the GDPR.

With respect to the "necessity" test in Article 49 of the GDPR, the EDPB explains that "[t]his test requires an evaluation by the data exporter in the EU of whether a transfer of personal data can be considered necessary for the specific purpose of the derogation to be used."[95] It then refers the reader to the "specific application of the necessity test" for each of the specific "derogations" in Article 49.[96]

This leads us to the specific interpretations of the Article 49 derogations offered by the EDPB. With respect to the derogation at Article 49 (1)(e), the EDPB explains that, among other forms of legal procedure, "data transfers for the purpose of formal pre-trial discovery procedures in civil litigation may fall under this

---

[90] Art. 29 WP. Available at https://ec.europa.eu/justice/article-29/documentation/index_en.htm.
[91] European Data Protection Board, "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679" (May 25, 2018). Available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf. [hereinafter "The Guidelines"]
[92] *Id.*
[93] *Id.* at 3.
[94] *Id.* (footnote omitted).
[95] *Id.* at 5.
[96] *Id.*

derogation. [However, T]he derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future."[97] The EDPB notes that

> The combination of the terms 'legal claim' and 'procedure' implies that the relevant procedure must have a basis in law, including a formal, legally defined process, but is not necessarily limited to judicial or administrative procedures ('or any out of court procedure'). As a transfer needs to be made in a procedure, a close link is necessary between a data transfer and a specific procedure regarding the situation in question. The abstract applicability of a certain type of procedure would not be sufficient.[98]

To put the text in the preceding paragraph into terminology more familiar to American lawyers, Article 49(e)(1) can be used for discovery seeking relevant information in the context of targeted discovery requests in a legal action, but not for fishing expeditions before a lawsuit has been filed.

This brings us back to the "necessity test," which some scholars have characterized as one that is a "high bar."[99] Even the EDPB, however, does not describe its test in these terms. Instead, it interprets the GDPR to mean that:

> A data transfer in question may only take place when it is necessary for the establishment, exercise or defense of the legal claim in question. This 'necessity test' requires a close and substantial connection between the data in question and the specific establishment, exercise or defense of the legal position. The mere interest of third country authorities or possible 'good will' to be obtained from the third country authority as such would not be sufficient. Whilst there may be a temptation for a data exporter to transfer *all possibly relevant personal data in response to a request* or for instituting legal procedures, this would not be in line with this derogation or with the GDPR more generally as this (in the principle of data minimization) emphasizes the need for personal data to be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*.[100]

This test is not a "strict" one as most would understand the term, but one that instead requires a close relationship between the information being sought and the legal claim in question – one that defines necessity in terms of adequacy and relevance for purpose. This guidance is not one requiring strict necessity, but rather

---

[97] *Id.* at 11.
[98] *Id.* at 11-12.
[99] *See* Gary Weingarden & Matthias Artzt, "Stuck in the middle with you: When US discovery orders hit GDPR," *IAPP* (Jan. 26, 2021). https://iapp.org/news/a/stuck-in-the-middle-with-you-when-u-s-discovery-orders-hit-the-gdpr/.
[100] The Guidelines at 12 (emphasis added).

actual relevance to a legal claim. The EDPB itself draws a distinction between transfer of "all possibly relevant personal data" (which is not permitted) and that which is "adequate, necessary, and relevant."[101] Again, this is a test rooted in reasonableness rather than strictness.

In the subsequent paragraph of the Guidelines, the EDPB further refines its definition of the 'necessity test.' It explains that:

> Whilst there may be a temptation for a data exporter to transfer all possibly relevant personal data in response to a request or for instituting legal procedures, this would not be in line with this derogation or with the GDPR more generally as this (in the principle of data minimization) emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[102]

This requirement should be read to require relevance rather than strict necessity; indeed, the EDPB itself uses the term "relevant" in its definition. Moreover, the personal data obtained must also be "adequate" and "limited to what is necessary" for the establishment of the claim.[103] This further reinforces the view that the EDPB's standard is far closer to the relevance standard familiar to American lawyers than the notion of strict necessity put forth by other scholars.[104]

Finally, while the EDPB does address the "layered approach" recommended by its predecessor the Article 29 Working Party under the now-superseded Data Protection Directive,[105] it describes this approach expressly in terms of relevance, which is a very different interpretation from the "strict" one that has been advanced by the Defendants here and in prior proceedings before this Court.[106] The EDPB notes:

> In relation to litigation proceedings the WP29, predecessor of the EDPB, has already set out a layered approach to the question of whether the personal data should be transferred, including the application of this principle. As a first step, there should be a careful assessment of whether anonymized data would be sufficient in the particular case. If this is not the case, then transfer of pseudonymized data could be considered. If it is necessary to send personal data to a third country, its *relevance* to the particular matter should be

[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *See* Weingarden & Artzt, *supra* note 87.
[105] The Guidelines at 3.
[106] *Id* at 12.

> assessed before the transfer – so only a set of personal data that is *actually necessary* is transferred and disclosed.[107]

Relevant to the conversation of the definition of "necessary," the EDPB uses "actually necessary" and "relevance" interchangeably to describe its standard.[108]

It is important to note that the EDPB analysis, by its terms, does not require data to be anonymized or pseudonymized in the first instance. Instead, it requires a layered approach to the data being requested.[109] If the personal data is relevant to the establishment of a legal claim, then the personal data must be disclosed.[110] Similarly, personal data that is not relevant to the legal claim need not be disclosed without redaction.[111] In this way, consistent with the overriding principle of proportionality in European law, the EDPB suggests that the GDPR balances the data protection rights of the Defendants' employees with the weighty interests of due process and consumer protection. This is the interpretation of the GDPR provisions best calculated to, in the language of GDPR Recital 4, ensure that "[t]he processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; *it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*."[112]

This test, then, is not "strict," except insofar as it requires strict adherence to the principle of relevance. The EDPB guidance may require a layered *analysis* of the information being sought before transfer, but it does not require presumptive bulk anonymization of data sought in pretrial discovery, particularly where the data will be disclosed under a protective order. A requirement of this sort would frustrate the ability of Plaintiffs to establish legal claims in ways that would seem to be highly disproportionate to the weighty interests on both sides of the calculus here, as well as to the general approach of reasonableness and proportionality that runs through European law here. In particular, anonymization or pseudonymization of emails, for example, would make it impossible to effectively conduct discovery into legal claims, particularly claims involving commercial fraud or unfair business practices which might require the connection of multiple individuals to establish the claim. Moreover, such a time-intensive, burdensome, and likely expensive approach to discovery in a complex civil case is at odds with both the GDPR's approach to reasonableness and proportionality and the plain text of Article 49.

---

[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *GDPR*, Recital 4 (emphasis added).

In July 2020, the Court of Justice of the European Union issued a decision that shook the relationship between the United States and the European Union's data relationship.[113] *Data Protection Commission v. Facebook Ireland, Schrems*,[114] or *"Schrems II"* is the second case in a saga regarding the validity of data transfers between the United States and the European Union.[115] In the first case, *Schrems I*, the Court invalidated the "Safe Harbour" that existed between the United States and the European Union because transfers to the United States made the data of European citizens vulnerable to unwanted processing and use.[116] In response, the United States and the European Union agreed to a provisional framework, the Privacy Shield, to replace the Safe Harbour and allow for lawful U.S. processing of EU citizen data.[117] *Schrems II* invalidated the Privacy Shield agreement, reading it as "incompatible with Article 45(1) of the GDPR, read in the light of Articles 7, 8, and 47 of the Charter."[118]

While the long-term impact of *Schrems II* is still being debated, the decision undoubtedly limited cross-border data transfers in a significant way.[119] *Schrems II* prohibits any transfer of data to a third country unless there is an adequacy determination for that country's privacy laws, meaning that they meet a standard "essentially equivalent" to that of the GDPR.[120] Two things are obvious from reading the opinion. First, there is a heavy emphasis on the rights of individuals and a concern for their being infringed. The Court's language implies that it is not so much concerned with the sanctity or integrity of the GDPR as a regulatory matter, but with "the issue of whether [the Privacy Shield] decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals."[121] Second, the language is highly restrictive of data transfers in the absence of an adequacy decision. For example:

> unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses

---

[113] Caitlin Fennessy, "The 'Schrems II' decision: EU-US data transfers in question," *IAPP* (Jul. 16, 2020). https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.
[114] Case C-311/18, Data Protection Comm'r v. Facebook Ireland, Ltd., Schrems, 2020 E.C.R. I-559. [hereinafter *Schrems II*].
[115] *See* Enrnst-Oliver Wilhelm, "A Brief History of Safe Harbor," *IAPP*. https://iapp.org/resources/article/a-brief-history-of-safe-harbor/. *See also* Case C-362/14, Schrems v. Data Protection Comm'r, 2015 E.C.R. I-650. [hereinafter *Schrems I*].
[116] *See generally Schrems I*.
[117] *See* Wilhelm, *supra* note 103.
[118] *Schrems II*, para. 199.
[119] Jordan L. Fischer, *The U.S. Perspective on Schrems II: The Challenges of the Extraterritorial Application of the EU Perspective*, 51 SETON HALL L. REV. 1565 (2021).
[120] *Schrems II*, para. 191.
[121] *Schrems II*, para. 158.

> adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation and by the Charter of Fundamental Rights, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.[122]

Given the concerns expressed by the opinion, it could be read to be more restrictive of data transfers and require more in their justification. However, the opinion, in its last line before the "Costs" section, reads:

> As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum, the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.[123]

In considering an explicit derogation at Article 49, *Schrems II* increases the need for a broader reading of these provisions. Because Article 49 is now, post-*Schrems II*, the legal regime in place for cross-border data transfers, the provision must be robust and substantive. While it may be tempting to read Article 49(1)(e) more narrowly in response to the principled language in *Schrems II*, the opinion left it to fill a legal vacuum necessitating a more robust interpretation.

As a final note on the GDPR's regulation of cross-border data flows, a common concern that EU defendants have cited in urging that the GDPR requires pseudonymous discovery is enforcement of fines and punishments against them for violating the GDPR. They have raised the specter that if they were to disclose personally identifiable information from relevant documents under a protective order, they would run the risk of the new fines introduced by the GDPR, and even the possibility of criminal sanctions.[124]

This argument is similarly unconvincing for several reasons. First, well-crafted discovery subject to a protective order, as explained above, should not be a violation of the GPDR. Enforcement actions in a society committed to the rule of law presuppose some legal violation to be enforced. Even in the instance that they are

---

[122] *Schrems II*, para. 203.
[123] *Schrems II*, para. 202 (citations omitted).
[124] *See*, *e.g.*, *In re Mercedes-Benz Emissions Litigation*, No. 16-cv-881 (KM) (ESK) 2020 WL 487288 (D.N.J.) at n.5.

violative of the GDPR, enforcement concerns are still simply not justifiable. It is correct that one of the most significant differences between the old Data Protection Directive and the new GDPR is that the GDPR permits imposing fines for data protection violations. Still, there are no instances in which an EU data protection authority has fined an EU company for producing records containing relevant personal information pursuant to a U.S. court order.

In recent months, European data protection authorities have imposed fines and engaged in litigation under the GDPR and other EU data protection rules,[125] including holdover litigation like the *Schrems* case[126] that involves pre-GDPR legal rules.[127] In the last few years, there have indeed been enforcement actions by European regulators that have resulted in fines, including actions by the German Data Protection Authority.[128] But we have seen similar fines and enforcement priorities in the United States as well in the data protection context, including an SEC fine imposed on Facebook for misleading securities disclosures over its privacy practices,[129] an FTC fine imposed on Facebook of $5 billion for the Cambridge Analytica Scandal,[130] and an FTC fine of nearly $600 million imposed on Equifax for its own enormous data breach.[131]

The hallmark of these cases on both sides of the Atlantic is that they involved serious breaches of privacy or data protection expectations – vast data breaches, election tampering, or securities law noncompliance. As a group of internationally renowned American and Dutch privacy scholars explained recently, "U.S. lawyers have fretted about perfect compliance, but in reality, European regulators rarely expect such compliance, nor will they impose 8-figure liability for imperfections. As

---

[125] *See*, e.g., Natasha Lomas, "WhatsApp faces $267M fine for breaching Europes' GDPR," *TechCrunch* (Sept. 2, 2021). https://techcrunch.com/2021/09/02/whatsapp-faces-267m-fine-for-breaching-europes-gdpr/.

[126] *See generally Schrems I*.

[127]

[128] *See*, *e.g.*, Lennart Schuessler & Oliver Schmidt-Prietz, "German Data Protection Authority imposes another major GDPR fine," *Bird & Bird*. (Sept. 202). https://www.twobirds.com/en/news/articles/2020/germany/german-data-protection-authority-imposes-another-major-gdpr-fine.

[129] Securities and Exchange Commission, Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data, July 24, 2019, available at https://www.sec.gov/news/press-release/2019-140.

[130] Federal Trade Commission, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, July 24, 2019, available at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[131] Federal Trade Commission, "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019). https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

we explain below, massive liability is years away, but it will also be keyed to serious wrongdoing rather than accident or simple noncompliance."[132]

3. International Comity.

The third and final stage in a court's analysis is what a US court supervising discovery must do if it finds that foreign law prohibits the transfer of personal data in the form that it is sought. In cases of this sort, U.S. courts have devised a system of balancing international objections with discovery concerns. In determining which rules apply to discovery procedures, U.S. courts look to the rule of international comity. Comity is defined as, "A principle or practice among political entities (as countries, states, or courts of different jurisdictions), whereby legislative, executive, and judicial acts are mutually recognized."[133] A comity analysis helps courts to determine whether or not to order discovery in the face of objections by foreign litigants,[134] in these cases, concerns over GDPR violations. The seminal case for analyzing comity is *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for the Southern Dist. of Iowa*.[135] In that case, the Court articulated a set of factors that have been used by district courts when dealing with issues of comity:[136]

1. the importance to the ... litigation of the documents or other information requested;
2. the degree of specificity of the request;
3. whether the information originated in the United States;
4. the availability of alternative means of securing the information; and
5. the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.[137]

---

[132] Chris Jay Hoofnagle et al., The European Union General Data Protection Regulation: What It Is And What It Means (September 24, 2018). UC Berkeley Public Law Research Paper. Available at SSRN: https://ssrn.com/abstract=3254511.
[133] Comity, Black's Law Dictionary (11th ed. 2019).
[134] *See* George L. Washington, Jr., *An Examination of Factors Considered by U.S. Courts in Ruling on Requests to Conduct Discovery of Information Located in Foreign Countries*, ABA Annual Meeting (Aug. 8, 2014).
[135] 482 U.S. 522 (1987).
[136] *See* Washington, Jr.*, supra* note 122.
[137] *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for the Southern Dist. of Iowa*, 482 U.S. 522, n.28 (1987).

Using the concept of comity as a precursor to their decisions, a number of U.S. courts have ruled on the GDPR cross-border discovery issue. In *In re Mercedes-Benz Emissions Litigation*,[138] the Defendants argued that the GDPR prevented them from disclosing certain documents during the discovery process and that there was potential for enforcement action against them should they produce.[139] The Court upheld the finding of the Special Master appointed to the case that "on balance, the U.S. had a stronger interest in protecting its consumers than the EU did in protecting its citizens' private data, particularly with a Discovery Confidentiality Order provision allowing producing parties to designate and protect foreign private data as 'Highly Confidential' information."[140]

The Special Master's ruling relied in part on a case captioned, *Finjan, Inc. v. Zscaler, Inc.*[141] This case stands for the proposition that, as part of the comity analysis, issuing a protective order diminishes the interest that the European company has in the privacy of individuals revealed by its documents under the GDPR.[142] The Court in *Finjan* ordered the production of emails over GDPR objection finding, "that the GDPR does not preclude the Court from ordering Defendant to produce the requested e-mails in an unredacted form, subject to the existing protective order."[143]

Related case law has revealed the same,[144] that American courts do not find the discovery process, especially when production is subject to a protective order, violative of the GPDR. This, of course, is subject to change under a common law system. However, the case law in favor of discovery reveals three things. First, when companies regulated by the GDPR cite to privacy concerns as a reason not to disclose relevant documents and information during discovery, they do so in opposition to a growing mound of case law saying that they must produce. Second, a group of trained and respected legal professionals in the United States are in agreement that the GDPR does not prevent such disclosures during discovery. Third, the enforcement and privacy concerns cited by these regulated companies have not realized in the time since these type of objections began to take place. Nevertheless, these assertions that the GDPR requires the obstacle of pseudonymization based upon a pretextual assertion of employee privacy by a company can prove to be unexpected, time-consuming, and difficult for courts and litigants to resolve. Particularly where the GDPR comes out of the blue to surprise an American trial judge who is unlikely to have had much experience with

---

[138] No. 16-cv-881 (KM) (ESK) (D.N.J.), 2020 WL 487288.
[139] *Id.* at *8.
[140] *Id.*
[141] No. 17-cv-06946-JST, 2019 WL 618554, at *1 (N.D. Cal. Feb. 14, 2019).
[142] *Id.* at *3.
[143] *Id.*
[144] *See supra* note 4.

European data protection law, claims of this sort can often only be resolved by resort to expensive battles of the experts, further adding to litigation costs and placing additional burdens on plaintiffs with meritorious claims who seek to vindicate them as part of their access to justice.

III. CONCLUSION: PRIVACY PRETEXTS AND THE CO-OPTION OF PRIVACY

American legal history is full of many examples in which powerful entities have tried to turn legal rules to their own advantage—often with surprising success. In the *Lochner* era, for instance, business interests were able to assert classically liberal claims of "freedom of contract" to forestall regulation and to force workers to accept substandard wages while they themselves build vast fortunes at a previously unimaginable scale. Indeed, a number of scholars (including the present author) have argued that digital platforms may be asserting a new generation of *Lochner*-style rules by wielding a libertarian reading of the First Amendment to eliminate restrictions on data flows under the misleading claim that "data is speech."[145] Power, it seems, is ever-eager to co-opt otherwise neutral rules to serve its own interests.

This leads us back nicely to the problem of pretextual readings of the GDPR that are used to advance the interests of the very entities that the GDPR seeks to regulate. In the form of a pretextual GDPR discovery objection, European corporations that are bound to observe the data protection rights of their employees and customers are seeking to turn the GDPR into a shield with which to forestall other forms of regulation such as consumer and environmental protection rules, making it more costly to vindicate claims of asserted commercial fraud by means of a reading of the GDPR that is itself a kind of falsehood. Moreover, there is a growing body of evidence that the pretextual uses of privacy claims are on the rise. In the cases involving the rights of trans people to use the bathrooms that correspond to their gender identities, for example, Susan Hazeldean has documented how anti-trans advocates have argued that the privacy interests of women and girls are violated by laws or policies that permit "men" (*i.e.*, those who identify as trans women) to use women's bathrooms – privacy interests that fall apart under scrutiny.[146] In a series of articles on corporate behavior and competition policy, Rory Van Loo has argued that digital platforms have used a variety of pretextual privacy and other claims to advance their interests in anticompetitive ways, including the anticompetitive blocking of financial technology startups,[147] and

[145] cite
[146] Hazeldean, *Privacy As Pretext*, supra, at 1721.
[147] Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 242–43 (2018).

undermining regulatory monitoring of their businesses more generally.[148] In an analogous vein, Rebecca Wexler has argued that platforms have often used privacy rationales to withhold potentially exculpatory evidence from criminal defendants.[149]

Such strategic and pretextual uses of privacy have started to gain the attention of regulators. In the summer of 2021, Facebook blocked a group of researchers NYU's Ad Observatory from accessing its systems under the rationale that it was required to do so under the terms of its FTC consent order stemming from the Cambridge Analytica scandal. (That scandal involved Facebook sharing vast amounts of customer data with a right-wing psychological warfare company that then sought to use the date to influence the 2016 Brexit Referendum in Britain and the 2016 Presidential election in the United States). When the FTC learned of Facebook's actions against the NYU researchers, the Director of the FTC's Bureau of Consumer Protection wrote to the company in his official capacity. The letter admonished both Facebook's pretextual use of the consent decree and its failure to seek guidance from the FTC about whether the consent decree justified such an action. The letter concluded with the warning that "[w]hile it is not our role to resolve individual disputes between Facebook and third parties, we hope that the company is not invoking privacy – much less the FTC consent order – as a pretext to advance other aims."[150] Subsequently, in her written testimony before Congress in October 2021, FTC Chair Lina Khan echoed this theme by noting that "recognizing that privacy and competition are interconnected is not the same as claiming that competition and privacy always align. Indeed, recent events are surfacing the ways in which the pretext of privacy may be weaponized to undermine competition on the merits, and scholars have long recognized that unfettered competition can fuel a race-to-the-bottom."[151]

The best conclusion that can be drawn from this mounting body of evidence is that privacy pretexts, which we should understand as the co-option of privacy rules to serve institutional rather than individual interests are on the rise. Moreover, the phenomenon of privacy pretexts seems to be more common than the existing privacy literature and discourse has appreciated. In practice, this means not just that scholars must pay an increased attention to the risks and practice of privacy co-

---

[148] Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L.REV. 1563 (2019).

[149] Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721 (2021).

[150] Letter from Acting Director of the Bureau of Consumer Protection Samuel Levine to Facebook Aug. 5, 2021, https://www.ftc.gov/news-events/blogs/consumer-blog/2021/08/letter-acting-director-bureau-consumer-protection-samuel

[151] Federal Trade Commission, Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security, https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf

option, but that policymakers creating new privacy rules and courts that interpret those rules must be vigilant against its risks. Given the ability of powerful entities to bend both actors and outputs to their own ends (and I include here policymakers and scholars as well as legal rules at their creation and in their application) there will be no easy fixes. However, recognizing the problem of co-option is an important place to start. In many ways, such problems are a product of privacy law's success, but the future of privacy law must find a way to transcend those problems if it is to live up to its intended promise.