RECONCILING U.S. BANKING AND SECURITIES DATA PRESERVATION RULES WITH EUROPEAN MANDATORY DATA ERASURE UNDER GDPR

Ronald V. Distante[*]

ABSTRACT

United States law, which requires financial institutions to retain customer data, conflicts with European Union law, which requires financial institutions to delete customer data on demand. A financial institution operating transnationally cannot comply with both U.S. and EU law. Financial institutions thus face the issue that they cannot possibly delete *and* retain the same data simultaneously. This Note will clarify the scope and nature of this conflict.

First, it will clarify the conflict by examining (1) the relevant laws, which are Europe's General Data Protection Regulation (GDPR), the U.S. Bank Secrecy Act, and Securities and Exchange Commission (SEC) regulations, (2) GDPR's application to U.S. financial institutions, and (3) U.S. law's extraterritorial application to financial institutions operating in Europe, under the U.S. Supreme Court's *Morrison-Kiobel* two-step analysis. Second, it will propose a solution by examining international law and U.S. foreign relations law.

United States law subjects financial institutions to multiple data-retention requirements. Securities regulations require broker-dealers to retain customer account and complaint records. The Bank Secrecy Act of 1970 requires financial institutions to retain customer data for at least five years. Sometimes, banks must permanently retain certain records.

GDPR empowers individuals to demand that companies erase their data. Couched in the theory of a right to erasure, GDPR lets customers

---

[*] J.D. Candidate, Fordham University School of Law, 2019; B.A., Economics and Political Science, Iona College, 2015. I would like to thank the editors and staff of the *Fordham Journal of Corporate & Financial Law* for their hard work and valuable contributions to this Note. I would especially like to thank Professor Marc Arkin, without whom this Note would not have been possible. Finally, I would like to thank my family and friends for their steadfast support during law school, especially during the months I spent on this Note.

withdraw their consent for a financial institution to process or retain their data. Violators may face fines of 4 percent of their worldwide revenue. GDPR applies broadly to U.S. data-processors that either (1) are established in the European Union, or (2) monitor or offer to sell goods or services to individuals in the European Union. Establishment is broadly construed by European courts and may be met by "a single representative in the European Union."

In U.S. law, a two-step analysis determines whether and to what extent federal statutes govern conduct abroad. First, courts analyze whether the presumption against extraterritoriality has been rebutted. The presumption derives from the canon that a statute, "unless a contrary intent appears, is meant to apply only within the territorial jurisdiction" of the United States. If the presumption is not rebutted, the court proceeds to the second step, when the court considers the statute's "focus" and whether the case involves the statute's domestic application. United States law has domestic application to data stored domestically, and sometimes possibly to data stored internationally; such data operations may also fall under GPDR's jurisdiction. Then, if a customer asks a financial institution to delete data, the financial institution will face conflicting laws.

This Note seeks to resolve the conflict, recommending that courts approach resolution from the framework of the Restatement (Third) of Foreign Relations Law.

TABLE OF CONTENTS

INTRODUCTION

United States financial law conflicts with European Union data protection law. United States financial law, meaning banking law and securities law, requires financial institutions to keep and maintain customer data for specified time periods.[1] Specifically, securities law requires certain classes of data to be kept and maintained on non-rewritable, non-erasable storage media.[2] European Union data protection law requires firms doing business with European customers to honor customer requests for data erasure.[3]

A U.S. financial institution doing business with customers from the European Union cannot possibly comply with both sets of laws as it cannot preserve and erase the same data simultaneously. Therefore, if a U.S.-regulated financial institution does business with a European customer who later demands erasure, the institution faces conflicting requirements. This issue is especially prominent in light of the financial system's international nature. Investors from EU Member States traded over $16.52 trillion U.S. securities in the first half of 2018, and at the end of 2017, 5.15 percent of FINRA member-firms had foreign offices.[4]

Part I of this Note focuses first on U.S. federal law. It discusses financial law and foreign relations law. Financial law consists of banking law and securities law. Each require U.S. financial institutions to keep and maintain customer data for minimum time periods. Securities law requires broker-dealers to keep and maintain much of this data in a format that cannot be altered or erased during the retention period.[5]

United States foreign relations law consists of two parts "(a) international law as it applies to the United States; and (b) domestic law that has [either] substantial significance for . . . foreign relations . . . or . . . substantial international consequences."[6] The domestic component

1. *See* 17 C.F.R. § 240.17a-4(a-b) (2019).

2. *See* 17 C.F.R. § 240.17a-4(f)(2)(ii)(A) (2019).

3. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43 (EU).

4. The statistics were calculated based on the data in these two reports: 2018 FINRA Industry Snapshot (2018), http://www.finra.org/sites/default/files/2018_finra_industry_snapshot.pdf [https://perma.cc/YY86-ZYGR]; Securities Indus. and Fin. Mkts. Ass'n, Foreign Activity Report: Second Quarter 2018 (Aug. 2018), https://www.sifma.org/wp-content/uploads/2018/08/US-Foreign-Activity-Report-2018-08-17-SIFMA.pdf [https://perma.cc/7E5Q-BY55].

5. *See generally*, Part I.A.2, *infra*.

6. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 1 (AM. LAW INST. 1987).

mainly consists of the Constitution, statutes, court decisions, federal rules, and federal regulatory actions.[7] The domestic component includes conflict of law rules, i.e., "law directed to resolving controversies between private persons . . . arising out of situations having a significant relationship to more than one state."[8]

Part I also focuses on two subjects in EU law. First, it discusses the data protection law: the General Data Protection Regulation. In particular, pursuant to Article 17(1), the General Data Protection Regulation compels firms who do business with European customers to erase personal data about any customers who demand erasure.[9] Second, Part I discusses European financial regulation under the Markets in Financial Instruments Directive. Specifically, it focuses on that law's limited data retention requirements for European investment firms. Such requirements are relevant to the interest balancing test discussed in Parts II and III.

Part II focuses on frameworks for resolving this conflict, both when litigated in U.S. courts and when litigated in European courts. United States foreign relations law and customary international law both suggest an interest balancing approach to resolving conflicts of law.[10] Understanding interest balancing requires understanding the concepts of jurisdiction to prescribe and international comity.[11]

United States foreign relations law does not bind the European Union.[12] Litigating data-related conflicts in European courts would likely result in a judgment against the U.S. financial institution when, as discussed in Part II, European conflict of law rules apply European data

7. *Id.* § 1 cmt. b.

8. *Id.* § 101 cmt. c. (citing RESTATEMENT (SECOND) CONFLICT OF LAWS § 2 (AM. LAW INST. 1969)) (noting that most countries call this topic "private international law" and including private international law in domestic foreign relations law because "many matters of private international law have substantial international significance and therefore may be considered foreign relations law" under section 1).

9. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU).

10. *See generally infra* Part II.

11. *See* discussion *infra* Part II.

12. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S., Introduction (AM. LAW INST. 1987) ("As the Reporters of the previous Restatement said (p. xii): '[t]he positions or outlooks of particular states, including the United States, should not be confused with what a consensus of states would accept or support.' Like the previous Restatement, this Restatement represents the opinion of The American Law Institute as to the rules that an impartial tribunal would apply if charged with deciding a controversy in accordance with international law.").

protection law instead of U.S. financial law.[13] Part II also discusses the European Union's jurisdiction to enforce judgments against non-European businesses in the United States.

Part III first balances each states' interest in applying its substantive law. Then, it performs balancing tests for banking law and securities law. In so balancing, it offers a resolution to the conflict when litigated in U.S. courts. Since European conflict of law rules govern the conflict in European courts, Part III examines the enforceability of European judgments against U.S. financial institutions in U.S. courts.

I. BACKGROUND

A. UNITED STATES FINANCIAL LAW

At the federal level, U.S. financial law includes securities law and banking law. Banking law is a patchwork of statutes and regulations, such as the Bank Secrecy Act and the Foreign Asset Control Regulations.[14] Securities law is an even more complex patchwork of statutes, regulations, and self-regulatory rules.[15] This section will first explain relevant banking law and then explain relevant securities law.

1. United States Banking Law

The Bank Secrecy Act of 1970 is one of the most important federal banking statutes. Treasury regulations under the Bank Secrecy Act require financial institutions to "retain records required by the Bank Secrecy Act for a period of five years."[16] These records include, *inter alia*:

---

13. *See* discussion *infra* Part II.

14. *See, e.g.*, 31 U.S.C. §§ 5311-5330 (2012); 31 C.F.R. § 500 (2019); OFFICE OF THE COMPTROLLER OF THE CURRENCY, Bank Secrecy Act (BSA) & Related Regulations, https://www.occ.treas.gov/topics/compliance-bsa/bsa/bsa-regulations/index-bsa-regulations.html (last visited Mar. 16, 2019) [https://perma.cc/DU2B-SHKY]; Elizabeth Fast, *Document Retention Policy for Banks*, SPENCER FANE LLP (Jul. 15, 2016), https://www.spencerfane.com/publication/document-retention-policy-for-banks/https://www.spencerfane.com/publication/document-retention-policy-for-banks/ [https://perma.cc/3HZ5-U9XL].

15. *See* discussion *infra* Part I.A.2.

16. Stacey Garrett, *Cybersecurity Law & Strategy, "Are U.S. Records Retention Requirements on a Collision Course with the GDPR's 'Right to Erasure?'",* L. J. NEWSLS. (May 2018) (citing 31 C.F.R. § 1010.430(d) (2019)).

> A record of each extension of credit in an amount in excess of $10,000 . . . [containing] the name and address of the person to whom the extension of credit is made . . .
>
> A record of each . . . instruction received or given regarding any transaction resulting (or intended to result . . .) in the transfer of currency or other monetary instruments, funds, checks, investment securities, or credit, of more than $10,000 to or from any person, account, or place outside the United States.
>
> A record of each . . . instruction given to another financial institution or other person located within or without the United States, regarding a transaction intended to result in the transfer . . . of more than $10,000 to a person, account or place outside the United States.[17]

The Bank Secrecy Act also requires banks to maintain Customer Identification Programs (CIPs).[18] A CIP must provide for the collection of identifying data about the bank's customers, e.g., their name, date of birth, and an identification number—such as a taxpayer identification number or passport number.[19] The bank must retain this data for at least five years after the account closes.[20] In addition to the Bank Secrecy Act, various other federal statutes also impose mandatory minimum document retention periods, such as the Equal Credit Opportunity Act, Truth in Lending Act, Truth in Savings Act, and Electronic Funds Transfer Act.[21]

17. 31 C.F.R. § 1010.410 (2019).

18. FED. FIN. INST. EXAMINATION COUNCIL, BANK SECRECY ACT ANTI-MONEY LAUNDERING EXAMINATION MANUAL: CORE EXAMINATION OVERVIEW AND PROCEDURE FOR REGULATORY REQUIREMENTS AND RELATED TOPICS: CUSTOMER IDENTIFICATION PROGRAM—OVERVIEW 45, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_011.htm (last visited Apr. 1, 2019) [https://perma.cc/9H3M-AUCL] (citing 12 C.F.R. §§ 21.21, 208.63(b), 211.5(m), 211,24(j), 748.2(b); 31 C.F.R. § 1020.220 (2019)) ("The CIP is intended to enable the bank to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information and practical risk-based procedures for verifying the identity of each customer.").

19. *Id.* at 47 (citing 26 U.S.C. § 6109 (2012)).

20. *Id.* at 49 (citing 31 C.F.R. § 103.38 (2019)).

21. Fast, *supra* note 14.

2. United States Securities Law

The Securities and Exchange Act of 1934 (the "Exchange Act") imposed a comprehensive federal regulatory system on the securities industry:[22] "The Exchange Act created the Securities and Exchange Commission (SEC), a federal agency with the authority to regulate the securities industry."[23] The SEC creates regulations under the Exchange Act and other federal statutes—such as the Securities Act of 1933—and also enforces federal securities law.[24] However, "because the SEC lacks the resources to police the entire industry, it relies on" (a) a self-regulatory scheme created by Congress and (b) "industry members to promote compliance with the securities laws and regulations to pursue enforcement actions."[25] In 1938, Congress passed the Maloney Act, which amended the Exchange Act to create "extensive guidelines for the formation and oversight of self-regulatory organizations," as well as to better regulate "over-the-counter brokers and dealers operating in interstate and foreign commerce . . . [and] to prevent acts and practices inconsistent with just and equitable principles of trade."[26]

Essentially, the Maloney Act authorized the SEC to delegate regulatory authority to a self-regulatory organization that registers as a national securities association.[27] Associations applying to register as national securities associations must provide their rules to the SEC.[28] Once registered, a national securities association needs SEC approval to change its rules, and the SEC may "abrogate, add to, or delete from . . . the rules . . . as the [SEC] deems necessary or appropriate to insure the

22. *See* Securities Exchange Act of 1934, Pub. L. No. 94-29, 48 Stat. 881 (1934); Karsner v. Lothian, 532 F.3d 876, 879–80 (D.C. Cir. 2008) (quoting Austin Mun. Sec., Inc. v. Nat'l Ass'n of Sec. Dealers, Inc., 757 F.2d 676, 680 (5th Cir. 1985)).

23. Legal Information Institute, *Securities Law History*, available at https://www.law.cornell.edu/wex/securities_law_history (last visited Mar. 16, 2019); *see also* Birkelbach v. SEC, 751 F.3d 472, 474 (7th Cir. 2014) (citing Gold v. SEC, 48 F.3d 987, 990 (7th Cir. 1995)).

24. *Securities Law History*, *supra* note 23; U.S. SEC. AND EXCH. COMM'N, WHAT WE DO (June 10, 2013), https://www.sec.gov/Article/whatwedo.html [https://perma.cc/4Z44-DEXE].

25. *Birkelbach*, 751 F.3d at 474 (citing *Gold*, 48 F.3d at 990); 15 U.S.C. § 78s (2012).

26. Maloney Act of 1938, Pub. L. No. 75-719, 52 Stat. 1070, 1070 (1938); *Karsner*, 532 F.3d 879–80 (quoting *Austin*, 757 F.2d at 680).

27. Maloney Act of 1938, Pub. L. No. 75-719, 52 Stat. 1070, 1070 (1938).

28. *Karsner*, 532 F.3d at 880 (citing 15 U.S.C. §§ 78o-3(a) (2012)).

fair administration of the self-regulatory organization [or] to conform its rules to [statutory requirements]."[29] Sections 15 and 19 of the Exchange Act create a comprehensive regulatory scheme for the SEC to delegate authority to and exercise control over self-regulatory organizations that register as national securities associations.[30]

Pursuant to this comprehensive regulatory scheme, the SEC delegated authority to Financial Industry Regulatory Authority (FINRA), a self-regulatory organization (SRO) "as a national securities association registered with the SEC pursuant to the Maloney Act . . . ."[31] FINRA has a monopoly on self-regulation of the securities industry because it is "the only officially registered national securities association" and all securities firms that "do business with the public" must be FINRA members and are thus subject to FINRA's comprehensive oversight authority.[32] FINRA is

---

29. *Id.* (citing 15 U.S.C. §§ 78s(b)(1), (c) (2012)); *see also Birkelbach*, 751 F.3d at 475 n.2 (citing Aslin v. Fin. Indus. Regulatory Auth., Inc., 704 F.3d 475, 476 (7th Cir. 2013)).

30. Scottsdale Capital Advisors Corp. v. Fin. Indus. Regulatory Auth., Inc., 844 F.3d 414, 424 (4th Cir. 2016) (citing 15 U.S.C. § 78s (2012)) ("Section 19 . . . lays out a comprehensive oversight scheme whereby Congress gives the SEC the authority to supervise FINRA's rules."); *see also* Doscher v. Sea Port Grp. Sec., LLC, 832 F.3d 372, 374 n.2 (2d Cir. 2016) (citing 15 U.S.C. §§ 78o-3, 78s (2012); Fiero v. Fin. Indus. Regulatory Auth., Inc., 660 F.3d 569, 571–72, 574 (2d Cir. 2011)).

31. *Fiero*, 660 F.3d at 571 (citing Maloney Act of 1938, Pub. L. No. 75-719, 52 Stat. 1070 (1938); Desiderio v. Nat'l Ass'n of Sec. Dealers, 191 F.3d 198, 201 (2d Cir. 1999)). FINRA was created in 2007 as a consolidation of the National Association of Securities Dealers—the securities industry's primary self-regulatory organization at the time—and the New York Stock Exchange's "enforcement, arbitration, and member regulation arm." Kashner Davidson Sec. Corp. v. Mscisz, 531 F.3d 68, 71 n.1 (1st Cir. 2008).

32. Virtually every circuit has so held. *See, e.g.*, Picet Overseas Inc. v. Helvetia Tr., 905 F.3d 1183, 1187 (11th Cir. 2018) (citing UBS Fin. Servs., Inc. v. W. Va. Univ. Hosps., Inc., 660 F.3d 643, 648 (2d Cir. 2011)) (acknowledging FINRA's comprehensive oversight authority); Reading Health Sys. v. Bear Stearns & Co., 900 F.3d 87, 90 n.1 (3d Cir. 2018) (citations omitted); Birkelbach v. SEC, 751 F.3d 472, 475 n.2 (7th Cir. 2014) (citing McDaniel v. Wells Fargo Invs., LLC, 717 F.3d 668, 673 (9th Cir. 2013)); Goldman, Sachs & Co. v. City of Reno, 747 F.3d 733, 737 (9th Cir. 2014) (citing FINRA Bylaws, art. IV, § 1(a)) (stating "FINRA has instituted rules with which its members . . . agree to comply"); *Birkelbach*, 751 F.3d at 475 n.2 (citing McDaniel v. Wells Fargo Invs., LLC, 717 F.3d 668, 673 (9th Cir. 2013)); *Fiero*, 660 F.3d at 571 (citing Sacks v. SEC, 648 F.3d 945, 948 (9th Cir. 2011)) (stating that "[a]s a practical matter, all securities firms dealing with the public must be members of FINRA."); *Karsner*, 532 F.3d at 880 (quoting Nat'l Ass'n of Sec. Dealers v. SEC, 431 F.3d 803, 804 (D.C. Cir. 2005)) (stating that "FINRA, as NASD's successor, is 'the only officially registered national securities association.'"); Rodriguez v. Charles Schwab Corp., No. 12-cv-2277 JTF-TMP, 2013

a "quasi-governmental agency with express statutory [regulatory] authority."[33] Nearly all federal circuits have recognized FINRA's regulatory authority, and none have rejected it.[34]

U.S. Dist. LEXIS 33217, at *6 n.3 (W.D. Tenn. Jan. 29, 2013) (citing P&M Corporate Fin., LLC v. Paparella, No. 2:10-cv-10448, 2010 U.S. Dist. LEXIS 112907, at *1 (E.D. Mich. Oct. 22, 2010)) (stating "FINRA has established a set of rules which its industry members must follow.").

Notably, while still recognizing FINRA's regulatory authority, the Second Circuit held FINRA lacks statutory authorization to judicially enforce penalties it assesses; however, it also affirmed FINRA's authority to enforce sanctions by, *inter alia*, barring members from the securities industry, and seeking SEC enforcement in appropriate circumstances. Jonathan Macey & Caroline Novogrod, *Enforcing Self-Regulatory Organization's Penalties and the Nature of Self-Regulation*, 40 HOFSTRA L. REV. 963, 970 n.42 (2012) (citing *Fiero*, 660 F.3d at 572).

33. *Karsner*, 532 F.3d at 880 (citing 15 U.S.C. § 78o-3(b)(7) (2012)). The Exchange Act requires FINRA to "provide a fair [disciplinary] procedure," authorizes it to "initiate a disciplinary proceeding against any FINRA member or associated person for violating any FINRA rule, SEC regulation, or statutory provision," and authorizes the SEC to "review a final disciplinary sanction imposed by FINRA." *Scottsdale*, 844 F.3d at 424 (citing 15 U.S.C. § 78s(e)(1) (2012)); *Fiero*, 660 F.3d at 572 (citing 15 U.S.C. § 78s(h)(3)). The statutory scheme and FINRA rules combine to form a robust adjudicative and appellate process. First, FINRA issues and files a complaint; then, a panel hears the matter and issues a decision; the panel decision is appealable to FINRA's National Adjudicatory Council ("NAC"); the NAC decision is appealable to the SEC; and the SEC decision is appealable to the United States Court of Appeals. *See* Macey & Novogrod, *supra* note 31, 970 n.42 (citing 15 U.S.C. § 78o-3(b)(8)).

34. *See e.g.*, *Picet*, 905 F.3d at 1187; *Bear Stearns*, 900 F.3d at 90 n.1; Wiley v. SEC, 663 Fed. Appx. 353, 356 n.1 (5th Cir. 2016); *Birkelbach*, 751 F.3d at 474–75; *Goldman*, 747 F.3d at 749; *Fiero*, 660 F.3d at 571–72; *UBS*, 660 F.3d at 648; *Karsner*, 532 F.3d at 880; *Mscisz*, 531 F.3d at 71 n.1.

The Eight and Tenth Circuits have not ruled on FINRA's authority. The only relevant Sixth Circuit holding was an unreported decision recognizing FINRA's authority. *See* Troszak v. SEC, 2016 U.S. App. LEXIS 24259, at *1 (6th Cir. June 29, 2016). Many district courts in these circuits have recognized FINRA's authority and none have rejected it. *See e.g.*, Balabon v. Ketchum, No. 1:17-CV-486-LY, 2018 U.S. Dist. LEXIS 22098, at *2 (W.D. Tex. Feb. 9, 2018); Wilbanks Sec., Inc. v. Fin. Indus. Regulatory Auth., Inc., No. CIV-17-481-R, 2017 U.S. Dist. LEXIS 71242, at *1–2 (W.D. Okla. May 10, 2017); Zola v. TD Ameritrade, Inc., 172 F. Supp.3d 1055, 1065 n.8 (D. Neb. Mar. 3, 2016); Klatte v. Buckman, Buckman & Reid, Inc., 995 F. Supp.2d 951, 953 n.1 (D. Minn. 2014); *Rodriguez*, 2013 U.S. Dist. LEXIS 33217, No. 12-cv-2277 JTF-TMP, at *2 n.3; Morgan Keegan & Co. v. Louise Silverman Tr., No. JFM-11-2533, 2012 U.S. Dist. LEXIS 3870, at *1–2 n.1 (D. Md. Jan. 12, 2012); Morgan Keegan & Co. v. Ras, No. 5:11-CV-352-KKC, 2011 U.S. Dist. LEXIS 150392, at *2–3 (E.D. Ky. Nov. 14, 2011); Gilmore v. Brandt, No. 11-cv-00151-REB-KMT, 2011 U.S. Dist. LEXIS

The Exchange Act requires FINRA to have rules that "provide for the enforcement of federal securities laws and [SEC] rules."[35] FINRA rules constitute federal securities laws as a result of its statutorily-created regulatory monopoly.[36] The rules also require members to "make and preserve books and records as required under the FINRA rules, the Exchange Act and the applicable Exchange Act rules."[37] The rules also require members to maintain and preserve customer data, including new account information, updates to new account information, correspondence with customers, written records of customer complaints, and documents related to the allocation of option exercise assignment notices.[38]

125812, at *14 n.6 (D. Colo. Oct. 28, 2011); Empire Fin. Grp., Inc. v. Penson Fin. Servs., No. 3:09-CV-2155-D, 2010 U.S. Dist. LEXIS 18782, at *1–2 (N.D. Tex. Mar. 3, 2010).

35. Sharemaster v. SEC, 847 F.3d 1059, 1062 (citing 15 U.S.C. §§ 78o-3(b)(6)–(8) (2012)) (9th Cir. 2017).

36. *See Birkelbach*, 751 F.3d at 475 n.2. FINRA's *de facto* regulatory authority is a product of the SEC approval process. Because FINRA is a private entity, SEC approval is a necessary procedural safeguard against the private non-delegation doctrine, which generally bars delegation of rulemaking authority to private entities. *See generally* Emily Hammond, *Double Deference in Administrative Law*, 116 COLUM. L. REV. 1705 (2016) (explaining the private non-delegation doctrine and FINRA's relationship to the SEC).

37. FINRA, RULE 4511(a): GENERAL REQUIREMENTS, FINRA MANUAL (2011), https://www.finra.org/rules-guidance/rulebooks/finra-rules/4511?element_id=9957&rbid=2403 [https://perma.cc/VEZ4-B396].

38. *See* FINRA, RULE 2360(b)(23)(C)(iii): OPTIONS, FINRA MANUAL (2019), available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/2360 (requiring, at Rule 2360(b)(23)(C)(iii), preservation of documents related to the allocation of option exercise assignment notices); *see also* FINRA, RULE 2210(b)(2): COMMUNICATIONS WITH THE PUBLIC, FINRA MANUAL (2019), available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/2210 (stating that Rule 2210(b)(2) subjects correspondence, including correspondence with customers, to the supervision and review requirements of Rules 3110(b) and 3110.06–09); *see also* FINRA, RULE 3110(b)(5): SUPERVISION, FINRA MANUAL (2017), available at http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=11345 (stating that Rule 3110(b)(5) requires members' Written Supervisory Procedures to "include procedures to capture . . . all written . . . customer complaints."); *see also* FINRA, RULE 4513(a): RECORDS OF WRITTEN CUSTOMER COMPLAINTS, FINRA MANUAL (2011), available at http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=9959 (requiring four-year retention of written customer complaints); *see also* FINRA, RULE 4512(a): CUSTOMER ACCOUNT INFORMATION, FINRA MANUAL (2019), available at http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=9958 (requiring maintenance and preservation of customer account information).

The SEC has authority under the Exchange Act to make rules requiring broker-dealers to "make and keep for prescribed periods . . . such records as necessary or appropriate in the public interest, for the protection of investors" or to achieve the Act's purposes.[39] Using this authority, the SEC issued Rules 17a-3 and 17a-4, directing which records broker-dealers must make, how to make them, how to maintain them, and how long to retain them.[40] SEC Rules 17a-3 and 17a-4 derive statutory authority from Section 17a(1) of the Exchange Act.[41]

SEC Rule 17a-4(f) requires broker-dealers to preserve electronic records "in a non-rewritable and non-erasable format."[42] This kind of format is called WORM storage, meaning "write once, read many."[43] To comply with Rule 17a-4, a broker-dealer's storage system must do more than merely "mitigate the risk a record will be overwritten or erased."[44] The system must make it impossible to "overwrite or erase records."[45] In addition, SEC Rule 17a-8 "requires broker-dealers to comply with the reporting, recordkeeping, and record retention rules" under the Bank Secrecy Act.[46]

The SEC's interpretive guidance on electronic storage of broker-dealer records explains these rules' purpose:

---

39. SEC Interpretation, Electronic Storage of Broker-Dealer Records, 68 Fed. Reg. 25281 (May 12, 2003), https://www.sec.gov/rules/interp/34-47806.htm [https://perma.cc/JV4L-Q8R7] (citing 15 U.S.C. § 78q(a)(1) (2012)).

40. *Id.* (citing 17 C.F.R. §§ 240.17a-3, 240.17a-4 (2019)).

41. *See* 15 U.S.C. § 78q(a)(1) (2012).

42. SEC Interpretation, Electronic Storage of Broker-Dealer Records, 68 Fed. Reg. at 25281 (May 12, 2003), https://www.sec.gov/rules/interp/34-47806.htm [https://perma.cc/JV4L-Q8R7].

43. Jonathan Fiur, *Deconstructing SEA FINRA 17a-4 (Worm Compliance)*, APRIMO: THE APRIMO BLOG (Jan. 2, 2019), https://www.aprimo.com/blog/deconstructing-sea-finra-17a-4-worm-compliance/ [https://perma.cc/MP5P-J83U].

44. SEC Interpretation, Electronic Storage of Broker-Dealer Records, 68 Fed. Reg. at 25282 (May 12, 2003), https://www.sec.gov/rules/interp/34-47806.htm [https://perma.cc/JV4L-Q8R7].

45. *Id.* (stating that "[a] broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.").

46. U.S. SECURITIES AND EXCHANGE COMMISSION, ANTI-MONEY LAUNDERING (AML) SOURCE TOOL FOR BROKER-DEALERS (2018), https://www.sec.gov/about/offices/ocie/amlsourcetool.htm [https://perma.cc/XQU2-MHEQ] (citing 17 C.F.R. § 240.17a-8 (2019)); *see supra* Part I.A.1 (explaining the Bank Secrecy Act).

> These requirements are integral to the [SEC] investor protection function because the preserved records are the primary means of monitoring compliance with applicable securities laws, including antifraud provisions and financial responsibility standards. Recent events involving the deletion of emails by broker-dealers have affirmed the need to have measures in place to protect record integrity.[47]

Congress has affirmed the importance of data preservation requirements. Senators Hollings, Wyden, and Sarbanes stated that "bank and other financial regulators need to require that records be retained in order that their examiners can insure the safety and soundness of the institutions and compliance with all relevant regulatory requirements."[48] Essentially, regulators must be able to expect broker-dealers "to furnish promptly . . . legible, true and complete copies of those records" per regulator request.[49] This public policy favoring data preservation is reflected in FINRA Rules 4511 and 8210.[50]

FINRA Rule 4511 requires member firms to preserve books and records in a format compatible with SEC Rule 17a-4.[51] FINRA Rule 8210 requires member firms to comply with FINRA's requests to "provide information . . . required to be [] maintained in electronic form" and to

47. SEC Interpretation, Electronic Storage of Broker-Dealer Records, 68 Fed. Reg. at 25282 (May 12, 2003), https://www.sec.gov/rules/interp/34-47806.htm [https://perma.cc/JV4L-Q8R7]; *see also* SEC Interpretation: Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media, 66 Fed. Reg. 22916, 22919 (May 7, 2001) (stating that "Commission enforcement actions against unscrupulous broker-dealers that improperly altered or destroyed records demonstrate the need for measures aimed at maintaining the integrity of broker-dealer records. These cases have included situations in which broker-dealer employers have changed or destroyed order tickets and other transactional records in an effort to shift firm losses to their customers or to conceal fraudulent activities.").

48. SEC Interpretation: Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media, 66 Fed. Reg. 22916, 22921 (May 1, 2001) (citing 146 CONG. REC. S5230 (daily ed. June 14, 2000) (statement of Sens. Hollings, Wyden, and Sarbanes)).

49. *Id.* at 22919.

50. *See* FINRA, RULE 4511(c): GENERAL REQUIREMENTS, FINRA MANUAL (2011), https://www.finra.org/rules-guidance/rulebooks/finra-rules/4511?element_id=9957&rbid=2403*; see also* FINRA, RULE 8210(a): PROVISION OF INFORMATION AND TESTIMONY AND INSPECTION AND COPYING OF BOOKS, FINRA MANUAL (2013), available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/8210.

51. FINRA, RULE 4511(c): GENERAL REQUIREMENTS, FINRA MANUAL (2011).

"provide information . . . [and] permit an inspection and copying of books, records, or accounts pursuant to this Rule."[52]

B. EUROPEAN UNION LAW

The European Union is comprised of twenty-eight Member States and has many federal aspects to it.[53] Two of its regulatory schemes are relevant to this Note. First is the General Data Protection Regulation (GDPR), which regulates processing of EU residents' personal data.[54] Second is the Markets in Financial Instruments Directive.[55]

1. General Data Protection Regulation

The GDPR is a binding regulation.[56] It replaced Directive 95/46/EC, the Data Protection Directive.[57] GDPR Article 5(1) requires data processors, including financial institutions, to process personal data "lawfully."[58] Processing is a technical term for data operations.[59] It

52. FINRA RULE 8210(a), (c): PROVISION OF INFORMATION AND TESTIMONY AND INSPECTION AND COPYING OF BOOKS, FINRA MANUAL (2013), available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/8210.

53. Amy Verdun *The Federal Features of the EU: Lessons from Canada*, 4 Pol. & Governance 100, 103–10 (2016).

54. Council Regulation 2016/679, art. 1, 2016 O.J. (L 119) 32 (EU).

55. Council Regulation 2014/65, art. 1, 2014 O.J. (L 173) (EC).

56. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU); *see, e.g.*, Types of EU Law, European Commission, https://ec.europa.eu/info/law/law-making-process/types-eu-law_en [https://perma.cc/T478-D95Z] (last visited Mar. 30, 2019); Regulations, Directives, and Other Acts, European Union, https://europa.eu/european-union/eu-law/legal-acts_en [https://perma.cc/TX7Z-P3UG] (last visited Mar. 30, 2019); Applying EU Law, European Commission, https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en [https://perma.cc/3TZJ-4MFY] (last visited Mar. 30, 2019). Regulations are binding on their own; with directives, responsibility rests with Member States to enact their own implementing laws.

57. Emily Pehrsson, *The Meaning of the GDPR Article 22*, 31 STANFORD-VIENNA TRANSATLANTIC TECH. F. 1, 1 n.1 (2018).

58. Council Regulation 2016/679, art. 5, 2016 O.J. (L 119) 35 (EU).

59. *See* Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 33 (EU).

includes collecting, storing, and using personal data.[60] Article 6(1) provides six lawful grounds for processing.[61] None of these six grounds recognize compliance with non-European law as a lawful basis for processing.[62]

* * *

60. *Id.*

61. Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 36 (EU).

62. *See id.* The grounds at Article 6(1)(c)–(e) are clearly inapplicable to U.S. financial institutions. Article 6(1)(c) permits processing necessary to comply with legal obligations; this does not include obligations imposed by U.S. law, since Article 6(3) limits 6(1)(c) to obligations under either European Union or Member State law. *Id.* Similarly, Article 6(1)(e), which permits processing necessary to a task performed "in the exercise of official authority vested in the controller," is inapplicable because Article 6(3) limits 6(1)(e) to the authority created by either European Union or Member State law. Article 6(1)(e) also permits processing necessary to a task performed "in the public interest." *Id.* That prong is also inapplicable because of Article 6(3)'s limitation and because it only applies to public authorities or private entities established in EU Member States, not in third countries. Council Regulation 2016/679, recital 128, 2016 O.J. (L 119) 24 (EU) (explaining that when public authorities or private bodies process data "in the public interest," exclusive regulatory authority rests with the "supervisory authority of the Member State where the public authority or private body is established."). Finally, Article 6(1)(d), which permits processing necessary to protect "vital interests" of the data subject or a natural person, is inapplicable to U.S. financial institutions because "vital interests" refers to interests which are "essential for the life of the data subject or . . . another natural person." Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 36 (EU); Council Regulation 2016/679, recital 46, 2016 O.J. (L 119) 8–9 (EU). Financial data is not "essential for the life" of any person.

Article 17 governs the right to erasure.[63] It requires compliance with procedurally valid erasure demands.[64] Understanding erasure requires an

---

63. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU). Article 17 has three sections. *Id.* Section 1 requires controllers to fulfill erasure orders from customers when any one of a disjunctive set of six grounds for erasure applies. *Id.* Section 2 governs the right to erasure when the controller has made personal data public and is thus outside the scope of this note. *Id.* at 44. Section 3 provides five exceptions to Sections 1 and 2. *Id.* at 44. The exceptions under Sections 17(3)(a)–(d) do not apply to financial institutions processing customer data. 17(3)(a) and 17(3)(c), respectively, provide exceptions for "freedom of expression and information" and "reasons of public health." Certainly these do not apply to financial institutions processing unpublished customer personal financial data. *See id.* 17(3)(d) provides an exception for "archiving purposes" consisted with Article 89, but as Article 89 makes clear, this applies to public archives of historical information, so it does not apply private data retention. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU); Council Regulation 2016/679, art. 89, 2016 O.J. (L 119) 84–85 (EU). Section 17(3)(b) provides an exception where processing is necessary for compliance with European Union or Member State obligations or "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 44 (EU). The public interest prong is inapplicable to United States financial institutions since it only applies to public authorities or private entities established in EU Member States, not in third countries. *See* discussion *supra* note 60. Notably, a litigant might argue that processing by a FINRA member firm constitutes an exercise of official authority. However, this argument is severely flawed and, in any event, fails to resolve the conflict. The GDPR defines "controller" to include a "legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." Given FINRA's dual status, a litigant could argue that FINRA's role as a "quasi-governmental agency" vests it with authority under the Maloney Act, while its role as a professional association for securities firms (especially considering the related contractual nature of FINRA membership) qualifies it as acting jointly with its members to determine the purposes and means of processing. *See* discussion *supra* Part I.A.2 (explaining FINRA). There are three problems with this argument. First, it presupposes that the term "official authority" as used in Section 17(3)(b) includes non-European authorities. Second, even if "official authority" does contemplate non-European authorities, it does not necessarily include FINRA specifically. The facts that FINRA is not a state actor and lacks judicial enforcement power militate against such a conclusion. *See* Hammond, *supra* note 35, at 1728 (explaining that FINRA is not a state actor); *see also* Macey & Novogrod, *supra* note 31, 965 n.42 (citing Fiero v. Fin. Indus. Regulatory Auth., Inc., 660 F.3d 569, 572 (2d Cir. 2011) (explaining the Second Circuit's holding that FINRA does not have judicial enforcement power)). Third, even if a litigant prevails on this argument, the 17(3)(b) exception only resolves the conflict with respect to FINRA rules. SEC Rules 17a-3 and 17a-4 still apply to securities firms regardless of their relationship with FINRA. *See* discussion *supra* Part I.A.2. Additionally, this theory only addresses the conflict between the GDPR and United States securities law; banking law is entirely unaffected.

understanding of Article 6(1)'s consent and legitimate interest grounds. If neither apply, data processing is unlawful *ab initio* and subject to mandatory erasure under Article 17(1)(d) absent a 17(3)(e) litigation exception.[65]

Article 6(1)(f) permits processing if the data processor's "legitimate interests" are not overridden by the customer's "interests or fundamental rights and freedoms . . . which require protection of personal data."[66] Legitimate interests do not include U.S. legal obligations for two reasons. First, strict limitation of Article 6(1)(c)'s "legal obligation" basis to European Union and Member State law suggests that the GDPR contemplates foreclosing on non-European legal obligations as exceptions to the GDPR's statutory scheme.[67] Second, even if U.S. legal

64. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU).

65. *Id.* Section 17(3)(e) provides an exception to Section 1's erasure requirements when processing is necessary "for the establishment, exercise or [defense] of legal claims." *Id.* In other words, a 17(3)(e) exception lets financial institutions prevent spoliation of evidence and comply with litigation holds. *See* Margaret Rouse & Stephen J. Bigelow,
Litigation Hold (Preservation Orders or Hold Orders), SEARCH STORAGE (July, 2007) https://searchstorage.techtarget.com/definition/litigation-hold [https://perma.cc/99HZ-RD3C] (explaining litigation holds and spoliation); Stephanie F. Stacy, *Litigation Holds: Ten Tips in Ten Minutes*, BAYLOR, EVNEN, CURTISS, GRIMIT & WITT, LLP https://www.ned.uscourts.gov/internetDocs/cle/2010-07/LitigationHoldTopTen.pdf [https://perma.cc/P28W-ZYEP] (last visited Mar. 31, 2019). So, a United States financial institution faces no conflict regarding data relevant to ongoing or anticipated litigation. Therefore, this note focuses on resolving the conflict outside the narrow context of a 17(3)(e) exception.

66. Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 36 (EU).

67. *See id.* The fact that this limitation is stated *explicitly and in a separate section* further supports this conclusion. *See id.* (providing the "legal obligation" basis in Section 1 and stating the limitation in Section 3). Further, Article 23(1) explicitly allows the European Union and Member States to restrict the "scope of the obligations and rights . . . ." provided in Articles 17 and 18 for specifically enumerated purposes. Council Regulation 2016/679, art. 23, 2016 O.J. (L 119) 46 (EU). Article 23(1)'s explicit statement "Union or Member State" indicates that non-European states cannot derogate the GDPR. *See id.* In addition, one of enumerated purposes refers to derogation necessary to safeguard "a monitoring, inspection or regulatory function connected . . . to the exercise of official authority." *Id. at 47.* The fact that Article 23 thus validates *Member States* law establishing regulatory schemes in derogation of the GDPR indicates that it does not also validate non-European regulatory schemes, since the drafters clearly contemplated exceptions for regulatory schemes and chose to limit such exceptions to those under European law.

obligations do constitute a legitimate interest, they will be overridden by the right to erasure, which the European Union considers fundamental.[68]

Article 6(1)(a) permits data processing when the customer consents thereto, subject to the conditions for consent under Article 7.[69] Article 17(1)(b) requires erasure when processing relies on Article 6(1)(a) consent, the demanding customer withdraws that consent, and "there is

---

68. *See* Case C-131/12, Google Spain, S.L. v. Agencia Española de Protección de Datos, 2014 E.C.R. 317 (calling the right to erasure a "fundamental right"). When balancing legitimate interests, the GDPR's recitals direct consideration of whether, *ab initio*, the data subject "can reasonably expect" the purpose for which their data will be processed. Council Regulation 2016/679, recital 47, 2016 O.J. (L 119) 9 (EU). Since the purpose of the U.S. data retention requirements is to preserve access to data for unforeseen future purposes, customers of United States financial institutions cannot reasonably expect, when the financial institution collects their personal data, the purpose for which it will be used. See supra notes 48–52 and accompanying text; *see also* discussion *supra* Part I.A.

69. Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 36–37 (EU); Council Regulation 2016/679, art. 7, 2016 O.J. (L 119) 37 (EU). A financial institution might include a consent clause in its standard customer agreements. Is a consent clause in an adhesion contract a valid demonstration of consent under Articles 6(1)(a) in light of the Article 7 conditions? Without resolving this issue, which is beyond the scope of this note, the issue itself is relevant when examining Article 17's erasure requirements. If resolving this issue points to 6(1)(a) not permitting United States financial institutions to process European customers' personal data, and Article 6(1)(f) does not permit processing, then Article 17(1)(d) (requiring erasure of unlawfully processed data) automatically applies since the processing was unlawful *ab initio*. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU). If resolving the issue points to 6(1)(a) permitting processing, then Article 17(1)(b) requires erasure if the customer withdraws consent and "no other legal ground for processing" applies. *Id.* In that case, the legitimate interest issue becomes apposite. If, as this note concludes, Article 6(1)(f) does not extend to U.S. legal obligations, then a 17(1)(b) demand requires erasure and thus conflicts with U.S. law. *See supra* note 64 and accompanying text (rejecting Article 6(1)(f)'s inclusion of United States legal obligations as a lawful basis for processing). Regardless of whether Article 6(1)(f) does or does not *initially* permit processing, a customer can still demand erasure by raising a particularized Article 21(1) objection to pursuant to Article 17(1)(c), because an erasure demand at the interstices of Articles 17(1)(c) and 21(1) raises the standard of lawfulness from "legitimate interest" to "compelling legitimate interest." Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU); Council Regulation 2016/679, art. 21, 2016 O.J. (L 119) 45–46 (EU). Even if the legitimate interest can encompass United States legal obligations, based *a fortiori* on the same argument, *supra*, against applying Article 6(1)(f)'s "legitimate interest" clause, the higher "compelling legitimate interest" test would militate against permitting processing. *See* Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU); Council Regulation 2016/679, art. 21, 2016 O.J. (L 119) 45–46 (EU).

no other legal ground for the processing."[70] Article 7(3) conditions consent on the customer being able "to withdraw his or her consent at any time" as easily as first given.[71] Thus, while consent may provide an initial lawful basis for processing, its withdrawal vitiates that lawful basis and puts the GDPR in conflict with U.S. law. The Article 7 conditions also raise the issue of whether consent is actually valid in the first instance.[72] Regardless, the issue is beyond this Note's scope because consent is the only applicable Article 6(1) lawful basis.[73] Therefore, if a financial institution falls short of Article 7's conditions for consent, erasure can be compelled under Article 17(1)(d); if the institution passes Article 7 muster, erasure can be required under Article 17(1)(b) when consent is withdrawn.[74]

---

70. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU). Article 17(1)(b) also requires erasure when consent was given under Article 9(2)(a), which is irrelevant to this note because 9(2)(a) lets data subjects waive the Article 9(1) prohibition on personal data about "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, . . . genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health . . . [and a natural person's] sex life or sexual orientation." Council Regulation 2016/679, art. 9, 2016 O.J. (L 119) 38 (EU). United States financial law does not require maintenance or preservation of any of these categories of data. *See generally supra* Part I.A (discussing the requirements imposed by United States financial law).

71. Council Regulation 2016/679, art. 7, 2016 O.J. (L 119) 37 (EU).

72. For example, the GDPR's recitals state a presumption that consent is not freely given when "the performance of a contract . . . is dependent on the consent despite such consent not being necessary for such performance." Council Regulation 2016/679, recital 43, 2016 O.J. (L 119) 8 (EU).

73. Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 36 (EU). Note that even if, for argument's sake, an Article 6(1)(f) "legitimate interest" provide a lawful basis, the standard to overcome an Article 17(1)(c) erasure demand is clearly higher. *See* Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU). Under Article 17(1)(c), a data subject can demand erasure by raising an Article 21(1) objection "on grounds relating to his or her particular situation" when processing is based no Article 6(1)(f). Council Regulation 2016/679, art. 21, 2016 O.J. (L 119) 45 (EU); *see also* Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43–44 (EU). Absent a litigation exception identical to Article 17(3)(e), a controller must demonstrate that its "*compelling* legitimate grounds for the processing . . . override the interests, rights and freedoms of the data subject." Council Regulation 2016/679, art. 21, 2016 O.J. (L 119) 45 (EU) (emphasis added). The burden of persuasion in a "compelling legitimate grounds" balancing test rests with the controller. Council Regulation 2016/679, recital 69, 2016 O.J. (L 119) 13 (EU).

74. *See supra* note 68 and accompanying text (discussing Article 17(1)(b)); *supra* note 63 and accompanying text (discussing Article 17(1)(d)).

2. *Markets in Financial Instruments Directive*

The Markets in Financial Instruments Directive II (MiFID) requires financial services companies to store communications related to business transactions for seven years.[75] MiFID applies to financial institutions "providing investment services or performing investment activities through the establishment of a branch in the Union."[76] Though MiFID's recordkeeping requirements do not apply to U.S. financial institutions, they warrant discussion for their relevance to the balancing test, which is discussed *infra*.[77] Specifically, MiFID's recordkeeping requirements suggest the European Union has recognized, in a limited context, the same public policy as U.S. regulators.[78] For example, MiFID Recital 57 states that:

> Recording of telephone conversations or electronic communications involving client orders is compatible with the Charter of Fundamental Rights of the European Union (the Charter) and is justified in order to strengthen investor protection, to improve market surveillance and increase legal certainty in the interest of investment firms and their clients.[79]

C. JURISDICTION TO PRESCRIBE

A state's jurisdiction to prescribe is its "authority to make its substantive laws applicable to particular persons and circumstances."[80]

---

75. Shaun Hurst, *Five Lessons to Learn from MiFID II*, SMARSH (Feb. 26, 2019), https://www.smarsh.com/blog/five-lessons-to-learn-from-mifid-ii/ [https://perma.cc/A3JR-8FXK].

76. Council Regulation 2014/65, art. 1, 2014 O.J. (L 173) 41 (EC).

77. *See* discussion *infra* Parts II and III.

78. *See supra* Part I.A.2 (discussing public policy considerations of SEC Rules 17a-3 and 17a-4).

79. Council Regulation 2014/65, recital 57, 2014 O.J. (L 173) 25 (EC).

80. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S., Part IV, Introductory Note (AM. LAW INST. 1987). Jurisdiction to prescribe is one of three classes of jurisdiction in conflict of law analysis; the other two are jurisdiction to enforce and jurisdiction to adjudicate. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 401; *see generally* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S., PART IV (regarding jurisdiction in foreign relations law). Jurisdiction to prescribe must exist before examining jurisdiction to adjudicate or enforce. *See* Denis T. Rice and Julia Gladstone, *An Assessment of the Effects Test in Determining Personal Jurisdiction in Cyberspace*, 58 BUS. L. 601, 603 (2003) (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 401). Jurisdiction to enforce refers to a state's power to

States may exercise jurisdiction outside their own territory,[81] referred to as "extra territorial jurisdiction."[82] International law approaches extraterritorial jurisdiction in two ways.[83] The prohibitive principles approach generally grants jurisdiction unless a contrary rule prohibits it.[84] The permissive principles approach only grants jurisdiction that is specifically provided for.[85] Essentially, the permissive approach tells states when they have jurisdiction, and the prohibitive approach tells them when they do not.

The Restatement (Third) of Foreign Relations Law of the United States summarizes and influences U.S. law on which jurisdiction to prescribe.[86] It adopts a permissive principles approach.[87] Section 402

"employ judicial or nonjudicial measures to induce or compel compliance or punish noncompliance with its laws or regulations, provided it has jurisdiction to prescribe." *Id.* at 604 (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 431(1)). This Note discusses both jurisdiction to prescribe and jurisdiction to enforce. By way of background, jurisdiction to adjudicate refers to tribunal's power to "resolve a dispute in respect to a person or thing where the country has jurisdiction to prescribe the law that is sought to be enforced." *Id.* at 603 (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S., CHAPTER 2, INTRODUCTORY NOTE); *see also* Stephanie M. Chaissan, Note, *"Minimum Contacts" Abroad: Using the International Shoe Test to Restrict the Extraterritorial Exercise of United States Jurisdiction under the Maritime Drug Law Enforcement Act*, 38 UNIV. OF MIAMI INTER-AMERICAN L. REV. 641, 648 (2007) (citing International Shoe Co. v. Washington, 326 U.S. 310 (1945); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 421) (explaining adjudicative jurisdiction in conflict of laws analysis by comparison to *International Shoe's* "minimum contacts" standard for state courts exercise of personal jurisdiction over other states' citizens in U.S. law).

81. *See generally* R.J.R. Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090 (2016).

82. *See generally id.*; Watson v. Emps Liab. Assurance Corp., 348 U.S. 66, 70 (1954).

83. CEDRIC RYNGAERT, JURISDICTION IN INTERNATIONAL LAW 21 (Oxford Univ. Press, 2d ed. 2008).

84. *See id.* at 23–25 (quoting S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18–19 (Sept. 7)) (stating an argument for the prohibitive principles approach, i.e., that "[t]he rules of law binding upon States . . . emanate from their own free will" and "restrictions upon the independence of states cannot therefore be presumed.").

85. *Id.* at 21.

86. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. §§ 402–03 (AM. LAW INST. 1987).

87. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 403 cmt. a (describing the jurisdictional links in § 402 as "generally necessary."). Customary international law also follows the permissive principles approach. *See* Ryngaert, *supra*

provides when states have jurisdiction to prescribe, subject to § 403's restraints.[88] While they are not controlling authority, U.S. federal courts often cite these sections.[89] Congress can regulate extraterritorially by clearly indicating its intent to so regulate.[90] It can also choose to override international law.[91]

This section outlines the Restatement's permissive rules for jurisdiction to prescribe. It also examines the grounds on which the United States and European Union have *prima facie* jurisdiction to prescribe. The next section examines whether each state actually exercises its jurisdiction, given that having jurisdiction is not the same as exercising it.[92]

---

note 81, at 27 (stating "[u]nder the customary international law of jurisdiction . . . extraterritorial prescriptive jurisdiction is arguably prohibited in the absence of a permissive rule."). Arguably, international law is part of United States foreign relations law. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 1(a); *see also* Ryngaert, *supra* note 81, at 41 (citing The Paquette Habana, 175 U.S. 677, 700 (1900) (holding that "[i]nternational law is part of our law.")).

88. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 402.

89. *See, e.g.*, F. Hoffmann-La Roche Ltd. V. Empagran S.A., 542 U.S. 155, 165–66 (2004); Mujica v. AirScan, Inc. 771 F.3d 580, 603–04 (9th Cir. 2014); United States v. Weingarten, 632 F.3d 60, 67 (2d Cir. 2011); United States v. Vilches-Navarrete, 523 F.3d 1, 22 (1st Cir. 2008); BP Chems. Ltd. V. Formosa Chem. & Fibre Corp., 229 F.3d 254, 266 (3d Cir. 2000); Leibovitch v. Islamic Republic of Iran, 188 F. Supp.3d 734, 757 (N.D. Ill. 2016) (noting "courts ordinarily employ" § 403's interest balancing test); NML Capital, Ltd. V. Republic of Arg., 2015 U.S. Dist. LEXIS 30625, at *46 (S.D.N.Y. Mar. 12, 2015) (citing Hilton v. Guyot, 159 U.S. 113, 163–64 (1895)) (noting the Second Circuit suggestion to address the § 403 factors).

90. Equal Emp' Opportunity Comm'n v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991) (hereinafter "EEOC").

91. United States v. Yunis, 924 F.2d 1086, 1091 (D.C. Cir. 1991) (stating that a United States statute "simply modifies or supersedes customary international law" insofar as it is inconsistent with international law); United States v. Bin Laden, 92 F. Supp.2d 189, 214 (S.D.N.Y. Mar. 13, 2000)) (stating "[i]t is well established that Congress has the power to override international law" and the presumption that Congress "generally intends its statutes to be consistent with international law" is rebuttable by "a clear statement of intent to override international law.").

92. *See* discussion *infra* Part I.D.

1. Restatement Provisions

Section 402 states five bases for jurisdiction to prescribe,[93] three of which rest on "links of territoriality."[94] A state has jurisdiction over conduct that happens "wholly or in substantial part" in its territory; conduct abroad that "has or is intended to have substantial effect" therein; and "the status of persons, or interests in things" therein.[95] The fourth basis rests on nationality.[96] A state has jurisdiction over "the activities, interests, status, or relations of its nationals" anywhere in the world.[97] Jurisdiction must rely on one of these bases and must be reasonable under § 403.[98] Section 403 determines reasonableness "by evaluating all relevant factors, including" the eight listed in § 403(2).[99]

2. United States Jurisdiction to Prescribe

When U.S. financial institutions do business with EU customers, the United States has jurisdiction no matter where the transactions occur. Accordingly, the United States has jurisdiction over foreign transactions since these have a substantial effect on U.S. financial markets.[100] In addition to the "links of territoriality" bases, the United States has jurisdiction arising from the financial institutions' "nationality" as U.S. institutions.[101]

---

93. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 402.

94. *Id.* § 402 cmt. a.

95. *Id.* § 402(1).

96. *Id.* § 402 cmt. a.

97. *Id.* § 402(2). While the Restatement also discusses the "protective" and "passive personality" principles as jurisdictional bases, these are not relevant to the present topic. *See id.* § 402 cmt. e, cmt. g; *see also* United States v. Bin Laden, 92 F. Supp.2d 189, 196 (S.D.N.Y. Mar. 13, 2000) (discussing the protective and passive personality principles). After passing the first step of the Section 402 inquiry, reasonableness is determined under Section 403 "by evaluating all relevant factors, including" the eight listed in Section 403(2). RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. §§ 403(1)–(2) (AM. LAW INST. 1987); *see also* discussion *infra* Part II.

98. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 403.

99. *Id.* § 403(2); *see also* discussion *infra* Part II.

100. *See supra* note 99 and accompanying text (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 402(1)).

101. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 402(2) (providing that a state has jurisdiction over "the activities . . . or relations of its nationals.").

If applying U.S. data preservation rules when U.S. financial institutions do business with European customers would constitute an extraterritorial exercise of jurisdiction, then the issue of whether the United States actually exercises such jurisdiction depends on the *Morrison-Kiobel* analysis, discussed *infra*.[102]

3. European Union Jurisdiction to Prescribe

The Restatement is not binding in European courts. European law provides the jurisdictional rules in Europe. When EU conflict of law rules apply EU substantive law, analysis of jurisdiction to prescribe would be immaterial in European court proceedings.[103] Therefore, this section focuses on the application of U.S. jurisdictional rules in U.S. courts.

European Union Member State courts will follow their own choice of law rules. If a Member State's rules point to applying U.S. law, then there is no conflict. More likely, though, member state courts would apply GDPR. Part III.C addresses this situation.

When litigated in U.S. courts, a court would first test whether the European Union has jurisdiction to prescribe—as that concept is understood in U.S. foreign relations law.[104] A U.S. court would likely find that the European Union has jurisdiction to prescribe laws respecting its Member States' citizens interactions with U.S. financial institutions, either based on nationality jurisdiction, or on status-based territorial jurisdiction. The European Union could exercise nationality jurisdiction because transactions with its Member States' citizens involve "the activities, interests . . . or relations of its nationals" regardless of where the transactions happen.[105] It could exercise status-based territorial jurisdiction because a European's transactions with a U.S. financial institution affect the "status of persons, or interests in things" within the European Union.[106] To wit, the transaction would affect the status of the European customers (persons) and their financial assets (things). The European Union likely cannot exercise objective territorial jurisdiction because doing so requires finding that the transactions were intended to

---

102. *See* discussion *infra* Part I.D.1.
103. *See* discussion *infra* Part II.B.1.
104. *See* discussion *supra* Part I.C.1.
105. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 402(2) (AM. LAW INST. 1987).
106. *Id.* § 402(1)(b).

have an effect on European persons and markets.[107] Proving a financial institution had such intent would be very difficult.

D. Actual Exercise of Jurisdiction to Prescribe

Jurisdiction allows a state to regulate but does not require it to do so.[108] The analysis does not end merely because the United States and the European Union both have jurisdiction under sections 402 and 403. A conflict only exists if both actually exercise their jurisdiction. This section discusses United States exercise of jurisdiction under the *Morrison-Kiobel* framework[109] and European Union exercise of jurisdiction under GDPR Article 3.

1. United States

United States courts determine a law's extraterritorial reach using the *Morrison-Kiobel* two-step analysis,[110] which relies on a canon of statutory construction called the presumption against extraterritoriality.[111] Under the presumption against extraterritoriality, courts presume that Congressional statutes and the regulations thereunder do not apply outside the United States unless "the statute demonstrates Congress' 'affirmative inten[t]' that the law should apply" extraterritorially.[112]

Step One asks whether Congress clearly and affirmatively rebutted the presumption.[113] If a court concludes that it did, the statute applies outside the United States, subject to any limits Congress explicated.[114] A "yes" at Step One signals that Congress exercised its jurisdiction to prescribe.

107. *See id.* § 402(1)(c).
108. *See* discussion *supra* Part I.C (defining jurisdiction to prescribe).
109. R.J.R. Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2093–94 (2016) (citing Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108 (2013); Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010)).
110. *Id.*
111. *Id.* at 2112 (Ginsburg, J., dissenting) (citing EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991)).
112. *Id.* (Ginsburg, J., dissenting) (citing *EEOC*, 499 U.S. 248).
113. *Id.* at 2101.
114. *Id.*

A regulation's extraterritorial reach derives from that of its authorizing statute.[115] If the statute fails Step One, so does the regulation.[116] So, whether Rules 17a-3 and 17a-4 apply extraterritorially depends on whether Exchange Act § 17 applies extraterritorially. *Morrison* held that §§ 10(b) and 30(b) did not apply extraterritorially.[117] Though each section of the Exchange Act must be analyzed separately, federal courts have not found § 17 to apply extraterritorially since *Morrison* was decided.[118]

If the answer is no at Step One, the court can still find that Congress exercised jurisdiction under *Morrison-Kiobel* or Step Two.[119] This step asks whether the case involves a "domestic application" of the law.[120] If it does, the statute and its regulations govern the conduct at issue.[121] Courts answer this question by identifying the conduct that is relevant to the statute's focus.[122] If the conduct "occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad."[123] The issue then is whether the conduct relevant to the Exchange Act's focus occurred in the United States.[124] This is "essentially an inquiry into whether the domestic contacts are sufficient to avoid triggering the presumption at all."[125]

---

115. *See* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 261–62 (2010) (citing United States v. O'Hagan, 521 U.S. 642, 651 (1997)) (holding that the regulation at issue in *Morrison*, Rule 10b-5, "does not extend beyond conduct encompassed by § 10(b)'s prohibition.").

116. *See id.*

117. *Id.* at 261–65 (citing 15 U.S.C. § 78dd(b)) (holding that Exchange Act § 30(b) does not apply extraterritorially).

118. *See id.*; *see also* R.J.R. Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2108 (2016) (applying the presumption separately to the Racketeering Influenced and Corrupt Organizations Act's substantive prohibitions and its private right of action).

119. *See Nabisco*, 136 S. Ct. at 2101.

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. *See id.*

125. United States v. Microsoft Corp., 829 F.3d 197, 216 (2d Cir. 2016) (citing Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 266–70 (2010); Mastafa v. Chevron Corp., 770 F.3d 170, 182 (2d Cir. 2014); Loginovskaya v. Batratchenko, 764 F.3d 266, 272–73 (2d Cir. 2014); Gottlieb v. Carnival Corp., 436 F.3d 335, 337 (2d Cir. 2006)).

Legislative history indicates that the focus of Exchange Act § 17 is on preserving data so regulators can enforce securities laws.[126] This policy, viewed in light of the Exchange Act's comprehensive regulatory framework for U.S. securities markets, indicates that data preservation is domestic in nature. Section 17's relevant conduct is clearly data preservation.[127] What constitutes preservation can be interpreted in two ways. If the relevant conduct is the act of storing data, then storing it on systems and networks in the United States is domestic in nature. If the relevant conduct is instead interpreted as refraining from deletion, then the internal decision by a U.S. business to refrain is domestic in nature. For this same reason, the data preservation requirements in banking law are also domestic in nature. Under the *Morrison-Kiobel* analysis, U.S. financial law applies to the situations this Note addresses.[128]

2. *European Union*

GDPR Article 3 applies the regulation's substantive provisions in two ways—on an "establishment" basis and on a global basis.[129] Article 3(1)—establishment application—applies the GDPR "to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, *regardless of whether the processing takes place in the Union* or not."[130] Article 3(2)—global application—applies the GDPR "to the processing of personal data of data subjects who are in the Union" by institutions outside the European Union who either enter its stream of commerce or monitor the behavior of European customers.[131] The latter form, based on a stream of commerce application, applies worldwide.[132]

---

126. *See supra* notes 46–48 and accompanying text (explaining Congress' and the SEC's positions that the mandatory data preservation scheme promotes regulatory certainty and market integrity).

127. *See generally* Securities Exchange Act of 1934, Pub. L. No. 94-29, 48 Stat. 881 (1934).

128. *See* R.J.R. Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2093–94 (2016) (citing Kiobel v. Royal Dutch Petroluem Co., 569 U.S. 108 (2013); Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010)).

129. *See* Council Regulation 2016/679, art. 3, 2016 O.J. (L 119) 32–33 (EU).

130. *Id.* (emphasis added).

131. *Id.*

132. *See* Una Dean & Melis S. Kiziltay Carter, *New Guidelines on GDPR's Territorial Scope Confirm It Reaches Far Beyond the EU*, N.Y. L. J. (Mar. 4, 2019),

E. Identifying the Conflict

The European Union and the United States both potentially exercise their respective jurisdictions to prescribe, with conflicting prescriptions. This calls for a resolution. Part II examines the doctrinal framework for that resolution: the interest balancing test under U.S. foreign relations law and customary international law. Part III examines and balances each state's interests to determine which state has a stronger interest in regulating financial institutions' data processing. It also addresses the enforceability of foreign judgments ordering U.S. financial institutions to erase data under the GDPR.

II. Conflict

A. Litigation in United States Courts

United States conflict of law rules rely on a three-step analysis of jurisdiction to prescribe.[133] The first step examines whether the state has a legal basis for jurisdiction under the permissive rules of section 402 of Restatement (Third) Foreign Relations Law of the United States.[134] Second, exercising jurisdiction must be reasonable under Section 403(2).[135] Third, if two states with conflicting prescriptions can reasonably exercise jurisdiction, an interest balancing test is used to determine which state's law should control.[136]

1. Rule of Reasonableness

Section 403(2) is a non-exhaustive list of eight factors for determining the reasonableness of a state's exercise of jurisdiction to prescribe under Section 402.[137] Federal courts frequently rely on Restatement Sections 402 and 403.[138] The Section 403 factors are:

---

https://www.friedfrank.com/siteFiles/Publications/NYLJ_Dean_Kiziltay%20Carter.pdf [https://perma.cc/8KRZ-4783].

133. Restatement (Third) of Foreign Relations Law of the U.S. §§ 402–03 (Am. Law Inst. 1987).

134. *Id.* § 402.

135. *Id.* § 403(2).

136. *Id.* § 403(3).

137. *Id.* §§ 403(2), 403 cmt. b.

138. *See supra* note 87.

> the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory;
>
> the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between the state and those whom the regulation is designed to protect;
>
> the character of the activity to be regulated, the importance of the regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted;
>
> the existence of justified expectations that might be protected or hurt by the regulation;
>
> the importance of the regulation to the international political, legal, or economic system;
>
> the extent to which the regulation is consistent with the traditions of the international system;
>
> the extent to which another state may have an interest in regulating the activity; and
>
> the likelihood of conflict with regulation by another state.[139]

As explained in Part III, each state has at least some reasonable basis for exercising jurisdiction. Resolving the issue centers around the interest balancing test, which is discussed below.

2. *Interest Balancing Test*

Under Section 403, when two states can reasonably exercise jurisdiction to prescribe, courts must conduct an interest balancing test using the reasonableness factors of Section 403(2).[140] The state with the

---

139. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 403(2).

140. *Id.* In United States foreign relations law, comity considerations are independent of *Morrison-Kiobel* analysis. Comity in United States courts dates back to the Supreme Courts' decision in *Murray v. The Schooner Charming Betsy*, where the court adopted the canon that an act of Congress "ought never to be construed to violate the law of nations if any other possible construction remains." *Murray v. The Schooner Charming Betsy*, 6 U.S. 64, 118 (1804). This was the first time this canon appeared in a Supreme

weaker interest should defer to the state with the stronger interest.[141] This responsibility belongs to whichever court, in the United States, hears the dispute. It is not a negotiation between the two states whose laws conflict. The Restatement's interest balancing test does not apply in European courts.

B. LITIGATION IN EUROPEAN COURTS

GDPR provides two enforcement mechanisms. Article 79 provides for judicial enforcement by granting data subjects a private right of action.[142] Proceedings by EU customers against financial institutions must be brought in Member State courts.[143] Articles 57 and 58 provides for administrative enforcement by Member States' supervisory authorities[144] and requires supervisory authorities to "monitor and enforce [the GDPR's] application" in their territories.[145] Article 58 provides, in relevant part:

> Each supervisory authority shall have . . . corrective powers:
>
> to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
>
> to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation . . .;
>
> to order the . . . erasure of personal data . . . pursuant to Article[] 17 . . .;
>
> to impose an administrative fine pursuant to Article 83 . . .

Court decision, but the canon was far from novel—it dates back to twelfth-century Italy. *See* Ryngaert, *supra* note 81, 46–47. Comity is "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws." Hilton v. Guyot, 159 U.S. 113, 164 (1895). The interest balancing test is a form of comity analysis.

141. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 403(3).
142. Council Regulation 2016/679, art. 79, 2016 O.J. (L 119) 80 (EU).
143. *Id.*
144. Council Regulation 2016/679, arts. 57–58, 2016 O.J. (L 119) 68–70 (EU).
145. Council Regulation 2016/679, art. 57, 2016 O.J. (L 119) 68 (EU).

> The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.[146]

If a Member State court issues a judgment against a U.S. financial institution—either to affirm an administratively imposed penalty under Article 58, or to adjudicate an Article 57 private action—U.S. law will determine the judgments' enforceability in the United States.[147] In an analogous case, *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, the Ninth Circuit refused to enforce a French judgment against a U.S. technology service provider.[148] Notably, the Ninth Circuit declined to reach the First Amendment issue, instead ruling the case was not ripe for decision.[149] However, in *dicta*, the Ninth Circuit adopted the Restatement's rule that "an American court will not enforce a judgment if the cause of action on which the judgment was based, or the judgment itself, is *repugnant to the public policy* of the United States."[150] Mere inconsistency between the foreign judgment and U.S. law is insufficient to constitute repugnancy.[151]

Part III.C advocates for applying the repugnancy approach to EU Member State judgments against U.S. financial institutions for violating GDPR's erasure requirements.[152]

Two standards of repugnancy are relevant for purposes of this Note. Under the first, "[e]xtreme, intolerable differences" give rise to a "public policy exception," whereby national courts may refuse to enforce foreign judgments "on the grounds of inconsistency with national public

---

146. Council Regulation 2016/679, art. 58, 2016 O.J. (L 119) 1.

147. Laker Airways, Ltd. v. Sabena, Belgian World Airlines, 731 F.3d 909, 937 (D.C. Cir. 1984) ("But no nation can expect its laws to reach further than its jurisdiction to prescribe, adjudicate, and enforce. Every nation must often rely on other countries to help it achieve its regulatory expectations.").

148. Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme (*Yahoo! France*), 433 F.3d 1199, 1253 (9th Cir. 2006).

149. *Id.* at 1221.

150. *Id.* at 1213–14 (quoting RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 482(2)(d) (AM. LAW INST. 1987) (emphasis added); RESTATEMENT (SECOND) OF THE CONFLICT OF LAWS § 117 cmt. c (AM. LAW INST. 1971)).

151. *See id.* at 1214.

152. *See* discussion *infra* Part III.C.

policy."[153] This comports with the rule that mere inconsistency of law does not constitute repugnancy, since this standard requires (a) that such differences be both extreme and intolerable, and (b) that the inconsistency be not just of laws but also of national public policies. Second, a "common formulation" of repugnancy weighs public policy concerns against comity. Comity generally directs national courts to enforce foreign judgments, except "where the original claim is repugnant to fundamental notions of what is decent and just in the State where enforcement is sought."[154] This Note refers to these three standards, respectively, as the "extreme, intolerable differences" standard and the "fundamental notions" standard.

III. RESOLUTION

A. RESOLVING THE CONFLICT WITH RESPECT TO U.S. SECURITIES LAW WHEN LITIGATED IN U.S. COURTS

1. Identifying and Analyzing Each States' Interests

Ultimately, courts should balance the United States' and European Union's interests. First, then, this analysis must identify those interests with respect to securities law.

a. Link of Activity to Regulating State's Territory

Section 403(2)(a) directs consideration of "the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct and foreseeable effect upon or in the territory."[155]

Regarding the extent to which the activity occurs in the regulating state's territory, as discussed in Part I, data processing occurs in the United States.[156] While the underlying financial transaction can be

---

153. Alex Mills, THE CONFLUENCE OF PUBLIC AND PRIVATE INTERNATIONAL LAW JUSTICE, PLURALISM AND SUBSIDIARITY IN THE INTERNATIONAL CONSTITUTIONAL ORDERING OF PRIVATE LAW 16 n.46, 257 (Cambridge Univ. Press, ed., 2009).

154. Mark D. Rosen, *Exporting the Constitution*, 53 EMORY L.J. 171, 177 (2004) (citing Will of Brown, 505 N.Y.S.2d 334, 341 (N.Y. Sur. Ct. 1986)).

155. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 402(2).

156. *See* discussion *supra* Part II.D (discussing the *Morrison-Kiobel* Step Two analysis).

considered as occurring partially in both states, the regulated conduct is not the transaction, but the treatment data arising therefrom. The United States has a stronger territorial link to the conduct taking place within its borders, since data processing is performed by securities firms in the United States.

Next is the issue of effect. Weighing where there would be a foreseeable effect is ultimately unhelpful, since the effect on market integrity in the United States and the effect on data privacy in the European Union would both be foreseeable. This leaves the inquiry to focus on which effect is more substantial or direct. The effect on the United States would be more substantial, because market integrity affects every participant in U.S. capital markets. By contrast, data retention would only affect the privacy interests of the narrow class of European customers who demand erasure. That said, for the same reason, the effect on those European customers would be more direct than the abstract effect on market integrity.

As to the effects, foreseeability is unhelpful, as the "substantial" prong weighs towards U.S. law, and the "direct" prong weighs toward EU law. So, the effects consideration is a wash overall. Therefore, considering the 403(2)(a) factors, the "extent" prong weighs towards U.S. securities law, so the 403(2)(a) analysis overall points toward the United States having a stronger interest.

b. Connections Between Regulating States and Principally Responsible Party

Section 403(2)(b) directs consideration of "the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between the state and those whom the regulation is designed to protect."[157]

Here, it is beyond cavil that the party principally responsible for the activity is the U.S. securities firm. Surely the United States has stronger connections with its securities firms than the European Union does. Therefore, this factor also points towards the United States having a stronger interest in regulating the relevant conduct.

---

157. *See* discussion *supra* Part II.A.1.

c. Character and Importance of Regulated Activity and the Extent to Which Other States Regulate It

Section 403(2)(c) directs consideration of "the character of the activity to be regulated, the importance of the regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted."[158] For U.S. securities regulators, mandatory data retention is very important, since allowing data erasure would undermine regulators' ability to monitor securities firms to ensure market integrity and investor protection.

While the European Union certainly considers data privacy rights important, the interaction of MiFID and the legal obligation exception to erasure requirements indicates that the European Union does not view data privacy rights with as high a level of importance as the United States views data preservation laws, which provide no exceptions. Therefore, this factor also points toward the United States having a stronger interest in regulating the relevant conduct.

On the extent to which other states regulate the relevant conduct, the tradition of MiFID again matters. MiFID shows that, internationally, it is not uncommon for states to require financial institutions to retain at least some data.[159] It reflects a shared policy interest of both the United States and the European Union.[160] On the other hand, the European Union is unique in mandating erasure on demand.[161] Thus, this factor should weigh even more strongly towards the United States having a stronger interest in regulating the relevant conduct.

d. Justified Expectations

Section 403(2)(d) directs consideration of "the existence of justified expectations that might be protected or hurt by the regulation."[162] Applying GDPR would hurt the justified expectation the US has. The

---

158. *See* discussion *supra* Part II.A.1.
159. Hurst, *supra* note 77.
160. *See* discussion *supra* Part I.A.2 (discussing public policy considerations of SEC Rules 17a-3 and 17a-4).
161. Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 33–34 (EU).
162. *See* discussion *supra* Part II.A.1.

United States expects data to be stored, sometimes in WORM format.[163] The requirement's purpose is to make data available to regulators for audits, Rule 8210 requests, and other data demands.[164] Regulators' expectations that securities firms will comply by providing "legible, true and complete" copies of required records would be "undermined to the extent that these records are inaccurate . . . or capable of alteration."[165] Applying U.S. securities law would thus protect this expectation. Conversely, applying GDPR's erasure requirement would hurt this expectation.

This factor should weigh the United States' interest in market integrity and regulatory competence more heavily than the European Union's interest in data protection. The former is a market-wide interest protecting the broad class of participants in U.S. capital markets, including both Americans and Europeans.

Other EU laws even recognize such an expectation as justified.[166] MiFID Recital 57 calls that directive's limited mandatory data preservation rule is "justified to strengthen investor protection, to improve market surveillance and increase legal certainty in the interest of investment firms and their clients."[167]

Even assuming a European customer has an expectation that the financial institution will honor his or her erasure demands, such expectation must not be "justified."[168] European customers can choose whether to enter U.S. capital markets; other participants cannot choose to exclude them. Adjudging the 403(2)(d) interest in favor of GDPR would forcibly deprive market participants of the U.S. regulatory system's expected benefits.[169] Adjudging in favor of U.S. securities law would not

---

163. *See supra* notes 47–48 and accompanying text (explaining regulators' expectation that securities firms will "promptly furnish legible, true and complete copies of" required records).

164. *See supra* notes 47–48 and accompanying text (explaining regulators' expectation that securities firms will "promptly furnish legible, true and complete copies of" required records); *see also supra* note 51 and accompanying text (explaining FINRA Rule 8210).

165. SEC Interpretation: Electronic Storage of Broker-Dealer Records, Exchange Act Release 34-44238 (May 1, 2001), https://www.sec.gov/rules/interp/34-44238.htm. [https://perma.cc/F29F-VGGK].

166. Council Regulation 2014/65, recital 57, 2014 O.J. (L 173) 25 (EC).

167. *Id.*; *see also* discussion *supra* Part I.B.2.

168. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 403(2) (AM. LAW INST. 1987).

169. *See id.*

deprive European customers of their expectation, since they can simply choose not to participate in the United States' capital markets. A European customer entering a foreign capital market should not deprive that market's regulators of its ability to enforce the regulatory scheme implemented by a democratically-elected Congress. Nor should they deprive other market participants of the market integrity benefit the regulatory scheme was designed to provide.

This remains true even when U.S. financial institutions market their services to European customers. Those customers can still choose whether to transact with U.S. financial institutions, which are governed by U.S. law.

The United States' interest in market integrity weighs in favor of applying U.S. law and weighs more heavily than the European interest in individual persons' erasure demands. Europeans concerned about their data privacy and erasure rights can simply avoid doing business with the United States. However, as long as the U.S. financial markets remain open to international business, other market participants cannot avoid the loss of market integrity that would result from giving special treatment to EU residents.

e. Importance to and Traditions of the International System

Section 403(e) and (f) direct consideration of a regulation's "importance . . . to the international political, legal, or economic system" and the "extent to which [it] is consistent with the traditions of" those systems.[170]

Even though MiFID may not necessarily apply, its existence creates a tradition that securities firms are different than other businesses and can reasonably be required to retain some data regardless of what the customer wants. That tradition should weaken the European Union's interest, since U.S. regulations are consistent with the tradition embodied by MiFID. The fact that the GDPR was enacted against the backdrop of MiFID, and provides a legal obligation exception, suggests that GDPR's enactment does not vitiate the tradition embodied by MiFID that mandatory data retention rules for financial institutions are not *per se* unreasonable.

---

170. *Id.*

2. Balancing the Interests

For these reasons, a court should conclude from the interest balancing test that the United States has a stronger interest than the European Union does in regulating securities transactions between U.S. securities firms and EU customers. Under Section 403(3) then, the GDPR must yield to U.S. securities law.

B. RESOLVING THE CONFLICT WITH RESPECT TO U.S. BANKING LAW WHEN LITIGATED IN U.S. COURTS

1. Identifying and Analyzing Each States' Interests

Next, this analysis identifies the United States' and European Union's interests with respect to banking law.

a. Restatement Factors 403(2)(a), (b), and (d)-(f)

The same considerations relevant to securities law are also relevant to banking law with respect to Restatement factors 403(2)(a), (b), (d), (e), and (f).[171] As with securities law, these factors weight more strongly toward the United States' interest in having its banking law apply as well. So, this section limits discussion to factor (c).

b. Character and Importance of Regulated Activity and the Extent to Which Other States Regulate It

Section 403(2)(c) directs consideration of "the character of the activity to be regulated, the importance of the regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted."[172] The character of data retention in banking law is even more important, given the anti-money laundering rules imposed by the Bank Secrecy Act. Given the ability of money launderers to move money to "high risk" countries, U.S. regulators have a very strong interest in having access to bank data to prevent laundered money from reaching "high risk"

---

171. *See* discussion *supra* Part III.A.
172. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 403(2).

countries, including countries with a high risk of terrorist financing activity.[173]

2. Balancing the Interests

For these reasons, a court should conclude from the interest balancing test that the United States has a stronger interest than the European Union does in regulating banking transactions between U.S. banks and EU customers. Under Section 403(3) then, the GDPR must yield to U.S. banking law.

C. Resolving the Conflict with Respect to European Court Judgments Against U.S. Financial Institutions

In *Yahoo! France*, the Ninth Circuit argued in *dicta* that U.S. courts could refuse to enforce foreign judgments where the judgment was based on a cause of action repugnant to U.S. public policy.[174] U.S. federal courts, and many state courts, apply the repugnancy standard; they should continue to do so because EU law should not be have the effect of disabling U.S. financial regulators and harming those they protect.[175] This Note argues that any U.S. court should refuse to enforce foreign erasure orders that conflict with U.S. financial law's mandatory data preservation requirements. They should so refuse because, as explained *supra* during the interest balancing tests, the erasure requirement is strongly contrary to U.S. public policy.

Congress has recognized that mandatory data preservation is central to U.S. public policy.[176] Preservation is central for three reasons. First, the financial regulatory regime recognizes that regulators have limited resources.[177] The SEC, for example, relies not just on FINRA, but also on securities firms to enforce securities laws.[178] Policing transactions *ex ante* would be impractical as well. To regulate firms' behavior *ex post*,

173. *See* Alicia Cortez, HIGH-RISK COUNTRIES IN AML MONITORING, ACAMS, http://www.acams.org/wp-content/uploads/2015/08/High-Risk-Countries-in-AML-Monitoring-Alicia-Cortez.pdf [https://perma.cc/ZVX3-6JW9].

174. *See* discussion *supra* Part II.B; *see also Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 433 F.3d 1199, 1213–14 (9th Cir. 2006).

175. *See* discussion *supra* Part II.B.

176. *See supra* note 47 and accompanying text.

177. *See supra* note 26 and accompanying text.

178. *See supra* notes 23–24 and accompanying text.

regulators need access to data about that behavior. So, regulators would have to maintain data themselves if firms were not required to. This would divert regulators' limited resources away from other regulatory operations. However, it would be regulators' only option since their expectations of firms' compliance would be undermined insofar as such records can be edited or deleted.[179]

Second, mandatory data preservation rules prevent regulated firms from shirking their responsibility for internally assuring compliance with financial law.[180] In the absence of such rules, profit motives could incentivize financial institutions to cut their expenses on compliance programs by not maintaining data. Since regulators rely on financial institutions to maintain data, these rules serve an important public policy of assuring regulators the data will be available without the risk that regulated entities delete it to save money.

Third, mandatory data preservation protects regulators from obstruction.[181] Without such rules, firms could hide regulatory violations from regulators by deleting inculpatory data. Data preservation rules counteract this incentive: deleting evidence of a violation is itself a violation.

Applying the "[e]xtreme, intolerable differences" standard, courts should refuse enforcement of European judgments requiring deletion because they are inconsistent with the U.S. public policy favoring data preservation. Given the importance of mandatory data retention rules just discussed, deviating from these rules would be extreme. Since financial regulators cannot properly regulate financial institutions without mandatory data retention rules, such deviation would also invalidate the public policy choices underlying U.S. financial regulation.

Applying the "fundamental notions" standard, courts should also refuse enforcement. Regulatory failure would likely result in regulatory violations going undetected. Because allowing exceptions to the data retention rules would compromise regulators' ability to regulate, such exceptions would likely result in regulatory violations going undetected. Regulation provides a blanket of protection against indecent and unjust

---

179. *See supra* note 183 and accompanying text.

180. See SEC Interpretation: Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media, 66 Fed. Reg. 22916, 22921 (May 1, 2001) (citing 146 CONG. REC. S5230 (daily ed. June 14, 2000) (statement of Sens. Hollings, Wyden, and Sarbanes)).

181. *See supra* notes 50–51 and accompanying text.

conduct. Cutting a hole in that blanket would thus be repugnant to U.S. public policy under the "fundamental notions" standard.

Under both standards, European judgments compelling data deletion are repugnant to U.S. public policy. Whichever standard courts adopt, they should thus refuse to enforce such European judgments. Data deletion orders are not merely inconsistent with U.S. law; they are exceedingly inconsistent with a central element of U.S. public policy judgments about how to regulate the securities and banking industries.

CONCLUSION

Resolving the conflict between U.S. financial law and GDPR thus requires two different approaches depending on the court in which the litigation commences. When litigation begins in U.S. courts, U.S. securities and banking law should prevail over GDPR since the interest balancing tests weigh in favor of U.S. law. However, when litigation begins in Europe, U.S. courts should refuse enforcement because the erasure requirement is repugnant to U.S. public policy.