Northwestern Journal of International Law & Business

Volume 42
Issue 1 *Fall*

Article 2

Fall 2021

Winter is Here: The Impossibility of Schrems II for U.S.-Based Direct-to-Consumer Companies

Vanessa Zimmer

Vol. 42, No. 1
Northwestern Journal of International Law & Business

Winter is Here: The Impossibility of *Schrems II* for U.S.-Based Direct-to-Consumer Companies

Vanessa Zimmer*

Abstract

In this paper, Vanessa Zimmer exposes the precarious position of Direct-to-Consumer (DTC) companies that are physically located in the United States but still subject to the European General Data Protection Regulation (GDPR) under Article 3(2) because they offer goods or services to European consumers online. Standard Contractual Clauses (SCCs) and supplementary measures have dominated privacy conversions in the year since the European Court of Justice invalidated the EU-U.S. Privacy Shield framework with its Schrems II decision.

However, Zimmer argues that the greater issue for U.S.-based DTC companies is the lack of clarity over what constitutes an international, or restricted, transfer under the GDPR in the first place. Is an international transfer any physical transfer of personal data from within the European Economic Area to outside its borders (the so-called "geographic" definition of international transfer) regardless of whether the foreign recipient is already directly subject to the GDPR? Or, is an international transfer only considered such if the recipient is located outside of the European Economic Area and not already directly subject to the GDPR (the so-called "jurisdictional" definition of international transfer)? Zimmer explains the rationale for each position and ultimately argues in favor of a jurisdictional definition of international transfers.

The European Data Protection Board of the European Commission (the EDPB) and individual Member State supervisory authorities have repeatedly failed to define international transfers since the passage of the GDPR. This repeated failure to clarify the interplay between the territorial scope of the GDPR under Article 3(2) and the transfer restrictions of the GDPR under Chapter V has left U.S.-based DTC businesses uncertain of whether they are making international transfers under the GDPR and whether they must subsequently implement safeguards, such as SCCs, to protect those transfers.

Zimmer explains how the Schrems II decision exposed the EDPB's failure and exacerbated the already uncertain status of European personal data processing

* Vanessa Zimmer is a Lecturer of Law at the University of Southern California Gould School of Law, a Lecturer in Legal Studies at the College of Business of the California State University, Long Beach, a practicing Attorney (Zimmer Legal, https://www.zimmer.legal/), a mother of three, and a *Game of Thrones* enthusiast.

by U.S.-based DTC companies. The EDPB has further complicated the status of international transfers in its post-Schrems II guidance and its issuance of new SCCs for international transfers.

Zimmer contends that it is vital for the sake of transatlantic trade and the continued integrity of the EDPB that the EDPB clearly defines international transfers and explains the applicability of transfer mechanisms to U.S.-based DTC companies.

TABLE OF CONTENTS

INTRODUCTION

For the past 24 months since the July 2020 *Schrems II* judgment of the European Court of Justice (CJEU), cross-border data transfers have been at the tip of every privacy professional's tongue. Overnight, the CJEU took an already fuzzy view of international transfers under the General Data Protection Regulation (GDPR) even further out of focus. Since then, we field questions from clients, discuss the topic amongst ourselves, attend webinars, and, if we counsel U.S.-based Direct-to-Consumer, or "DTC," companies on privacy matters, we pull our hair in frustration. However, even as guidance from the European Data Protection Board (EDPB) of the European Commission brings some things back into focus, the question of what constitutes an international transfer under the GDPR remains unanswered, to the detriment of U.S.-based DTC companies.

Since *Schrems II,* the European Commission has focused its guidance on the implementation of supplementary measures to complement the use of Standard Contractual Clauses (SCCs) and it has issued new SCCs in June 2021. However, this focus has distracted from the more important question of how DTC companies can lawfully continue to serve European customers from the United States when the SCCs (supplemented or not) are inappropriate for their use.

Somehow, in the age of the Internet where anyone can know anything in the blink of an eye, there is still an astounding lack of clarity around how the GDPR's territorial scope rules and data transfer rules interact with each other. As Christopher Kuner has pointed out, "[D]espite the obvious relevance of these two sets of rules to each other, and the fact that they are based on the same rationale, their interaction has received little attention in academic literature, court judgments, or DPA guidance, and has been shrouded in mystery."[1]

This enduring mystery causes hand-wringing and uncertainty and has financial costs. According to Axios, "U.S. businesses that operate internationally say they've lost 'tens of millions' of dollars thanks to the legal logjam, according to Jules Polonetsky, CEO of the Future of Privacy Forum, an industry-backed nonprofit. 'European companies are being cautious and not going ahead with transactions until there is clarity.'"[2]

At issue is the question of whether Chapter V of the GDPR is intended to restrict only transfers that would not otherwise be subject to the GDPR

---

[1] Christopher Kuner, *Territorial Scope and Data Transfer Rules in the GDPR: Realizing the EU's Ambition of Borderless Data Protection,* UNIVERSITY OF CAMBRIDGE, Paper No. 20/2021 (April 2021) (Eng.), at 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850.

[2] Ashley Gold, *Businesses fall into transatlantic privacy hole,* AXIOS (May 12, 2021), https://www.axios.com/businesses-fall-transatlantic-privacy-hole-5162814b-9684-469d-b0ba-bc0705ebb44b.html?mkt_tok=MTM4LUVaTS0wNDIAAAF9Bak0IfHkqb6niAeFt6DIzPc-Xu81TXyYeMmdgqQtk1-yw9lDs3r5VidhvHVaNUUFN6swqC1JiX80_XmnXRY2yqX6QCNtPPMhWFviyMkjf2dG.

(the "jurisdictional" view) or to restrict all physical movement of personal data outside of the European Economic Area (the "geographic" view). Under the jurisdictional view, U.S. DTC companies would need no safeguard, such as SCCs, to accept personal data from the European Economic Area (EEA). However, under the geographic view, they would need a safeguard, despite the current unavailability of any suitable safeguards.

In Part I of this paper, I provide an overview of the U.S. DTC market as context for the importance of the notion of international transfers under the GDPR. In Part II, I describe the history of restricted international transfers and explain that prior to the GDPR, the more limited territorial scope of European privacy law resulted in a broad, geographic notion of international transfers.

In Part III, I explain that the expanded territorial scope of the GDPR brought the very notion of international transfers into question. Did a geographic notion apply where processing by U.S.-based DTC companies that was an international transfer under the Directive remained so under the GDPR? Or did a jurisdictional notion apply where this processing was no longer an international transfer because it was a behavior that brought the company under the scope of Article 3(2)? I also explore the continued use of safeguards, including the EU-U.S. Privacy Shield, by U.S. DTC companies even after the GDPR's effect as a failsafe for compliance with the transfer restrictions of Chapter V of the GDPR if a geographic notion was intended.

In Part IV, I introduce the complexities of the *Schrems II* decision by the European Court of Justice. The Court's invalidation of the Privacy Shield framework as a safeguard further forced the question of how international transfers should be interpreted. Although the Court's decision implied a geographic view, this view would make it impossible for U.S.-based DTC companies to legally transfer data from the EU, as there are no suitable safeguards under Article 46 of the GDPR.

In Part V of this paper, I describe how, through a combination of contradictory regulation, caselaw, formal guidance, informal commentary, and silence, the Europeans have boxed themselves into a corner where neither the geographic definition nor jurisdictional definition of international transfer makes complete sense. As a result, U.S.-based DTC companies have little idea of whether their processing of EU data is viewed as an international transfer and whether they need to implement safeguards and supplementary measures to legalize the transfer.

In Part VI, I propose that the EDPB confronts past confusion head-on by issuing clear and practical guidance for U.S.-based DTC companies that serve European customers. I advocate for a jurisdictional definition of international transfers as the most logical way forward. The EDPB must go back to the basics of GDPR compliance and root its guidance in the unquestionable fact that the core principles relating to processing personal data under the GDPR apply to the collection of EU personal data by U.S.-based DTC companies regardless of whether Chapter V so applies.

I. THE U.S.-BASED DIRECT-TO-CONSUMER MARKET

The modern U.S. Direct-to-Consumer market is ubiquitous. Even those of us without Instagram accounts know a DTC ad when we see it—washed color-branding, inoffensive typeface, and the bold proclamation of offering you the last Chelsea boots, terry joggers, or cast-iron frying pan you will ever need. With technology moving at an ever-quickening pace, it is easy to overlook that DTC companies are a relatively new phenomenon. Prior to about 2010,[3] manufacturer-brands generally did not sell their products directly to consumers; rather they sold their products to intermediary distributors or wholesalers who in turn sold the products to retail consumers.[4] As a result, historically manufacturer-brands did not collect much, if any, consumer personal data.[5]

In fact, *no one* was collecting much, if any, consumer data prior to the DTC revolution. Short of addressing limited product safety recall concerns,[6]

---

[3] "Ever since the godfather of the DTCs, Warby Parker, emerged on the startup scene in 2010, venture firms have funded hundreds of startups trying to mimic that model." Maya Kosoff, *Why all the Warby Parker Clones are now Imploding*, MARKER (Mar. 9, 2020), https://marker.medium.com/why-all-the-warby-parker-clones-are-now-imploding-44bfcc70a00c.

[4] "Merchant wholesalers had dominated American distribution for much of the 19th century, buying from manufacturers and selling to retailers on their own terms, sometimes under their own unadvertised labels." George S. Low & Ronald A. Fullerton, *Brands, Brand Management, and the Brand Manager System: A Critical-Historical Evaluation,* 31 J. OF MARKETING RES. 173, 176 (May 1994), https://www.jstor.org/stable/pdf/3152192.pdf?ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A0bf9256df6ab81d19f7ffe2264062a58.

[5] By the 2000s, some manufacturer-brands like Proctor & Gamble had implemented nascent customer loyalty programs. However, many questions remained about the purpose of these programs and how they affected relationships between consumers, retailers, and manufacturer-brands. "With the technological advances we are seeing in industry, some new questions also arise: what role will/should manufacturers and retailers play in each other's loyalty programs? What is the impact of loyalty in one channel (say offline) on loyalty in an online channel? How will improved measurement of loyalty and its transparency affect the interaction between manufacturers and retailers? Large scale customer relationship programs (e.g., HomeMadeSimple.com by Proctor & Gamble) that provide data on tens of millions of customers to CPG manufacturers may also alter the relative push-pull power structure between manufacturers and competing retailers." Kusum L. Ailawadi, Eric T. Bradlow, Michaela Draganska, Vincent Nijs, Robert P. Rooderkerk, K. Sudhir, Kenneth C. Wilbur & Jie Zhang, *Empirical Models of Manufacturer-Retailer Interaction: A Review and Agenda for Future Research,* 21 MARKETING LETTERS 273, 281 (Sept. 2010), https://www.jstor.org/stable/pdf/40959646.pdf?ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3Ae81d65a9cadd33241d31de704f378715.

[6] *See* U.S. CONSUMER PRODUCT SAFETY COMM'N, RECALL HANDBOOK 19 (Mar. 2012), https://www.cpsc.gov/s3fs-public/pdfs/blk_pdf_8002.pdf ("[D]irect notice to consumers known to have the product – identified through registration cards, sales records, catalog orders, retailer loyalty cards, or other means" as a suggested method of identifying purchasers of a recalled product.").

retailers were not obligated to keep detailed logs of each consumer transaction. As such, retail outfitters focused on merchandising and bringing consumers to their stores for access to products that would have been otherwise unavailable.[7] The shopping mall was still king, and the brands stocked within its stores were mere feudal subjects.

The early exception was the rising powerhouse Amazon.com, which began to pivot from mere book-peddling to total world domination in August of 1998.[8] Jeff Bezos' personal life may be the stuff of tabloid fodder,[9] but his business acumen cannot be denied. Bezos understood and harnessed the power of consumer data while most retailers were still patting themselves on the back for having a customer loyalty program. Although it would be eleven years[10] before Amazon began manufacturing and selling its own house-brand of goods, it was able to leverage those years of direct relationships with Amazon customers to ensure its house brands would flourish.

Amazon had a data visionary bedfellow in Netflix. Founded in 1998, the company initially sent physical DVDs to its customers who managed their accounts through Netflix's website.[11] Netflix began offering streaming services in 2007,[12] and in 2012 inched even closer to a closed loop ecosystem when it began producing its own streaming content.[13]

However, aside from these two outliers, traditional brick-and-mortar retail continued to rule the roost until approximately 2010, when the ocular

---

[7] "[T]he mall offered access to a broader world than flyover country could easily access. And unlike the Sears catalog, it did so directly and immediately, live and in person." Ian Bogost, *When Malls Saved the Suburbs from Despair*, THE ATLANTIC (Feb. 17, 2018), https://www.theatlantic.com/technology/archive/2018/02/when-malls-saved-cities-from-capitalism/553610.

[8] *See* Saul Hansell, *Amazon.com is Expanding Beyond Books,* N.Y. TIMES (Aug. 5, 1998), https://www.nytimes.com/1998/08/05/business/amazoncom-is-expanding-beyond-books.html.

[9] Jim Rutenberg and Karen Weise, *Jeff Bezos Accuses National Inquirer of 'Extortion and Blackmail,* N.Y. TIMES (Feb. 7, 2019), https://www.nytimes.com/2019/02/07/technology/jeff-bezos-sanchez-enquirer.html.

[10] "Amazon introduced its first in-house brands—AmazonBasics and Pinzon, which both sell everyday household goods—in 2009." Kevin Lamb, *All you Need to Know about Amazon's Privacy Label Brands*, PATTERN (Jul. 2, 2021), https://pattern.com/blog/all-you-need-to-know-about-amazons-private-label-brands.

[11] NETFLIX, https://about.netflix.com/en (last visited Aug. 19, 2021) ("1998 – Netflix.com, the first DVD rental and sales site, is launched.").

[12] *Id.* ("2007 – Streaming is introduced, allowing members to instantly watch series and films.").

[13] *Id.* ("2012 – Membership reaches 25 million members, and expands into the United Kingdom, Ireland and the Nordic Countries. Netflix ventures into stand-up specials with 'Bill Burr: You People Are All the Same'. 2013 – 'House of Cards,' 'Hemlock Grove,' 'Arrested Development' and 'Orange Is the New Black' usher in the first slate of original series programming.").

disrupter Warby Parker burst onto the business scene.[14] It seems trite now, but at the time, it was downright revolutionary for a brand to market and distribute its physical products directly to customers over the Internet. In the words of Warby Parker themselves, "[I]t was really about bypassing retailers, bypassing the middle person that would mark up lenses 3 – 5x what they cost, so we could just transfer all of that cost directly to consumers and save them money."[15]

Warby Parker was almost immediately successful,[16] and thus, the Internet gave birth to a legion of copycats seeking to disrupt the way we sleep,[17] dress,[18] shave,[19] and even eat.[20] The DTC movement has been described by *Harvard Business Review* as: "defined by borrowed supply chains, web-only retail, direct distribution, social media marketing, and a specific visual brand identity (the now ubiquitous "blanding") that favored sans-serif type, pastel color palettes, and scalable logos that were easily adapted to a variety of digital media."[21]

Many of these companies also offer subscription services, which not only provide a steady stream of repeat sales, but also provide a steady stream of consumer personal data.[22] Whereas only a decade earlier, the average clothing brand knew relatively little about the person wearing their wares, the modern DTC clothing brand has a data lake from which to dredge the

---

[14] Steve Denning, *What's Behind Warby Parker's Success?*, FORBES (Mar. 23, 2016), https://www.forbes.com/sites/stevedenning/2016/03/23/whats-behind-warby-parkers-success/?sh=43f690c8411a ("Warby Parker was founded in 2010, by four friends, Neil Blumenthal, Dave Gilboa, Andy Hunt and Jeff Raider, who happened to be in business school.").

[15] *Id.*

[16] The company had obtained annual revenue of $35 million in 2013 and was valued at $450 million. Sara Ashley O'Brien, *Warby Parker could be next $1 billion company*, CNN (Mar. 5, 2015), https://money.cnn.com/2015/03/05/technology/warby-parker-valuation.

[17] CASPER, https://casper.com (last visited Aug. 19, 2021).

[18] EVERLANE, https://www.everlane.com (last visited Aug. 19, 2021).

[19] HARRY'S, https://www.harrys.com/en/us (last visited Aug. 19, 2021).

[20] BLUE APRON, https://www.blueapron.com (last visited Aug. 19, 2021).

[21] Leonard A. Schlesinger, Matt Higgins & Shaye Roseman, *Reinventing the Direct-to-Consumer Business Model*, HARV. BUS. REV. (Mar. 31, 2020), https://hbr.org/2020/03/reinventing-the-direct-to-consumer-business-model#.

[22] Tony Chen, Ken Fenyo, Sylvia Yang & Jessica Zhang, *Thinking Inside the Subscription Box: New Research on E-commerce Consumers*, MCKINSEY & COMPANY (Feb. 9, 2018), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/thinking-inside-the-subscription-box-new-research-on-ecommerce-consumers ("Subscriptions are an increasingly common way to buy products and services online. Although streaming-media subscriptions have been popular for some time—46 percent of consumers in our survey subscribed to an online streaming-media service, such as Netflix—shoppers are now also turning to subscriptions for consumer goods. Our research indicates that 15 percent of online shoppers have subscribed to an e-commerce service over the past year.").

most specific or general data about its consumers.[23] Those that were early to the party also had the benefit of "advertising arbitrage that could be exploited on underpriced social media platforms."[24]

It is debatable whether DTC has taken retail's crown, but irrefutable that DTC is at least a Great House,[25] with a total estimated revenue of almost 18 billion U.S. dollars in 2020.[26] There are roughly 400 DTC brands.[27] In 2021, e-commerce is expected to account for 6.6% of all consumer-packaged goods (CPG) sales, and the DTC movement accounts for 40% of the sales growth in the CPG sector.[28]

The DTC revolution means that a brand looking to jump across the pond into international consumer waters no longer needs to have a physical location in the European Union, nor do they need to find a European distribution partner. Rather, they merely need to start to accept orders from EU shipping addresses. In short, collecting EU consumer data and processing it back home in the United States has never been easier for U.S.-based companies.

II. PRE-GDPR RESTRICTIONS ON INTERNATIONAL TRANSFERS

Just as easily as a DTC company can be founded and funded, so too can it be grabbed by the long arm of European privacy law. Years before the GDPR (formally known as Regulation (EU) 2016/679 of the European Parliament) became the belle of the privacy ball, U.S.-based companies with European customers had to consider the European Union's restrictions on the international transfer of personal data. This is because although non-EU companies were not directly subject to the GDPR's predecessor, the European Commission Directive 95/46/EC (the Directive),[29] they were

---

[23] Elise Dopson, *DTC-First: Why More Brands are Using the Direct-to-Consumer Model*, SHOPIFY PLUS (Apr. 8, 2021), https://www.shopify.com/enterprise/direct-to-consumer ("Take Molson Coors, for example. After pivoting its business to sell DTC online, it made some optimizations based on data it had collected. That included: Catering to consumers' requests for a wider range of products. Optimizing its site visuals for mobile, since mobile traffic accounted for half of all store visits. Running A/B tests on landing pages and creative messaging to see which its consumers responded to best.").

[24] Schlesinger, *supra* note 21.

[25] A WIKI OF ICE AND FIRE, https://awoiaf.westeros.org/index.php/List_of_Houses (last visited Aug. 19, 2021).

[26] STATISTA, https://www.statista.com/statistics/1109833/usa-DTC-ecommerce-sales/#:~:text=In%202019%2C%20direct%2Dto%2D,Club%2C%20and%20mattress%20company%20Casper (last visited Aug. 19, 2021).

[27] Kosoff, *supra* note 3.

[28] Dopson, *supra* note 23.

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L. 281) art. 4 (emphasis added). National law applicable: "1. Each Member State shall apply the national provisions it adopts pursuant to this Directive

prohibited from receiving personal data from companies that were so subject unless certain safeguards were in place.[30] The territorial jurisdiction of the Directive staved off any pedantic debates about jurisdictional or geographic definitions of international transfers because each definition would result in the same consequence—that an international transfer was taking place and should be restricted unless protective measures were guaranteed.

In contrast, the free flow of personal data among European Member States have almost never been in doubt as "this principle is inferred from the four fundamental freedoms of movement which define the EU, i.e., free movement of persons, goods, services, and capital introduced by the 1957 Rome Treaty establishing the European Economic Community."[31]

In laymen's terms, the Europeans[32] trusted each other to honor their mutually understood and singular commitment to privacy as those in Westeros trust each other to honor their mutually understood and singular commitment to guest rights (that is, until Walder Frey came along).[33] Unsurprisingly, this trust did not extend to so-called "third countries" that are based outside of the European Economic Area, unless the third country had been deemed "adequate" in the eyes of the European Commission. An adequacy determination required that the laws of the third country "prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union."[34] On the basis of these criteria, the European Commission granted adequacy status to Argentina, Canada, Israel, Japan, New Zealand, Switzerland, and Uruguay under the Directive.[35]

Unfortunately, no such status was granted to the United States, perhaps due to the continents' "two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly

---

to the processing of personal data where: (a) the processing is carried out in the context of the activities of *an establishment of the controller on the territory of the Member State*; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law; (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated *on the territory of the said Member State*, unless such equipment is used only for purposes of transit through the territory of the Community."

[30] *Id.* art. 25.

[31] Mariusz Krzysztofek, GDPR: PERSONAL DATA PROTECTION IN THE EUROPEAN UNION 247 (Andrea Biondi ed., 2021).

[32] "*Id.* "Europeans" includes both European Union Member States and Iceland, Liechtenstein, and Norway, which are members of the European Economic Area.

[33] *Game of Thrones: The Red Wedding* (HBO television broadcast Jun. 2, 2013).

[34] Case C-362/14, *Schrems v. Data Prot. Comm'r*, EU:C:2015:650, ¶74 (Oct. 6, 2015) [hereinafter *Schrems*].

[35] KRZYSZTOFEK, *supra* note 31, at 252.

different laws of privacy."[36] Thus, since 1995, U.S.-based companies who wanted to receive personal data from the EEA had to take certain steps to legalize the transfers pursuant to Article 25 of the Directive, even if they themselves were not directly subject to the Directive.[37]

One step they commonly took was to implement SCCs between the European-based data exporting entity and the U.S.-based data importing entity. But while this method was quick and easy for many situations, it was not so for DTC companies as they do not have a separate legal entity based in the EU to act as a data exporter.

A second, more appropriate option for U.S.-based DTC companies was to self-certify to the EU-U.S. Safe Harbor framework. The Safe Harbor agreement was reached by the U.S. Department of Commerce and the European Commission in July 2000 (over the objections of the EU Parliament) as a method of ensuring the protection of personal data transferred from the EEA to U.S.-based companies.[38] Per Daniel Solove and Paul Schwartz:

> The Safe Harbor represented a bold policy innovation: it transplanted EU data protection concepts into U.S. law in a fashion beyond the willingness of Congress or the ability of the FTC and other regulatory agencies. Its Principles were intended to be close enough to those of EU data protection so that the U.S. companies in following them would provide 'adequate' data protection.[39]

By the time of its demise in 2015, over 5,000 companies had certified.[40]

Although the Safe Harbor framework provided U.S.-based companies with a relatively easy way to satisfy their limited obligations toward receiving personal data from Europe, or perhaps in part *because* it did this, a storm was brewing among European Union Member States.

Unlike its successor legislation, the GDPR, the Directive required EU Member States to achieve the results stipulated by Article 288 of the Treaty on the Functioning of the European Union by adopting their own, country-

---

[36] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1160 (2004). Interestingly, Whitman argues that a unique divergence between European and American privacy law is that Americans are wearier of government intrusions into their lives ("Most especially, state action will raise American hackles much more often than European ones."). I am not certain that this logic holds in light of *Schrems* & *Schrems II*, which focus almost entirely on the idea of excessive American government surveillance as being anathema to Europeans'.

[37] Directive 95/46/EC, *supra* note 29, art. 25.

[38] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1266 (Rachel E. Barkow et al. eds., 7th ed. 2021).

[39] *Id.*

[40] *Id.* at 1266-67.

specific implementing regulations.[41] In addition, the Directive functioned as a floor for regulation, and countries were free to reach for the ceiling by going beyond the minimum requirements of the Directive.[42] This resulted in a patchwork of "discrepancies between the regulations in each country,"[43] including those relating to international data transfers. For example, Austria, Belgium, Croatia, Cyprus, Estonia, France, Greece, Hungary, Latvia, Lithuania, Luxembourg, Malta, Norway, Portugal, Romania, Slovenia, and Spain each required consultation with (and in some cases approval by) the relevant data protection authority before the SCCs could be used as a transfer mechanism.[44] In the remaining Member States, no such formality was required, and implementation of SCCs was an internal corporate matter.

This lack of harmony ultimately undermined the Directive and gave way to the GDPR, which as a regulation needs no further action by Member States to be of full force and effect.[45] Regardless, the Directive was still in place when the Court of Justice of the European Union (CJEU) ended the

---

[41] "Directive 95/46/EC obliged the Member States, pursuant to Article 288 of the TFEU (Treaty on the Functioning of the European Union), to achieve the results stipulated therein, but it only defined the minimum required adjustment scope; any Member State could therefore go beyond those minimum requirements in the respective areas while adopting its own regulations, which led to discrepancies between the regulations in each country." KRZYSZTOFEK, *supra* note 31, at 5.

[42] *Id.*

[43] *Id.*

[44] "Despite pre-approval from the Commission, as a practical matter, some data protection authorities still require approval of the contractual clauses before transfer is permitted." HARVEY L. KAPLAN, MARK W. COWING, AND GABRIEL P. EGLI, A PRIMER FOR DATA-PROTECTION PRINCIPLES IN THE EUROPEAN UNION 44 (May 2009), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiJ8rn3jtLxAhXSo54KHfm8BsAQFjAHegQIEhAD&url=https%3A%2F%2Fwww.shb.com%2F-%2Fmedia%2Ffiles%2Fprofessionals%2Fc%2Fcowingmark%2Faprimerfordataprotectionprinciples.pdf%3Fla%3Den&usg=AOvVaw37V3j-D1nrblxLgerlLKYd. Pursuant to a protocol agreement between the Belgian Ministry of Justice and Belgian Privacy Commission, "all contractual clauses used to transfer personal data outside the EEA, to countries which do not offer an adequate level of protection, must now be submitted to the Privacy Commission for prior approval." Julie Hick, Vincent Wellens and Jacqueline Van Essen, *Standard Contractual Clauses for the Transfer of Personal Data: New Approval Procedure in Belgium*, MONDAQ (Jul. 17, 2013), https://www.mondaq.com/privacy-protection/251608/standard-contractual-clauses-for-the-transfer-of-personal-data-new-approval-procedure-in-belgium. "There are requirements for prior DPA approval of SCCs in Austria, Belgium, Croatia, Cyprus, Estonia, France, Hungary, Latvia, Lithuania, Luxembourg, Malta, Portugal (for transfers of non-sensitive data only), Romania, Slovenia, and Spain." LOKKE MOEREL, AN ASSESSMENT OF THE IMPACT OF THE SCHREMS JUDGMENT ON THE DATA TRANSFER GROUNDS AVAILABLE UNDER EU DATA PROTECTION LAW FOR DATA TRANSFERS TO THE U.S., 10 n.32 (2016), https://www.itic.org/dotAsset/d/2/d2988618-d28e-4888-a192-fd2cdc743a9a.pdf.

[45] It is important to note that there will still be some deviations in Member States' privacy and data protection laws both (1) in local areas where EU law does not apply and (2) where the GDPR itself permits such deviations, such as with regard to employment data under Article 88. KRZYSZTOFEK, *supra* note 31, at 6-8.

Safe Harbor's watch in its October 2015 judgement.[46]

The *Schrems I* case was brought by an Austrian plaintiff named Maximilian Schrems in response to Edward Snowden's leak of "documents that detailed widespread collaboration by American companies with the NSA and called into doubt the 'adequacy' of the protection in the [United States]."[47] Although the core privacy complaints of the case concern the social media monolith Facebook, Mr. Schrems raised the case as a complaint against the Irish Data Protection Commissioner "concerning the latter's refusal to investigate a complaint made by Mr. Schrems regarding the fact that Facebook Ireland Ltd ('Facebook Ireland') transfers the personal data of its users to the United States of America and keeps it on servers located in that country."[48] Because *Schrems I* predates the GDPR, the Court was forced to consider Facebook's U.S. processing of EU personal data in the context of international transfers under the Directive. Thus, while *Schrems I* does not give us direct guidance on the question of how to define international transfer under current EU privacy law (the GDPR), it does presuppose that Facebook Ireland's sharing of Mr. Schrems' personal data with Facebook in the United States constituted an international transfer under the GDPR's predecessor, the Directive.

In the wake of *Schrems I*, the U.S. Department of Commerce and the European Commission went back to the drawing table for a new solution. The result was the EU-U.S. Privacy Shield Framework, which was approved only four months after *Schrems I*, in February 2016.[49] Yet only two months after Privacy Shield's debut, the European Parliament passed the GDPR which would go into effect on May 25, 2018.[50] This timeline is important in understanding the current confusion over the definition of international transfer under the GDPR and whether U.S.-based DTC companies need to implement safeguard transfer mechanisms.

III. THE EXPANDED REACH OF THE GDPR AND THE INTERNATIONAL TRANSFER HOT POTATO

The European Commission and the U.S. Department of Commerce crafted Privacy Shield with the Directive in mind as a vehicle for U.S.-based companies that were not otherwise subject to EU privacy law to receive EU personal data from EU-based companies that were so subject. However, the GDPR vastly expanded the territorial scope of EU privacy law beyond just

---

[46] *Schrems, supra* note 34. *Game of Thrones: And Now His Watch Has Ended* (HBO television broadcast Apr. 21, 2013).

[47] SOLOVE AND SCHWARTZ, *supra* note 38, at 1267.

[48] *Schrems, supra* note 34, at ¶ 2.

[49] SOLOVE AND SCHWARTZ, *supra* note 38, at 1267.

[50] European Data Protection Supervisor, *The History of the European General Data Protection Regulation*, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Jul. 1, 2022).

those companies that were based within the European Union, bringing the future utility of Privacy Shield into question.

A. The Extraterritorial Scope of the GDPR

The GDPR clearly applies to EU-based companies and EU-based branches of foreign companies because they are "in the Union."[51] However, foreign companies need only jump from Article 3.1 to Article 3.2(a) to learn that the GDPR also clearly applies to companies with no physical presence in the EU if those companies offer goods or services to data subjects in the Union.[52] In the words of the EDPB:

> Article 3 of the GDPR defines the territorial scope of the Regulation on the basis of two main criteria: the 'establishment' criterion of physical location, as per Article 3(1), and the 'targeting' criterion of 'market location' as per Article 3(2).[53] Where one of these two criteria is met, the relevant provisions of the GDPR will apply to relevant processing of personal data by the controller or processor concerned.[54]

Prior to the EDPB's official guidance on the territorial scope of the GDPR, which was issued in November 2019, there had been much debate about what it meant to "offer goods or services" in the context of the territorial application of the GDPR.[55] Was it enough to merely make one's website available to users in the EU, or does one also need to actively market or otherwise target EU users?[56] Was the availability of content in the local

---

[51] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), 2018 O.J. (L 119) art. 3.1.

[52] *Id.* art. 3.1(a).

[53] SOLOVE & SCHWARTZ, *supra* note 38 at 1247 ("This provision relies on the 'principle of market location,' or, as the concept is expressed in German, the '*Marktortprinzip'*.").

[54] Wim Nauwelaerts, *EU: EDPB guidelines on the territorial scope of the GDPR*, ALSTON & BIRD 4 (Jan. 2020), https://www.alston.com/-/media/files/insights/publications/2020/01/eu-edpb-guidelines-on-the-territorial-scope-of-the.pdf.

[55] Renzo Marchini, *Does the EDPB answer frequently asked questions on territorial scope?*, FIELDFISHER (Nov. 28, 2018), https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/does-the-edpb-answer-frequently-asked-questions-on-territorial-scope ("Article 3 is supposed to answer the important questions of when GDPR applies (depending on the location of an entity processing personal data, or of the individuals whose data is being processed). Unfortunately, Article 3 was drafted in a way that left many key concerns unanswered.").

[56] Kuner, *supra* note 1, at 10. (The former EC Article 29 Working Party had previously noted that the transmission of personal data via cookies from an individual within the EU to a server stored outside the EU was enough to bring the server within the ambit of the national law of the EU Member State in which the individual resided.).

language relevant?[57] These are important questions, particularly for companies that offer the purchase of online services rather than physical goods. However, for the latter, it is clear that routinely accepting orders and shipping physical goods to the EU will qualify as offering those goods in the Union, and those DTC companies will be subject to the GDPR under Article 3(2).[58]

With regard to those DTC companies offering services, the EDPB's territorial guidelines include the fact that a "controller offers the delivery of goods in EU Member States"[59] as merely one consideration for whether the "targeting criterion" has been met.[60] However, just two paragraphs later, the EDPB "recalls that when goods or services are inadvertently or incidentally provided to a person on the territory of the Union, the related processing of personal data would not fall within the territorial scope of the GDPR."[61] Thus, it seems undisputed that anything other than an accidental fulfilment of an order from the EU would bring a DTC company within the territorial jurisdiction of the GDPR. Accordingly, regularly accepting consumer account registrations from the EU would subject it to the same.

The extraterritorial jurisdiction of the GDPR, in contrast to the more limited territorial jurisdiction of the Directive, means that, on the effective date of the GDPR, many Privacy-Shield certified companies would pivot from being mere recipients of transferred EU personal data to being directly subject to EU privacy law in their own right. This overnight pivot placed U.S.-based DTC companies and the privacy lawyers who counsel them in the unenviable position of having to become armchair experts[62] on the GDPR in a relatively short period of time.[63]

---

[57] "To establish whether a controller has such intention, the EDPB suggests assessing a combination of various factors, including reference to an EU address or phone number on an offering document and the use of a language or currency of one or more EU Member States." *Nauwelaerts*, *supra* note 54. The November 2019 EDPB guidelines include language as an indicator of "targeting" to be "taken into account in any *in concreto* analysis in order to determine whether the combination of factors relating to the data controller's commercial activities can together be considered as an offer of goods or services directed at data subjects in the Union." European Commission European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), Version 2.1,* 22 (Nov. 12, 2019), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [hereinafter EDPB Territorial Scope Guidelines].

[58] *Id.* at 18.

[59] *Id.*

[60] *Id*. at 17.

[61] *Id*. at 18.

[62] *Armchair Expert*, https://armchairexpertpod.com. (Armchair Expert is a funny, insightful, and downright delightful podcast hosted by Monica Padman and Dax Shephard. They have hosted hundreds of episodes on topics ranging from systemic racial inequality to UFOs, but to my knowledge have not yet devoted an hour to privacy and data protection. Monica & Dax, call me.)

[63] Over the past four years or so, I have often found myself wanting to say "[I am] not an

B. Restricted Transfers Under the GDPR

The GDPR continues the Directive's restrictive tradition by limiting international transfers to "a third country or to an international organization" to those that are conducted via the "conditions laid down" in Chapter V.[64] The first such condition is through an adequacy determination that was made prior to or after the effective date of the GDPR. The EDPB issued its first adequacy determination under the GDPR to Japan in 2019.[65] Two years later, it issued a draft decision in favor of adequacy for South Korea.[66] Most importantly, on June 28, 2021, the Commission issued a final (though temporary) adequacy determination for a post-Brexit United Kingdom.[67] However, adequacy has remained elusive for the United States.[68]

EU-certified attorney; I just play one on TV . . . er, I mean spend my days researching EU privacy law for fun."

[64] Regulation (EU) 2016/679, *supra* note 51, art. 44.

[65] KRZYSZTOFEK, *supra* note 31, at 252.

[66] European Commission Press Release IP/21/2964, *Data protection: European Commission launches the process towards adoption of the adequacy decision for the Republic of Korea* (Jun. 16, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964. Interestingly, the draft decision makes an exception for 3 categories of personal data relating to religious missionaries, candidates for political office, and certain personal credit information. These exceptions provide a window into the possibility (though admittedly not probability) of what a future U.S. adequacy decision could resemble. Might it be possible for the EDPB to regard the United States as adequate, subject to sectoral or FISA/Executive Order exceptions?

[67] European Commission Press Release IP/21/3183, *Data protection: Commission adopts adequacy decisions for the UK* (Jun. 28, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183. This was despite the fact that less than a month earlier, the European Court of Human Rights ruled that the U.K.'s spy agency, known as GCHQ, unlawfully collected massive amounts of surveillance data on Europeans, in violation of their privacy rights. Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14 and 24960/15 (May 25, 2021), https://hudoc.echr.coe.int/eng#%7B%22documentcollectionid2%22:%5B%22GRANDCHAMBER%22,%22CHAMBER%22%5D,%22itemid%22:%5B%22001-210077%22%5D%7D. It is likely no coincidence that two days later, on June 18, 2021, Elizabeth Denham, the U.K. Information Commissioner, issued a statement on the use of live facial recognition technology in public places. The Commissioner expressed that she is "deeply concerned about the potential for live facial recognition (LFR) technology to be used inappropriately, excessively or even recklessly," and acknowledges that "In the [U.S.], people did not trust the technology. Some cities banned its use in certain contexts and some major companies have paused facial recognition services until there are clearer rules." Elizabeth Denham, *Blog: Information Commissioner's Opinion addresses privacy concerns on the use of live facial recognition technology in public places,* INFO. COMMI'R'S OFF. (Jun. 18, 2021), https://ico-newsroom.prgloo.com/news/blog-information-commissioners-opinion-addresses-privacy-concerns-on-the-use-of-live-facial-recognition-technology-in-public-places?mkt_tok=MTM4LUVaTS0wNDIAAAF9vwtjrOvYQqAZ0xxGiDsic--Jo9z3H1JF1irh2cD1o1SUmS9ywdjEmxACGxEanTU8IxF5oVC6iQGgF9Nt0JJc4FArDBwChdbv2rhJWWyIr971.

[68] No country, not even my beloved United States of America, is perfect. However, I believe the United States has a strong argument for adequacy, particularly in light of the

As with the Directive, the GDPR does not entirely prohibit transfers to countries without an adequacy decision. Rather, the GDPR permits the transfer if the organization "has provided appropriate safeguards and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available."[69] At this point, DTC companies may be wondering, "[W]hat's the big deal? Can't we just put some language in our privacy policy and be done with it?" Oh, my sweet summer children;[70] if only.

Although the GDPR sets forth various safeguards for transfer,[71] notice via privacy policy is not one of them. Thus, while including a sentence like "By using this website, you consent to the transfer of your personal data from your country of residence to the United States," might make you feel good, it is not an approved safeguard under the GDPR (or a valid consent, for that matter). Rather, under Chapter V, transfers may occur pursuant to: (a) a legally binding and enforceable instrument between public authorities or bodies;[72] (b) binding corporate rules (BCRs);[73] (c) the Commission's SCCs;[74] (d) other standard data protection clauses adopted by an EU supervisory authority and approved the by the European Commission;[75] (e) an approved code of conduct;[76] or (f) an approved certification mechanism.[77]

At first glance, this seems like a cornucopia of safeguards from which U.S.-based DTC companies may choose. However, for reasons explained in Part IV below, each of these options are currently[78] unavailable to U.S.-based DTC companies in a post-*Schrems* world.

C. Defining "International Transfer" Under the GDPR Before Schrems II

The entirety of this paper up to this point assumes that an international transfer is taking place, and thus, needs to be safeguarded against. However, under the GDPR, it is far from clear that this is the case when a U.S.-based DTC company collects personal data from its EU customers.

Commission's findings regarding Argentina, Canada, Israel, and Uruguay. Alas, no one has asked my opinion on the matter (though to be honest, that has never stopped me from giving it) and the United States remains woefully inadequate in the eyes of our European peers.

[69] Regulation (EU) 2016/679, *supra* note 51, art. 46.1.

[70] *Game of Thrones: Lord Snow* (HBO television broadcast May 1, 2011) (Old Nan: "Oh my sweet summer child, what do you know about fear?"). Slang Lang, https://www.slanglang.net/slang/sweet-summer-child/ (last visited Aug. 20, 2021) ("The expression is used to describe someone who is naïve, inexperienced and untested by the harsh reality of the world.").

[71] Regulation (EU) 2016/679, *supra* note 51, at ch. V, art. 60.

[72] *Id.* art. 46(2)(a).

[73] *Id.* 46(2)(b).

[74] *Id.* art. 46(2)(c).

[75] *Id.* art. 46(2)(d).

[76] *Id.* art. 46(2)(e).

[77] *Id.* art. 46(2)(f).

[78] As of Aug. 20, 2021.

Determining the confines of a "transfer" or "international transfer" has always required wading in murky waters. In the 2003 *Lindqvist* case, the CJEU noted that the Directive did "not define the expression transfer to a third country in Article 25 or any other provision, including Article 2,"[79] and argued if "Article 25 of Directive 95/46 were interpreted to mean that there is transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet."[80] However, since *Lindqvist*, the CJEU has repeatedly declined to "opine on the conditions under which EU data protection law might (or might not) apply in third countries," demurring the pleas of referring national courts and others to address the interplay between the territorial scope of EU data protection law and data transfer restrictions in its *Google Spain*, *Schrems,* and *Schrems II* judgments.[81]

Thus, the result feared by the *Lindqvist* court in 2003 may have come to pass. As Krysztofek explains, a transfer will now be deemed to occur by the transmission of data:

> within an IT system belonging to the data controller, between the controller's units (departments, branches, joint service centres), even if the transfer does not involve any entities other than the controller . . . . The rules for transferring data apply to all forms of transfer, including sending personal data by e-mail, allowing someone access to a customer database, exchange of data through a dedicated application, communicating data in a telephone conversation or handing them over in paper documents etc."[82]

Given this broad definition, perhaps we should be asking what *is not* an international transfer, rather than what *is* an international transfer. The logical place to look for an answer to either of these questions would be the text of the GDPR itself. However, as Mariusz Krzysztofek points out, no legal definition of "transfer of data" is provided for in the text of the GDPR, and "the GDPR does not differentiate the requirements applicable to the transfer of data according to the intended scope of their processing in the third country after the transfer."[83] This open-endedness means that "international transfers" may include the obvious, such as when they are hosted on servers physically located outside of the EU (even if access to the data is not provided to persons located outside of the EU), as well as the less obvious, such as mere access of data that is hosted within the EU by persons located outside

[79] Case C-101/01, Criminal proceedings against Bodil Lindqvist, 2003 E.C.R. I-12971 (Nov. 6, 2003) [hereinafter *Lindqvist*].

[80] *Id.* ¶ 69.

[81] Kuner, *supra* note 1, at 8.

[82] KRZYSZTOFEK, *supra* note 31, at 248.

[83] *Id.*

of the EU.[84]

Either way, the European Parliament's failure to clearly define international transfer within the GDPR, and the EDPB's subsequent failure to issue an opinion on the matter, as it may do under Article 64(2) of the GDPR, left Privacy Shield adherents in a bind.[85] These U.S.-based companies were left to speculate about whether the sharing of data that was clearly an international transfer under the Directive remained an international transfer under the GDPR and whether they should remain certified to the Privacy Shield framework. After all, if a transfer was not occurring, why would they avail themselves of a transfer safeguard mechanism?

The EDPB's failure was noted by privacy watchers on the wall as soon as the EDPB issued its draft guidelines on the territorial scope of the GDPR in November 2018. At the time, DLA Piper noted, "the Guidelines do not address other key interpretive questions arising from Art. 3 and Chapter V (transfer restrictions)."[86] The Centre for Information Policy Leadership (CIPL) similarly requested guidance in its official comments to the draft guidelines.[87] It succinctly explained the critical consequences of the EDPB's continued failure to address the issue as follows:

> For the proper functioning of the GDPR legal regime, it is essential that this issue is considered and clarified by the EDPB and the EU Commission in consultation with experts and stakeholders. It is not clear whether this has been considered at all during the legislative debates on the GDPR and there is no evidence that the text of the GDPR contemplates what the interaction should be between Article 3 and Chapter V. Yet, as the jurisprudence and developments on data transfers mechanisms take course, this point will become critical.[88]

Interestingly, this much needed guidance on the interplay of Article 3.2 and Chapter V had purportedly appeared in an unpublished draft of the guidelines that was circulated two years before they were finalized.[89] That unpublished draft stated that Chapter V (the data transfer rules) should *not apply* in cases where the GDPR applies directly under Article 3, because "when the processing of personal data carried out by the data recipient

---

[84] *Id.* at 248-49.

[85] *See* Regulation (EU) 2016/679, *supra* note 51, art. 64(2).

[86] DLA Piper, *EU: New EDPB Guidelines on the Territorial Scope of the GDPR*, PRIVACY MATTERS (Nov. 28, 2018), https://blogs.dlapiper.com/privacymatters/eu-new-edpb-guidelines-on-the-territorial-scope-of-the-gdpr.

[87] Hunton Andrews Kurth, *Comments by the Centre for Information Policy Leadership on the European Data Protection Board's "Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)" Adopted on 16 November 2018*, CTR. FOR INFO. POL'Y LEADERSHIP, 19 (Jan. 18, 2019), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_edpbs_territorial_scope_guidelines.pdf [hereinafter *CIPL Comments*].

[88] *Id*. at 19.

[89] Kuner, *supra* note 1, at 17.

(controller or processor) in a third country is covered by the scope of the GDPR in accordance with Article 3, there is no lack of protection and Chapter V shall not apply to the passing of the data to the data recipient."[90] That is, the EDPB embraced a jurisdictional definition of international transfer in this unpublished draft.

Unfortunately, this crystal-clear guidance was missing from the EDPB's actual final guidelines on the territorial scope of the GDPR. In its place was a mere holding statement that the EDPB "will also further assess the interplay between the application of the territorial scope of the GDPR as per Article 3 and the provisions on international data transfers as per Chapter V. Additional guidance may be issued in this regard, should this be necessary."[91]

Alas, no further assessment has been publicly undertaken by the EDPB, despite global law firm Baker Hostetler's succinct response that "[i]ndeed, as noted by public commentary, it is necessary."[92] Baker's BigLaw counterpart, Sidley Austin, also explained that "during the public consultation many stakeholders raised questions about the interaction between the provisions in the GDPR around territorial scope and Chapter V of the GDPR."[93] Finally, the law firm Alston & Bird noted:

> A missing piece in the Guidelines is the interplay between the application of the territorial scope of the GDPR, as per Article 3, and the provisions on international transfers, as per Chapter V of the GDPR. Further regulatory guidance on this interplay is considered essential, as conventional data transfer mechanisms such as SCCs are not always suitable.[94]

The EDPB has provided no public reason for its failure to pick a side in the ongoing jurisdictional versus geographic debate. However, a recent comment by longtime Hamburg data protection enforcer Johannes Caspar provides a hint: "[o]ne of the faults in the GDPR system, he points out, is the way it gives regulators 'lots of room for interpretation' of the rules. 'At the end of the day, our energies are spent on infighting.'"[95]

---

[90] *Id*.

[91] EDPB Territorial Scope Guidelines, *supra* note 57, at 22.

[92] Andreas T. Kaltsounis, *Reexamining the GDPR's Territorial Scope*, BAKERHOSTETLER (Jan. 24, 2020), https://www.bakerlaw.com/alerts/2020/reexamining-the-gdprs-territorial-scope.

[93] Sidley Austin, *The Extra-Territorial Reach of EU Data Protection Law* (Jul. 2019), https://www.sidley.com/en/insights/publications/2019/07/the-extra-territorial-reach-of-eu-data-protection-law.

[94] Alston & Bird, *supra* note 54.

[95] Stephanie Bodoni, *Europe's Data Law Is Broken, Departing Privacy Chief Warns*, BLOOMBERG (June 25, 2021), https://www.bloomberg.com/news/articles/2021-06-25/eu-s-broken-gdpr-needs-fixing-departing-privacy-chief-warns?mkt_tok=MTM4LUVaTS0wNDIAAAF98ot6OBTo1xuOweoMmBkskQgPIPSsojPDXfgWPbG8Urm2MdGUgJiznyIy9YU5ICHKXO7xeW_Ih8VlgiSUdi8V4tB7rcib6FZC76BW1VThdrv0.

But while the EDPB has remained publicly mum on the matter, some individual Member States (or in the case of the United Kingdom, former Member States) have spoken out. For example, the U.K. Information Commissioner's Office has stated that an international transfer to an organization whose processing of the transferred data is also subject to the GDPR (albeit the U.K. GDPR) is not a restricted transfer and requires no additional safeguards.[96] Although the ICO has engaged in a consultation process that invites input on this stance,[97] its current jurisdictional definition is consistent with the EDPB's unpublished draft from September 2018.[98]

After the EDPB's publication of its final Article 3 guidelines, the CIPL continued to argue in favor of the jurisdictional definition, stating that in these situations where "the personal data flows directly from the data subject in the EU to the controller outside of the EU" the "non-EU organisation is subject to all GDPR provisions by virtue of Article 3(2)" and thus, "should not be subject to the provisions of Chapter V of the GDPR for the transfer of personal data between the EU data subject and the non-EU controller."[99] The CIPL had earlier entreated the EDPB to consider that "having organisations implement and accumulate different layers of compliance obligations may ultimately run counter to operational compliance and accountability."[100] The CIPL supported a jurisdictional definition of international transfer by noting both the reference to a "controller or processor" in Article 46; that is, without a "controller or processor in the EU, there can be no transfer of personal data under Chapter V."[101]

---

[96] Kaltsounis, *supra* note 92; in fact, the ICO has gone even further, stating that a transfer is not "restricted" if it is to someone "employed by you or by your company or organisation" and that transfer restrictions "only apply if you are sending personal data outside your company or organisation." U.K. Information Commissioner's Office, *Are We Making a Transfer of Personal Data Outside the UK?*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit (last visited Nov. 8, 2021).

[97] In August 2021, the ICO issued a draft international data transfer agreement (IDTA) and guidance to replace the old SCCs, which are still to be used for UK transfers (the new SCCs do not apply to the United Kingdom, as it is no longer part of the European Union after Brexit), as well as draft updates to its general guidance on international transfers under the UK GDPR. Within its document called "Consultation paper and questions," the ICO has maintained its position that "in order for a restricted transfer to take place, there must be a transfer from one legal entity to another." (*See* Proposal 1, page 10 of Consultation paper and questions.). However, with regard to transfers from one legal entity to another, the ICO has proposed retracting its current guidance that a restricted transfer only takes place where the importer's processing of the data is not subject to the UK GDPR. INFO. COMM'R'S OFF., *ICO consults on how organisations can continue to protect people's personal data when it's transferred outside of the UK*, https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-data-transferred-outside-of-the-uk.

[98] *See* Kuner, *supra* note 1, at 20.

[99] *CIPL Comments*, *supra* note 87, at 20.

[100] *Id*. at 19.

[101] *Id*. at 20.

Others have concurred, arguing that application of the data transfer rules of Chapter V of the GDPR requires the exporting entity to be located in the EU: "See Article 44 GDPR, which refers to compliance by 'the controller and processor,' meaning that the presence of a controller or processor in the EU carrying out the transfer seems to be a requirement for application of the rules."[102] Thus, it is feasible that without a controller or processor located in the EU, there can be no transfer from the EU; there is only a direct collection of data by the controller located outside of the EU.[103]

Despite these very convincing arguments for the inapplicability of transfer mechanisms to U.S.-based companies that were newly subject to European privacy law under GDPR Article 3(2), the U.S. Department of Commerce did not express an opinion one way or the other. The Department addressed the passage of the GDPR and the expanded territorial jurisdiction of EU privacy law under the GDPR. However, the U.S. architect of the Privacy Shield framework did not offer an opinion on how the GDPR affected U.S.-based companies who had certified to the Privacy Shield framework prior to the GDPR's effective date.[104] Rather, the careful wording of its "important note" deflects the issue, suggesting that even the Department may not know the European Commission's intended definition of international transfer.[105]

Member State supervisory authorities have also remained largely silent, perhaps in order to keep a broad, geographic definition of international transfers in their enforcement back pocket, in case it becomes useful.[106] In the absence of clear direction from either governmental body, it appears that companies chose to stay within the status quo of the framework rather than risk potential noncompliance with Chapter V in the event it was not precluded by Article 3(2). I am unaware of any organizations withdrawing from the Privacy Shield framework post-GDPR for this reason. To the contrary, from July 2017 (roughly a year before the GDPR went into effect) to July 2020, the framework saw a 125% increase in participants—from 2,400 to 5,400 companies.[107] U.S.-based DTC companies such as Amazon,

---

[102] Kuner, *supra* note 1, at 23, n. 91.

[103] CIPL Comments, *supra* note 87, at 20.

[104] *See* U.S. Department of Commerce International Trade Association, *European Union – Data Privacy and Protection*, PRIVACY SHIELD, https://www.privacyshield.gov/article?id=European-Union-Data-Privatization-and-Protection (last visited Aug. 20, 2021).

[105] *Id.* ("The legal environment for data transfers to the United States continues to evolve. Companies that transfer EU citizen data to the United States as part of a commercial transaction should consult with an attorney, who specializes in EU data privacy law, to determine what options may be available for a transaction").

[106] *See* Kuner, *supra* note 1, at 25. ("Data transfer rules also provide more enforcement possibilities than an extraterritorial application of the GDPR, since many transfer rules can be enforced against the data exporter in the EU").

[107] *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing before the U.S. S. Comm. On Commerce, Sci. and Transp.*, 116th Cong. 3

Casper, Cuyana, Facebook, Glossier, Harry's, and JustFab continued to certify to the framework[108] until its demise on July 16, 2020.[109]

IV. THE STATE OF INTERNATIONAL TRANSFERS AFTER *SCHREMS II*

After digesting the news that the EU-U.S. Privacy Shield framework had been invalidated by the CJEU in their judgment widely referred to as *Schrems II*,[110] I thought of the scene in *Game of Thrones* (GOT) where Sansa and Jon share a knowing chuckle as snow gently falls around them:

> Sansa: "Winter is here."
>
> Jon: "Well, Father always promised, didn't he?"[111]

As a GOT fan and Stark loyalist, "winter is coming" are my house words. Ned Stark may have lost his head, but he knew what he was talking about—you need to expect and prepare for the worst at all times.[112] As such, privacy practitioners were generally unsurprised that the Privacy Shield framework was short-lived since there had been rumblings of its impending doom since its inception.

Nonetheless, the Court's judgment was sweeping in its scope, going beyond the CJEU Advocate General's non-binding opinion that had encouraged the CJEU to focus solely on the SCCs rather than the Privacy Shield.[113] In one fell swoop, the CJEU declared European Commission Decision 2016/1250 (the "Privacy Shield Decision") invalid and the SCCs suspect.[114] The Court acknowledged that although:

> [t]he Commission found, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield, the latter being comprised, inter alia, under Article 1(2) of that

(Dec. 9, 2020) (Statement of James M. Sullivan, Deputy Assistant Sec'y for Servs., Int'l Trade Admin, U.S. Dep't of Commerce), https://ogc.commerce.gov/sites/default/files/media/files/2021/2020-12-09_eu-us_privacy_shield_james_sullivan_testmony.pdf [hereinafter Sullivan Testimony].

[108] U.S. DEP'T OF COM. INT'L TRADE ASS'N, *Privacy Shield List*, PRIVACY SHIELD, https://www.privacyshield.gov/list (last visited Aug. 20, 2021).

[109] *See* Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559 (Jul. 16, 2020) [hereinafter *Schrems II*].

[110] *Id*.

[111] *Game of Thrones: The Winds of Winter* (HBO television broadcast June 26, 2016).

[112] On reflection, I think Ned Stark would have been a better privacy and data protection lawyer than he was Lord.

[113] *Data Prot. Comm'r v. Facebook Ireland Ltd, Maximillian Schrems*, Opinion of Advocate Gen. Saugmandsgaard ECLI:EU:C:2019:1145 (Dec. 19, 2019).

[114] *See Schrems II, supra* note 109.

> decision, of the Principles issued by the US Department of Commerce on 7 July 2016 as set out in Annex II to the decision and the official representations and commitments contained in the documents listed in Annexes I and III to VII to that decision.[115]

In short, the CJEU determined that what was intended to be a narrow exception to permit the limitation of the Privacy Shield principles "to the extent necessary to meet national security, public interest, or law enforcement requirements," was in practice a broad loophole that undermined the integrity of the entire framework.[116]

A. International Transfers and Available Safeguards in Light of Schrems II

Frustratingly, the Court did not expressly address the question of whether the Privacy Shield framework even applied to Facebook Inc.'s post-GDPR processing of Max Schrems' personal data in the first place. That is, although the Court described that "[s]ome or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing,"[117] it did not definitively state whether the Court viewed this act of transfer and processing constituted an "international transfer" by Facebook Ireland to Facebook Inc. under Article 44 of the GDPR, a processing by Facebook Inc. in the context of the activities of the establishment of Facebook Ireland in the Union under Article 3.1 of the GDPR, or a direct collection by Facebook Inc. under Article 3.2 of the GDPR.

Using the same logic as applied to *Schrems I*, one could assume that the Court's invalidation of the Privacy Shield as a transfer safeguard mechanism presupposes that an international transfer was taking place under the GDPR, as it was under the Directive. That is, the fact of *Schrems II's* existence suggests a geographic definition of international transfers. Under this geographic definition, U.S.-based DTC companies receiving personal data from the EU are forced to go back to square one of Chapter V of the GDPR, under which international transfers to the U.S. may occur pursuant to one of the following familiar safeguards: (a) a legally binding and enforceable instrument between public authorities or bodies;[118] (b) binding corporate

---

[115] *Id.* at ¶ 163.

[116] U.S. DEP'T OF COMM. INT'L TRADE ASS'N, *EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, PRIVACY SHIELD, ¶ I.5(a) https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg (last visited Aug. 20, 2021).

[117] *Schrems II, supra* note 109, at ¶ 51.

[118] Regulation (EU) 2016/679, *supra* note 51 at Art. 46.2(a).

rules;[119] (c) our old friend, the SCCs;[120] (d) other standard data protection clauses adopted by an EU supervisory authority and approved by the European Commission;[121] (e) an approved code of conduct;[122] or (f) an approved certification mechanism.[123]

Unfortunately for all U.S.-based organizations, options (a), (d), & (e) are immediately off the table, as to date, there is no treaty or other "legally binding and enforceable instrument" between the United States and the European Union with regard to data transfers, nor has the European Commission approved other standard data protection clauses or approved a code of conduct. Of course, option (f) would be the dearly departed Privacy Shield and Safe Harbor frameworks.

Option (b), BCRs are a viable path for multinational companies with years to wait and legal fees to burn. But the process surrounding BCRs is opaque, and there is no publicly available information regarding the average cost and time to complete the process of application and approval. However, it is telling that in the three years since the GDPR became effective, only seven companies have been approved by the EDPB,[124] and under the Directive, only 133 companies were ever approved for BCRs.[125] Among these two hundred total companies, nary a U.S.-based DTC company can be found.

That leaves U.S. DTC companies to consider option (c), the SCCs, which may still be acceptable under *Schrems II*, but may require the "adoption of supplementary measures by the controller in order to ensure compliance with" the level of protection required under EU law.[126] In the immediate wake of *Schrems II*, the SCCs that had been implemented under the Directive (let's call them the old SCCs) assumed that the company has one entity located in the EU to act as the data exporter and another separate entity located in an inadequate country, in this case, the United States, to act as the data importer. These two entities can be affiliates of the same corporate group or they can be two distinct businesses, but at the end of the day, it takes two to tango and to contract.

This means that when *Schrems II* was decided, the old SCCs were not appropriate for U.S.-based companies who: (1) act as a data controller, but

---

[119] *Id.* at art. 46.2(b).

[120] *Id.* at art. 46.2(c).

[121] *Id.* at art. 46.2(d).

[122] *Id.* at art. 46.2(e).

[123] *Id.* at art. 46.2(f).

[124] EUR. COMM. EUR. DATA PROTECTION BD., *Approved Binding Corporate Rules under the GDPR*, https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en (last visited Aug. 20, 2021).

[125] EUR. COMM. EUR. DATA PROTECTION BD., *List of companies for which the EU BCR cooperation procedure is closed*, https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50116 (last visited Jul. 1, 2022).

[126] *Schrems II*, *supra* note 109, at ¶ 133.

(2) do not have an "establishment in the Union" to act as a data exporter, and (3) do not have a third party co-controller in the Union to act as the data exporter, but (4) who are subject to the GDPR pursuant to Article 3(2) because they offer goods or services to data subjects in the Union. In short, they were not appropriate for many U.S.-based DTC companies who had been Privacy Shield-certified.

This is precisely why the Privacy Shield (and Safe Harbor before it) were so valuable; they gave over five thousand small to midsize companies a way to legally serve European customers without having to establish a separate presence in the EEA.[127] Rather, under the GDPR, these companies were merely required to designate a representative in the Union under Article 27 as a way "to compensate for the difficulty of legal enforcement of the GDPR against non-EU data controllers and processors."[128] One consequence of the invalidation of the Privacy Shield is that these companies need to establish an entity in the EEA for the mere purpose of having a data exporter avail themselves of the SCCs. This is bizarre, to say the least because it goes far beyond the actual language and apparent intent of the GDPR.

B. Derogations for Specific Situations in Light of Schrems II

Assuming that an international transfer is taking place, there is one last possible mechanism for permitted transfers under the GDPR in light of *Schrems II*—reliance on one of the very limited "derogations for specific situations," where the transfer is based on: (i) the consent of the data subject;[129] (ii) the performance of a contract;[130] (iii) public interest, the vital interest of an individual, or a public register;[131] or (iv) the establishment, exercise or defense of legal claims.[132] In contrast to the safeguards of Article 46, reliance on a derogation is an admission that there is no safeguard but that the transfer will be made nonetheless. This is obviously not a preferable outcome, and as such, the derogations must be narrowly interpreted and applied.[133]

Per the EDPB, in their guidance on derogations that were released just days after the effective date of the GDPR, any consent must be "specifically given for the particular data transfer or set of transfers."[134] Article 49 (1)(a)

---

[127] SOLOVE AND SCHWARTZ, *supra* note 36 at 1267. ("Over 5,300 U.S. companies joined this agreement before the CJEU invalidated it in its *Schrems II* decision on July 16, 2020.")

[128] Kuner, *supra* note 1, at 12.

[129] Regulation (EU) 2016/679, *supra* note 51, art. 49.1(a).

[130] *Id.* at art. 49.1(b) & (c).

[131] *Id.* at art. 49.1(d), (f), & (g).

[132] *Id.* at art. 49.1(e).

[133] European Commission European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* (May 25, 2018), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf [*hereinafter* EDPB Derogations Guidelines].

[134] *Id* at 7.

also requires that the data exporter inform the data subject "of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards."[135] However, the EDPB notes that it "is sometimes impossible to obtain the data subject's prior consent for a future transfer at the time of the collection of the data, e.g., if the occurrence and specific circumstances of a transfer are not known at the time consent is requested, then the impact on the data subject cannot be assessed."[136] Lastly, where there is any processing that is based on consent, it must be as easy to withdraw as to give consent.[137] Thus, by the EDPB's own admission, "the GDPR sets a high threshold for the use [of] the derogation of consent. This high threshold, combined with the fact that the consent provided by a data subject can be withdrawn at any time, means that consent might prove not to be a feasible long-term solution for transfers to third countries."[138]

We also know that the derogations for performance of a contract are only applicable if the transfers are "not repetitive" and concern "only a limited number of data subjects."[139] The examples given are for one-time transfers relating to a specific individual or set of individuals. This does not reflect the situation of most Direct-to-Consumer e-commerce companies who are making continuous transfers in order to serve EEA consumers *en masse*.

Furthermore, the transfers must also be "necessary" under this derogation.[140] However, necessity will be interpreted very narrowly and requires a "close and substantial connection" between the data transfer and the purposes of the contract.[141] Business advantage or preference alone does not seem to be sufficient: "This derogation cannot be used for example when a corporate group has, for business purposes, centralized its payment and human resources management functions for all its staff in a third country as there is no direct and objective link between the performance of the employment contract and such transfer."[142] In light of the EDPB's guidance, it appears that almost nothing other than geographic necessity (e.g., travel to another country) would constitute a necessity.

In short, the derogations are to be used as an exceptional surgical instrument and not as an everyday tool.

C. Interim EDPB Guidance After Schrems II

Just one week after the CJEU's decision, the EDPB issued its initial

---

[135] Regulation (EU) 2016/679, *supra* note 51, art. 49(1)(a).
[136] EDPB Derogations Guidelines, *supra* note 133, at 7.
[137] Regulation (EU) 2016/679, *supra* note 51, art. 7(3).
[138] EDPB Derogations Guidelines, *supra* note 133, at 8.
[139] *Id.* at 4.
[140] *Id.* at 8.
[141] *Id.*
[142] *Id.*

guidance on the *Schrems II* world of data transfers.[143] This guidance was helpful for companies already using SCCs since the EDPB made "clear data could continue to flow, including to the United States, so long as companies adopted supplementary measures to ensure adequate protection."[144] However, this was cold, inapplicable comfort for DTC companies that had relied on Privacy Shield as their basis for the transfer, as the FAQs confirmed the limited use of derogations.[145] The EDPB also declined to offer guidance on whether it took a jurisdictional or geographic view of international transfers and the Irish Data Protection Commissioner declined to respond to related questions via chat during an online speaking engagement.[146]

Four months later, in November of 2020, the EDPB issued a draft recommendation on measures to supplement data transfer rules under the GDPR and new draft SCCs.[147] This guidance again focused on the SCCs and the inclusion of contractual, technical or organizational supplementary measures if there are impediments (such as government surveillance) to the effectiveness of the SCCs. If supplementary measures cannot be taken and impediments remain, the transfers should be suspended.[148] This guidance gave privacy practitioners ample material for speculation regarding how European exporters should assess potential impediments when using the SCCs.[149] It also gave European regulators ample material for beginning

---

[143] EUR. COMM. EUR. DATA PROTECTION BD., *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Jul. 23, 2020), https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf.

[144] Caitlin Fennessy, *'Schrems II' DPA investigations and enforcement: Lessons learned*, IAPP THE PRIVACY ADVISOR (Jun. 17,2021), https://iapp.org/news/a/schrems-ii-dpa-investigations-and-enforcement-lessons-learned/?mkt_tok=MTM4LUVaTS0wNDIAAAF9ugtYwxh1drLdKfWBVwITnqSHb-Z6iC5D_Z9fY_4B0PwzZCwuyq_RJy5Snb3TH5MX2JQ8PXFTAw0BG0Fh8t56lzZsm-dvSv4Csgg_-q50qf60.

[145] *Id*.

[146] IAPP Linkedin Live Event, *The CJEU Decision Unpacked: DPC v. Facebook Ireland, Schrems* (Jul. 17, 2021), https://www.linkedin.com/video/live/urn:li:ugcPost:6689936710362558464/. Panelists, including Irish Data Protection Commissioner Helen Dixon, did not respond to questions from virtual attendees regarding safeguards for U.S.-based companies who cannot rely on SCCs.

[147] EUR. COMM. EUR. DATA PROTECTION BD., *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (Nov. 10, 2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf [hereinafter EDPB Supplementary Measures Guidelines].

[148] *Id.*

[149] Gary Weingarden & Matthias Artzt, *Demystifying data transfers to US data importers: Looking at 'Schrems II' from a different angle*, IAPP THE PRIVACY ADVISOR (May 25, 2021), https://iapp.org/news/a/demystifying-data-transfers-to-us-data-importers-looking-at-schrems-ii-from-a-different-angle/?mkt_tok=MTM4LUVaTS0wNDIAAAF9cc7U9q420PjvgxLWOGFTr13lKUHnXDVwBgqGZUqroM4tMWcOAPFIBGvVm3_9--avfBecy-YijUgmkNnzWngSLH0zrDDqy1xm4ZJOJ7F_Um9D.

enforcement proceedings against companies that failed to assess potential impediments when using the SCCs, though their approaches have been inconsistent.[150]

As Caitlin Fennessy of the International Association of Privacy Professionals (IAPP) explains:

> Supervisory authorities, with sometimes divergent interpretations of a challenging CJEU decision, began to enforce its provisions. The proactive and complaint-driven investigations related to public statements and enforcement actions sent privacy professionals as well as EU and U.S. diplomats scrambling yet again. EU supervisory authorities' actions and statements have raised a host of concerns regarding organizations' post-"Schrems II" response. These range from simply suggesting there is an inherent need to investigate companies' data transfers, particularly to the United States, to finding fault with companies' failure to assess transfers, to adopt any supplementary safeguards at times even when U.S. service providers localize data processing in the EU. Each one of these actions adds to companies' uncertainty regarding compliance options, their wariness concerning data transfers and their demands for a government-led solution.[151]

This uncertainty and wariness were compounded for U.S.-based DTC companies, as the EDPB once again refused the call[152] to address the interplay between Article 3.2 and Chapter V. Step one of the draft guidelines may be to "know your transfers," but it is hard, if not impossible, to be "fully aware of your transfers" without having a clear definition of what constitutes a transfer in the first place.[153] With this in mind, I would disagree with Christopher Kuner's assertion that "[t]here is little evidence about whether the co-existence of territorial scope and data transfer rules actually presents problems."[154] I believe the lack of a valid transfer safeguard mechanism for U.S.-based DTC companies is evidence in itself, particularly where these companies cannot be certain if a restricted transfer is even occurring. For

---

[150] *See* the action by the Bavarian data protection authority where it suspended a German exporter's use of U.S. based Mailchimp due to a failure by the controller to assess the transfers being made to the U.S. via Mailchimp. BayLfD, LDA-1085.1-12159/20-IDV (Mar. 15, 2021), https://gdprhub.eu/index.php?title=BayLDA_-_LDA-1085.1-12159/20-IDV.

[151] Fennessy, *supra* note 144.

[152] *Game of Thrones: The Winds of Winter*, *supra* note 111. (Lyanna Mormont: "Your son was butchered at the Red Wedding, Lord Manderly, but you refused the call. You swore allegiance to House Stark, Lord Glover, but in their hour of greatest need, you refused the call. And you, Lord Cerwyn, your father was skinned alive by Ramsay Bolton. Still, you refused the call. But House Mormont remembers. The North remembers. We know no king but the King in the North whose name is Stark. I don't care if he's a bastard. Ned Stark's blood runs through his veins. He's my king from this day until his last day").

[153] EDPB Supplementary Measures Guidelines, *supra* note 147, at 8 ("The first step is to ensure that you are fully aware of your transfers. Know your transfers").

[154] Kuner, *supra* note 1, at 21.

these companies, the issue is not so much the conflict between territorial rules and data transfer rules (because they should be treating the personal data in accordance with the GDPR either way); the issue is the threat of a supervisory authority alleging that they have transferred personal data without a legal basis for which to do so.

D. Final EDPB Guidance and New SCCs

Unfortunately, the European Commission has continued to kick the proverbial can down the road by failing to define international transfer, even as it published new SCCs and a final implementing decision on June 4, 2021.[155] In contrast to the old SCCs, the new SCCs are designed for use by data exporters subject to the GDPR under both Articles 3(1) and 3(2).[156] However, the implementing decision merely acknowledges the tension between Article 3(2) and Chapter V. Nonetheless, it does not clarify whether "international transfer" refers to a geographic transfer outside the European Economic Area or to a legal transfer outside the jurisdiction of the GDPR.[157] In fact, the implementing decision only further confuses the EDPB's position on the matter and how U.S.-based DTC companies may use the new SCCs in lieu of Privacy Shield.

The primary source of confusion is the first sentence of Recital Seven, which reads as follows: "A controller or processor may use the standard contractual clauses . . . for the transfer of personal data to a processor or controller established in a third country, without prejudice to the interpretation of the notion of international transfer in Regulation (EU)

---

[155] European Commission Press Release IP/21/2857, European Commission adopts new tools for safe exchanges of personal data (Jun. 4, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847?mkt_tok=MTM4LUVaTS0wNDIAAAF9dvKSLGXYALNrW9exH1JWC-mfoyq44LSftDUmzx2H59VIbpLWuDOg4XDTdQySYvvxCb5lW2NfTEFmvHWGc9soXzPLu592-gOeOwxzXEcIOqsl.

[156] *See* European Commission European Data Protection Board, *Standard Contractual Clauses (SCC)* (June 4, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en ("On 4 June 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR)."). *See also* Commission Implementing Decision (EU) 2021/914 of 4 June 2021, on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, (O.J. (L 199/31) 13, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en [*hereinafter* SCC Implementing Decision] ("[w]here the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2)").

[157] Joseph Duball, *Getting Acclimated with Updated SCCs,* IAPP THE PRIVACY ADVISOR (June 16, 2021), https://iapp.org/news/a/getting-acclimated-with-updated-sccs/?mkt_tok=MTM4LUVaTS0wNDIAAAF9tMhWpcbyVME5B6wU1wtjAvnb0P4Al0FPTpFv_kwE0fEsrf0n4TLwYH3gpw5oCapGbi8VP24xHUaFwPRoI_CS7x-T9SFLnknUMcmsBi4lumH8.

2016/679."[158] The structure of the sentence alone suggests that the EDPB reserves the right to define an international transfer in the jurisdictional as opposed to geographic sense. To paraphrase, they seem to be saying, "your use of the SCCs as a safeguard does not mean we concede that an international transfer is actually taking place." This is a strange thing to say, as a safeguard would only be necessary if there was an international transfer taking place. However, if the EDPB agreed on a geographic definition, they would not need to reserve the right to take a later contrary view. Recital Seven of the implementing decision continues:

> The standard contractual clauses may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679. This also includes the transfer of personal data by a controller or processor not established in the Union, to the extent that the processing is subject to Regulation (EU) 2016/679 (pursuant to Article 3(2) thereof) because it relates to the offering of goods or services to data subjects in the Union or the monitoring of their behaviour as far as it takes place within the Union.[159]

In layman's terms, Recital Seven precludes the use of SCCs where the processing by the importer already falls within the scope of the GDPR. This would exclude the use of SCCs for intracompany transfers where a foreign legal entity is collecting EU personal data and storing it on its servers owned and operated by that same legal entity in that foreign country (the U.S.-based DTC company example). It would also exclude the use of SCCs for intercompany transfers from a corporate group's EU-based legal entity that is subject to the GDPR under Article 3(1) to a foreign-based legal entity that is also subject to the GDRP (the situation of Facebook in *Schrems I & II*). However, it also may exclude the use of SCCs by a foreign-based exporter that is subject to the GDPR under Article 3(2) and its foreign-based service-provider/importer that is also subject to the GDPR under Article 3(2).

Others have noted that the logic here appears to be that "the objective of the SCCs is to ensure that exported data is processed to a standard that is essentially equivalent with the GDPR, and if the data importer's processing is already subject to the GDPR then the SCCs are redundant in this context."[160] This logic, of course, leads us to a jurisdictional definition where an international transfer is not even occurring in the above scenarios. This would be supported by the CIPL's argument that:

---

[158] SCC Implementing Decision, *supra* note 156.

[159] *Id.*

[160] Phillip Lee*, The Updated Standard Contractual Clauses – A New Hope?*, IAPP THE PRIVACY ADVISOR (June 7, 2021), https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/?mkt_tok=MTM4LUVaTS0wNDIAAAF9ho57U4QkZATMc91Tszlzxn7ziNEN8wiQAKnTyYci4YEHEvTA-SSeuuMbwnTmZEuJ-3P3bs5gjBuZgTeg8J5OQfI1geTmeGyFnatOtbZRfrr2.

> an accumulation of the obligations under Article 3(2) of the GDPR and Chapter V of the GDPR would not make sense. An organisation acting within the scope of Article 3(2) must put in place all the measures and safeguards of the GDPR. There is no added value in requiring this organisation to additionally comply with the obligations of Articles 46, 47, and 49 of the GDPR because the organisation is already bound by all obligations stemming from these latter provisions.[161]

Unfortunately, the EDPB's implementing decision is strictly limited to the new SCCs and does not reference the applicability of other Article 46 safeguards to companies subject to the GDPR under Article 3(2).

Aside from Recital Seven, Recital Six supports a jurisdictional view of international transfer. That Recital sets forth a variety of "significant developments" in the digital economy that prompted the EDPB to modernize the new SCCs.[162] This would have been the ideal place for the EDPB to mention that the digital economy has also made it much easier for foreign e-commerce companies to directly collect personal data from EU consumers rather than through an EU-based intermediary. In fact, a DTC scenario is a much more likely scenario for international transfer than a scenario in which a foreign e-commerce company establishes a complex and unnecessary chain of processing in order to serve EU consumers. However, Recital Six does not mention direct collection at all; perhaps its omission is an indication that some members of the EDPB feel the DTC scenario is not an international transfer at all?

V. U.S. DTC COMPANIES: STUCK BETWEEN A GEOGRAPHIC WALL AND A JURISDICTIONAL MOUNTAIN

A. Can Anything Be "Right"?

In its press release announcing the new SCCs, the EDPB describes how they offer "more legal predictability to European businesses . . . to ensure compliance with requirements for safe data transfers."[163] This predictability, however, does not extend to non-EU businesses that are subject to the GDPR under Article 3(2). Rather, they are still faced with the unanswered question of whether their processing of EU data constitutes a transfer in the first place; if a geographic definition is taken, it does constitute a transfer, but if a jurisdictional definition is taken, it does not.

Thus far, I have made a case for a jurisdictional definition. Yet, as Ruth

---

[161] CIPL Comments, *supra* note 87, at 19.

[162] SCC Implementing Decision, *supra* note 156 ("[m]oreover, since the decisions were adopted, the digital economy has seen significant developments, with the widespread use of new and more complex processing operations often involving multiple data importers and exporters, long and complex processing chains, and evolving business relationships").

[163] European Commission Press Release IP/21/2857, *supra* note 155.

Boardman has eloquently pointed out, defining "international transfer" in this jurisdictional way would have the "somewhat mind-blowing effect that the "Schrems II" case invalidated (the EU-U.S. Privacy Shield) for processing that was not even an international transfer. I don't think that can be right."[164] Her logic on this point is sound, and I am not inclined to disagree with her. Ms. Boardman is a privacy rock star and far smarter than me. I would, however, argue that the EDPB, CJEU, and individual Member State supervisory authorities have complicated the issue of international transfers to a point where almost nothing can be right.

For instance, taking a geographic rather than jurisdictional notion of international transfer would mean that there is now a broad category of international transfers that are acknowledged by European privacy regulators but for which there is no appropriate safeguard or derogation. Are we to infer that these transfers are now entirely prohibited? *This* does not seem right.

However, taking the jurisdictional notion would mean that no safeguards or supplementary measures are required to collect personal data by a U.S.-based DTC company that is directly subject to the GDPR under Article 3(2). This is in contrast to a scenario where safeguards *and* supplementary measures would be required if that same U.S.-based company had formed a European legal entity to act as its data exporter and GDPR-heat shield. Sensing the danger of this view, IAPP contributors have pointed out that as a consequence of Recital Seven of the EDPB's implementing decision for the new SCCs, "[s]ome companies working outside the EU but still subject to the GDPR via their EU establishment may see Recital 7 as a reason to skip a transfer mechanism altogether, regardless of their third-country status."[165]

Still, flipping back to a geographic notion forces us to compound Chapter V on top of Article 3(2), turning Chapter V into a "regime of general application, to all non-EU controllers and processors subject to Art 3.2."[166] Could it be the Commission's intent to embrace the result feared by the *Lindqvist* Court in 2003?[167] After all, the European Data Protection Supervisor, in its *Case Law Digest* has stated:

---

[164] Duball, *supra* note 157.

[165] *Id.*

[166] Robert Madge, *GDPR's Global Scope: The Long Story,* MEDIUM (May 12, 2018), https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f.

[167] *Lindqvist*, *supra* note 79, ¶ 69 ("If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of the Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.").

> These data flows (transfers and onward transfers) are subject to the rules set out in Chapter V of the GDPR, as well as to all rules and principles of the GDPR, notably the principles under Article 5 (lawfulness, fairness, and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability).[168]

Christopher Kuner argues in favor of this, stating, "Since the GDPR does not contain any provision regulating the interaction between territorial scope and data transfer rules, either explicitly or implicitly, both sets of rules apply when the conditions for their application are triggered, meaning that they may apply simultaneously in some cases."[169]

However, one needs to consider whether a regime of general application (and the geographic definition of international transfer that creates it) is an impossible "legal fiction, since by their nature parts of the GDPR were not designed to apply outside the EU" (for example, Articles 36 & 58)?[170] Furthermore, Article 3(2) only sweeps-in those companies that target goods and services to EU consumers, while Chapter V applies to all personal data collected from the EU; could it really be the EDPB's intent to stretch the long arm of European privacy law to Mr. Fantastic proportions by covering *any and all* processing of EU data by non-EU controllers?[171] I am not the only one begging for clarity on these questions.[172]

B. The Consequence of "Wrong"

The current state of international transfers is perplexing for anyone who dabbles in privacy, but particularly for those of us who consider ourselves pragmatic privacy lawyers (no, that's not an oxymoron). Clients need real answers to overcome their real problems, not a thirty-page exploration of the problem (these thirty pages are for my fellow privacy nerds). However, the past year has pushed even the most practical practitioners to the brink of esotericism.

Prior to the *Schrems II* decision, privacy lawyers may have been tempted to dismiss this entire issue as an academic frivolity. One could bypass the question of whether an international transfer was occurring and simply self-certify under the Privacy Shield framework as a prophylactic measure. Indeed, the sheer number of self-certifications indicates that many companies did just that. However, in a *Schrems II* world, these companies are left with a conundrum. Should they concede that they had always believed

---

[168] EUR. DATA PROTECTION SUPERVISOR, EDPS CASE LAW DIGEST: TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES, 2 (Nov. 10, 2020), https://edps.europa.eu/system/files/2021-06/21-06-09_case-law-digest_en.pdf.

[169] Kuner, *supra* note 1, at 16.

[170] *Id.* at 25.

[171] Madge, *supra* note 166.

[172] Lee, *supra* note 160.

in a geographic notion where an international transfer was taking place under the GDPR, and thus, a replacement safeguard would be required after the invalidation of Privacy Shield? Or should they now boldly assert a jurisdictional notion, where their Privacy Shield self-certification was a big misunderstanding and no international transfer has ever taken place under the GDPR? Neither of these answers puts DTC companies in a favorable regulatory light. Furthermore, it is not clear which of these answers is the "right" one in the eyes of the EDPB.

Of course, the most compliant path forward would be for U.S. DTC companies to avoid collecting EU personal data in the first place. I will admit, at times, I have wondered if that might be the EDPB's desired effect. But, short of an explicit declaration that they may not serve EU customers, most U.S. DTC companies will continue to do so. Some U.S.-based companies who act as processors rather than controllers, like Microsoft, have transitioned to solutions that store and process EU cloud customer data within the EU. [173] However, while a company with a large EU presence and billion-dollar market cap such as Microsoft can afford to do this, the average U.S. DTC company cannot. In addition, a DTC company acts as a data controller rather than the processor, and thus, merely storing the data within the EU will not prevent a transfer if it is also being accessed and processed from the U.S.

The reality is that post-*Schrems II*, United States based DTC companies are continuing to directly collect and process European personal data exactly as they were before the invalidation of the Privacy Shield. While the safeguards may have changed, the business operations have not. These companies are aware that their collection may be in contravention of Chapter V of the GDPR, but they have no choice, as ceasing to do business is really no choice at all. Data transfer issues are big enough to cause public companies to file Form 10-K disclosures with the U.S. Securities and Exchange Commission regarding risks over the legality of their transfers and the impact of a regulator ceasing those transfers.[174]

---

[173] Brad Smith, *Answering Europe's Call: Storing and Processing EU Data in the EU,* MICROSOFT EU POL'Y BLOG (May 6, 2021), https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary.

[174] "As the two sides of the Atlantic alliance move out of sync, companies are paying a price. Securities and Exchange Commission filings from dozens of different businesses filed this year say the ongoing confusion over the legality of U.S.-EU data transfer may hurt finances, operations and service offerings overseas." Gold, *supra* note 2. "But now that corporate anxiety is being reflected in earnings reports with the Securities and Exchange Commission, according to a Morning Consult analysis of all SEC filings from publicly traded companies in 2020. Companies outside of the tech sector—like shopping channel QVC and ViacomCBS Inc.—have begun adding warnings to their investors about the possible revenue hit the court decision and continued discussions about a replacement deal could have on their businesses." Sam Sabin, *As Officials Hash Out Deal to Replace Privacy Shield, More Companies — Beyond Tech — Warn Investors About the Risk*, MORNING CONSULT (Apr. 20, 2021), https://morningconsult.com/2021/04/20/privacy-shield-compliance-sec-filings.

Vera Jourová, the EDPB's Vice-President for Values and Transparency, has asserted that the new SCCs were a "needed solution in the interconnected digital world where transferring data takes a click or two."[175] She is correct, but this is all the more reason that the EDPB should not continue to ignore the international transfer question, as the question of what constitutes an international transfer must be answered before we ask the question of how to safeguard the transfer.

VI. FORTHCOMING EDPB GUIDANCE ON INTERNATIONAL TRANSFERS: A DREAM OF SPRING?[176]

It is rumored that the EDPB will finally answer both of these questions in a forthcoming opinion entitled *Territorial scope (Article 3) of the GDPR and its interplay with Chapter V*.[177] Unfortunately for the EDPB, what might have been a simple, clear-cut opinion in 2018, before the invalidation of Privacy Shield, will now almost certainly be a complex untangling of the contradictions exposed in this paper. We've all been told by our mothers that two wrongs can't make a right, but the EDPB must now make two wrong notions of international transfer into a right one. In order to do this, the EDPB must reconcile the following in any opinion it issues:

- The expanded territory of European privacy law under Article 3(2) of the GDPR;
- The continued restrictions on international transfers in Chapter V of the GDPR;

---

[175] European Commission Press Release IP/21/2857, *supra* note 155.

[176] The HBO series *Game of Thrones* is based on the book series, *A Song of Ice and Fire* by George R.R. Martin. Martin published the first five volumes between 1996 and 2011 which contain various loose threads and cliff-hangers. Martin began work on the sixth installment, to be called *The Winds of Winter*, in 2010. In 2006, he had announced the title of the seventh and final installment, *A Dream of Spring*. However, it appears he has not yet begun to write this novel and the HBO series began to surpass the book series in season five. As a result, seasons six, seven, and eight of the show are just not that good (at least when compared to the first five seasons). That said, I have empathy for the show's writers and showrunners who struggled to translate Martin's notes and hints at what the last two books will contain, much as I have empathy for the EDPB which has struggled to translate the CJEU's and EU Parliament's notes and hints at how international transfer should be defined. Writing someone else's story for them is hard. GOT geeks like myself still hope that *A Dream of Spring* will deliver the satisfying resolution that the TV series failed to deliver.

[177] Ruth Boardman, Ariane Mole, & Gabriel Voisin, *Replacement Standard Contractual Clauses (SCCs): European Commission Publishes Final Text*, BIRD & BIRD NEWS CENTRE (June 2021), https://www.twobirds.com/en/news/articles/2021/uk/replacement-standard-contractual-clauses?mkt_tok=MTM4LUVaTS0wNDIAAAF9i47Vr8xiLFjmYhCKp5sPA3AJDQvkruy335276NlsX8e7iLcpCar_NveRYeRojfk_4Flj4nxIRS86QawGfi4LERsHQGoYXMuoPuK1WzyXJNum ("[t]he EDPB is currently considering the point and this is likely to be addressed in an upcoming opinion entitled 'Territorial scope (Article 3) of the GDPR and its interplay with Chapter V'").

- The continued use of Privacy Shield by companies who were clearly making international transfers under the Directive but may not be doing so under the GDPR;
- The CJEU's *Schrems II* opinion that suggests a geographic definition of international transfers;
- The United Kingdom's ICO's guidance (and unpublished draft EDPB guidance) that suggests a jurisdictional definition of international transfers; and
- The EDPB's own implementing decision for the new SCCs and the new SCCs themselves which suggest a geographic definition at one turn and a jurisdictional definition at the next.

This is no easy task, but then again, almost nothing related to global privacy and data protection is "easy." Indeed, difficult tasks are often those most in need of doing. The members of the EDPB certainly have the intellect to assess the above issues and draft an opinion that offers clear and practical guidance. The question is whether the twenty-seven EU Member States will be able to agree on the substance of what that guidance should be. It appears they may be close to an agreement, as the first substantive item of the minutes from their plenary meeting on September 14, 2021 is "[ITS ESG] Guidelines on the interplay between Art. 3 and Chapter V – discussion."[178] At four sentences, the item description is brief, but revealing:

> The lead rapporteur shared information about the state of play and the progress of the discussions on the draft guidelines on the interplay between Article 3 and Chapter V GDPR. During their discussion the EDPB members highlighted the importance of this work and exchanged their views on the notion of a transfer, the relevant criteria to define this notion and examples to be included in the draft guidelines. They underlined the importance to quickly finalise those guidelines. The EU COM confirmed, that, after the draft guidelines are adopted, they intend to develop a specific set of SCCs regarding transfers to importers subject to Article 3(2) GDPR.[179]

The first three sentences are both comforting and frustrating; they show that the EDPB is aware of the urgency of resolving the notion of a transfer while confirming that the EDPB members hold differing views on that notion. However, the fourth and final sentence is the most telling. Upon an

[178] European Commission European Data Protection Board, *Minutes, 54th Plenary Meeting* (Sep. 14, 2021) 2, https://edpb.europa.eu/system/files/2021-10/20210914plenfinalminutes_54thplenary_public.pdf [hereinafter EDPB 54th Plenary Meeting Minutes].

[179] EDPB 54th Plenary Meeting Minutes, *supra* note 178.

initial reading, I wondered, "could this be our Azor Ahai?"[180], as this sentence seems to confirm a geographic notion of international transfer. Although I believe a jurisdictional notion better aligns with the text and spirit of the GDPR, at this point clarity either way would be welcome.

However, as Tyrion Lannister has noted, "[p]rophecy is like a half-trained mule . . . . It looks as though it might be useful but the moment you trust in it, it kicks you in the head."[181] Indeed, this fourth sentence only partially addresses the conundrum of Recital Seven of the new SCC implementing decision. As stated above in Section IV.D of this paper, that recital precludes the use of the new SCCs in three EU-to-U.S. scenarios where the processing by the importer already falls within the scope of the GDPR: (1) U.S.-based DTC intracompany-type transfers (i.e., the U.S. legal entity is directly processing EU personal data); (2) intercompany transfers from a corporate group's EU-to-U.S. legal entities; and (3) extra-company transfers from a U.S.-based exporter that are subject to the GDPR under Article 3(2) and their U.S.-based service-provider/importer that is also subject to the GDPR under Article 3(2). The EDPB's development of a "specific set of SCCs regarding transfers to importers subject to Article 3(2) GDPR" only addresses the second and third scenario.[182] With regard to the first, it does not ultimately resolve the question of whether a transfer is occurring for U.S.-based DTC companies because SCCs are unavailable to them (remember, it takes two to both tango and to contract). In that sense, our prince that was promised has not yet arrived and privacy practitioners are left to write their own fanfic on the DTC question.[183]

In my ideal world, the EDPB's opinion would start with an introduction

---

[180] Azor Ahai is a mythical legend in the GOT universe. He wielded a sword called Lightbringer and saved Westeros from a dark ancient period known as the "Long Night." Melisandre and her cadre of prophets believe that Azor Ahai will be reborn in their lifetime as "the prince that was promised" to save Westeros from the Night King and his army of the dead. For seven seasons of the show, we were led to believe that multiple characters including Jon Snow, Daenerys Targaryen, Arya Stark, and even Samwell Tarly may be Azor Ahai reincarnated. For reasons unknown, the showrunners abandoned this prophecy entirely in the final season. Although Arya Stark kills the Night King at Melisandre's urging, we have no indication of whether she, or anyone else, have fulfilled the prophecy of Azor Ahai.

[181] GEORGE R.R. MARTIN, A DANCE WITH DRAGONS loc. 74916 (Bantam Books 2011) (ebook).

[182] EDPB 54th Plenary Meeting Minutes, *supra* note 178.

[183] Indeed, the IAPP has also noted the confusion caused by the plenary meeting minutes, calling them a "change in course" for the European Commission. In addition, while my paper focuses on U.S.-based DTC companies that are subject to the GDPR under Article 3(2), the IAPP notes that it is also unclear how Recital Seven and the minutes of the EDPB meeting apply to situations "when the GDPR applies directly to the data importer based on Article 3(1) GDPR (where a non-EEA controller has establishments in the EU and the data is also processed in the context of the EU establishment)." Lokke Moerel and Alex van der Wolk, *Why it is unlikely the announced supplemental SCCs will materialize*, IAPP PRIVACY PERSPECTIVES (Nov. 4, 2021), https://iapp.org/news/a/why-it-is-unlikely-the-announced-supplemental-sccs-will-materialize.

that recognizes the need for reconciliation of the above points. The EDPB would then solidify a jurisdictional definition of international transfer and clarify that the restrictions imposed by Chapter V of the GDPR are not required for the direct collection of personal data by foreign-based companies that are subject to the GDPR through Article 3(2).

The EDPB might even be so kind as to include an example of the same, along the lines of, for example, where Company X is located solely in the United States, with no establishment in the EU, but Company X accepts orders directly from, and ships goods directly to, customers in the European Union, such processing of EU customers' personal data does not constitute a restricted transfer under Chapter V of the GDPR and does not require any safeguards such as Standard Contractual Clauses or Binding Corporate Rules.

With regard to further processing of that EU customer personal data by service-providers of Company X, the EDPB would ideally also confirm that Chapter V does not apply where the service-provider is already subject to the GDPR. For example, Company X uses the website hosting platform of Service-Provider Y, a U.S.-based company that is also subject to the GDPR through Article 3(2). In this case, the sharing of EU customers' personal data with Service-Provider Y does not constitute a restricted transfer under Chapter V of the GDPR.

Lastly, the EDPB would be clear that although a jurisdictional definition narrows the universe of international transfers and safeguards, it does not result in a degradation of privacy for data subjects. Something like the following would do the trick: The absence of an international transfer by Company X does not relieve Company X (a) of its obligation to ensure the security of processing under Article 32 of the GDPR at all stages of collection, use, transfer, sharing, and disposal, or (b) of its obligations toward the use of processors under Article 28; indeed, Company X may need to implement supplemental measures in order to meet these obligations when personal data is being processed outside of the European Union.

This last point is important because it addresses the core fear of the *Schrems II* Court—that the security guaranteed to EU personal data by the GDPR will be subverted by wanton government surveillance in third countries. Some European supervisory authorities may be clinging to a geographic definition for fear that a jurisdictional one leaves EU personal data vulnerable to this surveillance. However, a jurisdictional definition of international transfer does not preclude the EDPB from requiring foreign-based companies to consider the location in which they store and process European personal data as part of their holistic GDPR compliance strategy, including making security assessments under Article 32. In other words, U.S.-based DTC companies, and other foreign-based companies subject to the GDPR via Article 3(2), would still be responsible for assessing the impact of how and where they collect, transfer, and store EU personal data.

These companies would still be required to evaluate the practices of the

public authorities where personal data is stored in order to determine whether the legislation and/or practices of the host country impinge—in practice—on the effectiveness of the GDPR as a whole and not just on the effectiveness of those transfer tools under Art. 46.[184] More specifically, the EDPB can still offer guidance on the use of encryption and pseudonymization to protect EU personal data from wanton government surveillance. In addition, the EDPB can still require that foreign-based businesses provide EU individuals with recourse for violations of the GDPR. A jurisdictional notion of international transfer *can* be right, if the EDPB opinion is clear, rational, and practical.

Most important, by clarifying a jurisdictional view of international transfers, the EDPB would be directing foreign organizations back to the basics of privacy and data protection under the GDPR. U.S.-based DTC companies have a myriad of obligations under the GDPR, separate and apart from any obligations under Chapter V. Privacy-by-design, data subjects' rights, data minimization, storage limitation, and security are all crucial for protecting the personal data of EU consumers. Yet, the effects of *Schrems II* have dominated the privacy conversation for the past year, perhaps at the expense of other privacy compliance efforts. I would implore the EDPB to consider that when an organization's privacy lawyer devotes time to exploring the uncertainties raised by this paper, that person is not spending that time on core compliance activities like privacy impact assessments.

Furthermore, the current lack of clarity around international transfers encourages U.S.-based DTC companies to take a bureaucratic approach to intercompany data sharing and vendor management by "papering" those interactions with ill-fitted SCCs as a prophylactic measure. In the vendor context, long SCCs are often explained away as boilerplate or compliance requirements, which serves no one. We know that controllers subject to the GDPR under Article 3(2) are required to comply with the GDPR regardless of where and how they process EU personal data. Thus, going round and round in tautological circles of safeguards and supplementary measures are a distraction from the fact that the *Schrems II* judgment "reminds us that the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes."[185] It is hard to see how transfer safeguards under Article 46 of the GDPR ensure that protection better than general compliance with Articles 28 and 32. The EDPB should take this opportunity to refocus the post-*Schrems II* dialogue on core compliance

[184] Press Release, European Data Protection Board, EDPB adopts final version of Recommendations on supplementary measures, letter to EU Institutions on the privacy and data protection aspects of a possible digital euro, and designates three EDPB Members to the ETIAS Fundamental Rights Guidance Board (June 21, 2021), https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en?mkt_tok=MTM4LUVaTS0wNDIAAAF9zoGrYP_-GaSBkmaYFAjHIUGMwAO8Zx8LbRl7SW-YcTuTcJBBcSpfGu-epm1Sh4NsmKPVzyocXBwPkM9whyTc5XuDDcyZjWDTn0AZ4-k_F-Sf.

[185] EDPB Supplementary Measures Guidelines, *supra* note 147, at 2.

activities by foreign-based companies subject to the GDPR under Article 3(2).

CONCLUSION

It is easy for academics and regulators to veer toward the obtuse. However, in the case of international transfers under the GDPR, the practical implications are clear. In his December 2020 testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, Deputy Assistant Secretary for Services James Sullivan testified to the enormous importance of transatlantic data flows to the $5.6 trillion annual value of transatlantic trade.[186] Viewed through this lens, the EDPB risks approximately $15 billion each day that it delays in issuing an opinion on the interplay of Article 3(2) and Chapter VI of the GDPR. In addition to the economic costs of their delay, they risk their own credibility when they refuse to address such a fundamental issue.

In the words of Johannes Caspar, the Hamburg data protection authority, "[a]uthorities have to work fast and effectively to be able to give clearly deterring signs that certain behaviors are not OK. If that doesn't happen, law and reality are at odds."[187] Unless and until the EDPB issues its formal guidance on Article 3(2) and Chapter VI, law and reality will continue to be at odds, and privacy lawyers must continue to dream of Spring.

POSTSCRIPT

Shortly before this paper's publication, the EDPB issued draft guidelines on the interplay between the territorial jurisdiction of the GDPR (Article 3) and the GDPR's provisions on international transfers (Chapter V).[188] To say this is welcome news would be an understatement since my paper entreats the EDPB to do this.[189] Even more welcome is the EDPB's preliminary position that it is not a transfer under Chapter V of the GDPR when a U.S.-based DTC company collects personal data directly from its EU

---

[186] Sullivan Testimony, *supra* note 107 ("[t]he United States and the European Union enjoy a $7.1 trillion economic relationship—with $5.6 trillion in transatlantic trade annually. According to some estimates, nearly $450 billion of this trade involves digital services. In truth—given the ongoing digitization of virtually every industry sector and the fact that cross-border data flows between the U.S. and Europe are the highest in the world—far more of that overall $5.6 trillion in trade is facilitated in some way by cross-border transfers of data.").

[187] Bodoni, *supra* note 95.

[188] EUR. COMM. EUR. DATA PROTECTION BD., *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR,* 5 (Nov. 18, 2021), https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf.

[189] I haven't been this excited since we learned that Jon Snow is not Ned Stark's biological son. *Game of Thrones: The Winds of Winter* (HBO television broadcast June 26, 2016).

customers.[190] The EDPB even kindly provides an example of this scenario that almost exactly matches what I advocate for in Section VI of my paper.[191] I am cautiously optimistic that these positive developments will be maintained in the EDPB's final guidelines. However, it is possible that this draft could substantially change in the months after the public consultation period closes on January 31, 2022. Time will tell; in the meantime, I hope you enjoyed my paper.

[190] "This second criterion cannot be considered as fulfilled where the data are disclosed directly and on his or her own initiative by the data subject to the recipient. In such case, there is no controller or processor sending or making the data available ("exporter")." *Id.*

[191] *See* "Example 1: Controller in a third country collects data directly from a data subject in the EU," featuring an Italian consumer named Maria who purchases a dress from a Singaporean e-commerce site. *Id.*