Alone Together: How the FTC Can Develop a Transatlantic Approach to Consumer Privacy in the Age of Surveillance Capitalism

Luke Posniewski*

TABLE OF CONTENTS

* J.D., May 2025, The George Washington University Law School. B.A. 2018, International Relations and German, Colgate University. I would like to thank the FCLJ Editorial Board as well as Professors Daniel Solove, Tawanna Lee, and Dawn Nunziato for their guidance. I also want to thank my family for their constant love and support.

I. INTRODUCTION

In 2010, David Fincher and Aaron Sorkin put an acclaimed spotlight on the origins of the social media empire Facebook (now Meta) with their film *The Social Network*.[1] The film depicted the drama and personalities involved in the creation but avoided a fundamental question: if the social media product is free for users, how does it earn its billions? That same year, on the other side of the Atlantic, Austrian student Max Schrems learned the answer to this question when he requested Facebook provide him with the data the company retained related to his account.[2] The result was a 1,200-page document detailing Schrems' activity on the site, as well as some information about him that he never originally supplied to Facebook.[3] Schrems' discovery helped illustrate how websites like Facebook collect vast troves of data on their users to develop detailed profiles through which they serve targeted advertisements to generate revenue.[4]

This example highlights the logic behind the metaphor of personal data as the "oil" that fuels the digital economy.[5] In fact, the desire for inferences about consumer behavior has driven so much demand that there is a lucrative market populated by "data brokers," which are companies that collect, aggregate, and share personal information about people as their primary business.[6] As online participation becomes more ubiquitous, data brokers and other companies seeking to monetize consumer data have developed sophisticated tools for tracking consumer behavior on the Internet and inferring details about individual consumers through analysis of personal and behavioral data.[7]

Some argue that these practices create an overall benefit for both consumers and businesses.[8] From this perspective, the free flow of data allows companies to assess consumer demand down to the individual.[9] The data industry can then provide this detailed information to companies selling products or services that meet the demands of particular consumers.[10]

---

1. THE SOCIAL NETWORK (Columbia Pictures 2010).

2. Olivia Solon, *How Much Data Did Facebook Have on One Man? 1,200 Pages of Data in 57 Categories*, WIRED (Dec. 20, 2012), https://www.wired.co.uk/article/privacy-versus-facebook [https://perma.cc/59F8-8FPW].

3. *Id.*

4. Michelle Castillo, *Here's How Facebook Ad Tracking and Targeting Works*, CNBC (Mar. 19, 2018), https://www.cnbc.com/2018/03/19/how-facebook-ad-tracking-and-targeting-works.html [https://perma.cc/KX5U-L6RW].

5. Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019) https://www.wired.com/story/wired-guide-personal-data-collection/ [https://perma.cc/RF75-CQWM].

6. *See generally* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014).

7. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51273-74 (Aug. 22, 2022) (to be codified at 16 C.F.R. Ch. 1).

8. Orly Lobel, *The Problem With Too Much Data Privacy*, TIME (Oct. 27, 2022), https://time.com/6224484/data-privacy-problem/ [https://perma.cc/2M2P-2PDX].

9. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY at ii-iii (2014).

10. *Id.* at iv-v.

Indeed, the demand for consumer data will only grow as companies will require more comprehensive datasets about individuals to infer consumer behavior.[11] However, advocates, scholars, and government regulators have noted that this comprehensive collection of consumer personal data poses substantial risks to those consumers.[12]

These risks can manifest into harm in a number of ways. For example, in an instance where a credit monitoring company incorrectly lists a consumer as a terrorist, they could face adverse credit decisions that harm them economically.[13] Less specifically, one entity's aggregation of information about a consumer creates a number of risks if that information is disclosed to a party seeking to exploit the information.[14] To that end, the aggregation of personal information facilitates identity theft of those individuals if the data brokers are subject to a data breach.[15] Finally, the widespread availability of personal information for purchase creates the risk of effective social engineering campaigns by entities who can use this data to exploit certain information about individuals to influence them into making certain decisions.[16]

In response to these risks, governments have attempted to pass laws that seek to characterize the consumer data collected by companies, define and limit the risks and harms that occur with the collection of that data by establishing certain obligations on entities that collect consumer data, and enforce penalties on entities that violate these laws. The foremost example has been the European Union (E.U.)'s enactment and enforcement of the General Data Protection Regulation (GDPR) in 2018.[17] This comprehensive privacy law governs the general rights people have to their data and sets out rules for entities that seek to collect and use that data.[18] Much of the world has followed the E.U.'s approach and enacted similar laws that comprehensively address information privacy in their jurisdiction.

The United States (U.S.) has developed an alternative approach. Rather than a general regulation, the U.S. takes what is known as a sectoral approach, where Congress has created regulations for certain areas of commerce (e.g., Fair Credit Reporting Act (FCRA) regulations on financial institutions).[19]

Recently, a number of U.S. states have passed their own privacy

---

11. *See, e.g.*, *Using AI to Predict Consumer Behavior*, HIVO, https://hivo.co/blog/using-ai-to-predict-consumer-behavior [https://perma.cc/P7NM-L546] (last visited Oct. 16, 2024).

12. *See e.g.* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 BOSTON UNIV. L. REV. 793 (2022).

13. *See generally* TransUnion LLC v. Ramirez, 594 U.S. 413 (2021).

14. Citron & Solove, *supra* note 9, at 816.

15. Erika Harrell, *Just the Stats Data Breach Notifications and Identity Theft, 2021*, DEP'T OF JUST. (Oct. 2, 2023), https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021 [https://perma.cc/ZC6W-U95D].

16. Justin Sherman & Anastasios Arampatzis, *Social Engineering as a Threat to Societies: The Cambridge Analytica Case*, THE STRATEGY BRIDGE (July 18, 2018), https://thestrategybridge.org/the-bridge/2018/7/18/social-engineering-as-a-threat-to-societies-the-cambridge-analytica-case [https://perma.cc/J28E-T45J].

17. 2016 O.J. (L 119) 87.

18. Shannon Togawa Mercer, *The Limitations of European Data Protection as a Model for Global Privacy Regulation*, 114 AJIL UNBOUND 20, 20-21 (2020).

19. *See, e.g.*, 15 U.S.C. § 1681(a)-(x).

regulations, each with its own set of definitions and requirements, which generally apply to the information of their own citizens or the companies who collect their information.[20] Under this system, U.S. information privacy law for consumers operates as a patchwork where the requirements a data collector must follow are specific to their industry, location, and the source of the data.[21]

Such an arrangement of laws creates difficulties for companies who operate online and collect user data of Americans, as they are concurrently subject to many of these state regulations except for the parts of their business that may fall within the scope of one of the federal sectoral statutes. In addition, companies often collect data from users outside of the U.S., so they must also comply with foreign regulations for consumers subject to those jurisdictions.[22] While there have been efforts to codify a comprehensive federal privacy law, fundamental disagreements between stakeholders have made it unlikely for Congress to agree on a particular set of rules.[23] The closest thing resembling comprehensive consumer privacy protection in the U.S. is the Federal Trade Commission's (FTC) authority to protect consumers against unfair and deceptive trade practices. The agency has taken this authority to regulate the privacy practices of companies in the U.S. In addition, the FTC enforces the E.U.-U.S. Data Privacy Framework, which sets the standard for the transfer of personal data between the U.S. and E.U. member states.[24] In particular, this framework provides a pathway for U.S. companies to process the personal data of E.U. subjects.[25] The FTC's role in regulating consumer privacy has become so fundamental that the agency has initiated rulemaking procedures to develop regulations related to commercial surveillance and data security.[26]

This Note will argue that the FTC should use the E.U.-U.S. Data Privacy Framework to codify its current data privacy practices and harmonize data privacy law for commercial entities on both sides of the Atlantic in a way

---

20. *See* CAL. CIV. CODE § 1798.100 (West 2024) (regulating businesses' collection and use of consumers' personal information and data).

21. Elizabeth R. Pike, *Defending Data: Toward Ethical Protections and Comprehensive Data Governance*, 69 EMORY L.J. 687, 711-12 (2020).

22. Joseph Duball, *EDPB Issues Binding Decision Banning Meta's Targeted Advertising Practices*, INT'L ASS'N OF PRIV. PROS. (Nov. 1, 2023), https://iapp.org/news/a/edpb-issues-binding-decisions-banning-metas-targeted-advertising-practices/ [https://perma.cc/3MSG-JKB6].

23. Lucas Ropek, *There's One Big Problem With the New Federal Data Privacy Bill*, GIZMODO (Apr. 9, 2024), https://www.cnbc.com/2018/03/19/how-facebook-ad-tracking-and-targeting-works.html [https://perma.cc/KX5U-L6RW] (explaining privacy advocates' concern over a federal privacy law that overrides state protections). *See also* Joe Duball, *Calif. Privacy Agency Takes Aim at Dismantling Federal Privacy Protection*, INT'L ASS'N OF PRIV. PROS. (July 29, 2022), https://iapp.org/news/a/cppa-takes-aim-at-dismantling-american-data-privacy-and-protection-acts-preemption/ [https://perma.cc/A75Y-PSSG] (explaining state regulator's concern that a federal law will override their preferred protections).

24. *Data Privacy Framework*, FED. TRADE COMM'N., https://www.ftc.gov/business-guidance/privacy-security/data-privacy-framework [https://perma.cc/A2FL-CWJN] (last visited Sept. 29, 2024).

25. Commission Implementing Decision EU 2023/1795, 2023 O.J. (L 231) 118, 119.

26. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51277 (Aug. 22, 2022).

that practically enhances consumer privacy while creating a standard, predictable regulatory environment for companies that engage in transatlantic data transfers. First, it will critique the inadequacy of the current American system in addressing the risks posed by online surveillance by private entities. Then, it will look to the FTC's role as the U.S.'s privacy regulator to argue that it is uniquely situated to address the issue of online consumer privacy. Finally, this Note will suggest that the FTC can adopt regulations derived from the E.U.-U.S. Data Privacy Framework to enforce privacy standards that enhance general privacy protections for U.S. consumers, create an official expectation of privacy standards for U.S. firms to observe, and facilitate a regulatory environment that promotes firms to comply with the data transfer standards under the GDPR.

II. BACKGROUND

A. U.S. Federal Consumer Privacy Protection

At a general level, the FTC protects consumer privacy as part of its mission to "[protect] consumers from unfair or deceptive business practices and from unfair methods of competition."[27] Under its statutory authority known as "Section 5," the agency enforces consumer protection by seeking injunctions for "unfair" and "deceptive" trade practices.[28] A deceptive practice is one that is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[29] An unfair practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[30]

The FTC has taken a leading role in addressing online consumer privacy since 1995.[31] In this nascent stage of online marketplaces, the FTC employed a hands-off approach by advocating self-regulation based on a set of "fair information principles."[32] However, by the turn of the century, the FTC observed that industry self-regulation was not sufficient to address the standards stated in the principles.[33] As recounted by legal scholars Daniel Solove and Woodrow Hartzog, the FTC's enforcement role began as the "backstop" to the rules created by the companies themselves in the form of

27. *Mission*, FED. TRADE COMM'N., https://www.ftc.gov/about-ftc/mission [https://perma.cc/C5M9-VAMB] (last visited Sept. 29, 2024).

28. 15 U.S.C. § 45(a)(1).

29. Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Com. (Oct. 14, 1983) (on file with the Federal Trade Commission).

30. 15 U.S.C. § 45(n).

31. *See* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 16 (1999).

32. *Id.* at 3.

33. *See* FED TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 35 (2000).

privacy policies.[34] In this form of enforcement, the FTC would hold that a company took part in a deceptive practice by violating its own privacy policy.[35] However, this was an inherently limited form of enforcement, as the FTC lacked the ability to enforce anything if the company did not have its own privacy policy.

The FTC gained status as a national privacy authority through its role in enforcing specific statutes that govern some of the consumer privacy practices for specific types of businesses.[36] In addition, the FTC has responsibility for enforcing the E.U.-U.S. Data Privacy Framework.[37] As Solove and Hartzog observe, the FTC's broad authority under Section 5 and other statutes has led to a number of settlements with alleged violators that serve as a form of FTC "common law," guiding companies in developing their own privacy and security standards.[38]

B. Recent U.S. Legislative Attempts

On the congressional stage, a close attempt to pass a comprehensive privacy bill took place in 2022 when the American Data Privacy and Protection Act (ADPPA) moved out of committee to the full House of Representatives.[39] However, the bill failed to move through the legislative process as it faced resistance on key issues, such as whether to enable a private right of action and whether to preempt state law.[40] Some states, like California, passed extensive consumer privacy legislation and feared that a weaker federal bill would remove their ability to enforce the protections they preferred.[41] Additionally, opponents resisted the bill's inclusion of a limited private right of action, claiming that allowing this narrow private litigation

34. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598-99 (2014).

35. *Id.*

36. *Id.* at 604 (noting that enforcement actions under statutes like COPPA and the Gram-Leach-Bliley Act followed the same model as enforcement actions under Section 5).

37. DEP'T OF COM., E.U.-U.S. DATA PRIVACY FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE 1 (2022), https://privacyshielddev.blob.core.windows.net/publicsiteassets/Full Text_EU-U.S. DPF.pdf. [https://perma.cc/6Q42-M765] (last visited Apr. 9, 2024).

38. Solove & Hartzog, *supra* note 34, at 583.

39. JONATHAN GAFFNEY ET AL., CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 1 (2022).

40. *See* Christiano Lima, *Top Senate Democrat casts doubt on prospect of major data privacy bill*, WASH. POST (June 22, 2022, 5:53 PM), https://www.washingtonpost.com/technology/2022/06/22/privacy-bill-maria-cantwell-congress/ [https://perma.cc/6LES-2JKQ]*; see also* Daniel Castro, *Review of the Proposed "American Data Privacy and Protection Act," Part 1: State Preemption and Private Right of Action*, INFO. TECH. & INNOVATION FOUND.: INNOVATION FILES (June 6, 2022), https://itif.org/publications/2022/06/06/american-data-privacy-and-protection-act-review-part-1-state-preemption-and-private-right-of-action/ [https://perma.cc/6UL5-6G2V].

41. Joe Duball, *Calif. Privacy Agency Takes Aim at Dismantling Federal Privacy Protection*, INT'L ASS'N OF PRIV. PROS. (July 29, 2022), https://iapp.org/news/a/cppa-takes-aim-at-dismantling-american-data-privacy-and-protection-acts-preemption/ [https://perma.cc/A75Y-PSSG].

would lead only to mostly meritless outcomes because individuals could only sue for claims that the FTC or a state Attorney General refused to enforce.[42]

Currently, nineteen states have enacted comprehensive privacy laws, and more state legislatures are considering their own privacy bills.[43] With the previous resistance of California to federal preemption, it seems unlikely that these other states would defer to another legislative push from Congress for comprehensive privacy legislation. However, this lack of general federal consumer protection means that there is no governing standard outside the FTC's general Section 5 enforcement for circumstances outside the specific scope of state consumer privacy statutes or federal sectoral privacy statutes.

C. Europe's General Data Protection Regulation (GDPR)

In 2016, the European Parliament passed what is now known as the GDPR.[44] This comprehensive law established personal data protection as a fundamental right for individuals.[45] In short, the law designates and places regulations on parties that "control" and "process" data about individuals with "controllers" being those who determine the purpose and means of processing the data while the "processor" is the entity who processes the data on behalf of the controller.[46] To lawfully process personal data, a data controller must have a justification, such as an obligation to fulfill a contractual duty, a legitimate interest, or consent from the data subject.[47] The GDPR also creates a special category of data that controllers and processors may not process due to the sensitive information it reveals about the individual.[48] These restrictions, however, do not apply when the circumstances trigger statutory exceptions, such as the "explicit consent" of the individual.[49] Unlike the U.S., the E.U. has a data protection board (EDPB) that oversees the enforcement of the GDPR alongside data protection authorities (DPAs) of member states.[50]

European regulators have interpreted the provisions of the GDPR to find that large online platforms, like Meta, did not comply with the GDPR when processing user data for the purpose of delivering targeted advertisements.[51] In 2023, the Court of Justice of the European Union (CJEU) opined that consent is not a valid legal basis for processing personal data

42. *See* Castro, *supra* note 40 (arguing that the FTC and state attorney generals would likely only enforce claims with merit, so most private lawsuits would likely consist of meritless claims).

43. Andrew Folks, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (Jan. 28, 2024), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#enacted-laws [https://perma.cc/M2GR-2QB8].

44. 2016 O.J. (L 119) 1.

45. *Id.*

46. *Id.* at 33.

47. *Id.* at 36-37.

48. *Id.* at 38.

49. *Id.*

50. *The European Data Protection Board*, EUR. DATA PROT. BD., https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en [https://perma.cc/F6K3-Q3LM] (last visited Oct. 7, 2024).

51. Duball, *supra* note 19.

where there is a "clear imbalance" between the parties.[52] Furthermore, the court elaborated that consent is not necessarily "freely given" within the meaning of the GDPR when "performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[53] In November 2023, the EDPB announced an E.U.-wide ban on Meta's use of user personal data for targeted advertising, reasoning that Meta lacked a "contract" legal basis for these purposes and had not demonstrated compliance with a consent legal basis.[54]

D. E.U.-U.S. Data Privacy Framework

Under the GDPR, data controllers may not freely transfer personal data to another country unless the European Commission has issued a decision stating that the other country possesses an "adequate" level of data protection.[55] As of this Note, the European Commission has not yet determined that the U.S. has adequate data protection under the GDPR. Consequently, commercial entities cannot freely transfer the personal data of those protected by the GDPR to the U.S. This means that large companies like Facebook or Amazon need to prevent data transfers across the Atlantic in the absence of a separate legal arrangement allowing that data transfer. For firms that derive value from the mass aggregation of consumer data, the regulatory situation limits the value of the data they possess because they cannot combine the data protected under the GDPR with other data to create a more global, comprehensive profile of consumer data.[56] In fact, this data flow has serious economic implications, as the U.S. Bureau of Economic Analysis valued E.U.-U.S. data flows in 2020 at $264 billion.[57] Naturally, some argue that restrictions on cross-border data flows pose a significant economic risk to the global economy.[58]

To enable this data flow, the U.S. Department of Commerce created a program known as the E.U.-U.S. Data Privacy Framework (DPF).[59] This program allows U.S. companies to receive data transfers from the E.U.

---

52. Case C-252/21, Meta Platforms, Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537, ¶ 43 (July 4, 2023).

53. *Id.*

54. *EDPB Urgent Binding Decision on Processing of Personal Data for Behavioural Advertising by Meta*, EUR. DATA PROT. BD. (Nov. 1, 2023), https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en [https://perma.cc/AN6V-YUXY].

55. 2016 O.J. (L 119) 61.

56. *See* Dwyer v. Am. Express Co., 237 Ill. App. 3d 742, 749 (Ill. App. Ct. 1995) (holding that the defendants created a value in a list of consumers through the aggregation and categorization of the consumer data).

57. RACHEL F. FEFER & KRISTIN ARCHICK, CONG. RSCH. SERV., IF11613, U.S.-EU TRANS-ATLANTIC DATA PRIVACY FRAMEWORK 1 (2022).

58. Kimberley Bella & Supheakmungkol Sarin, *Free-flowing Data is Good for People and the Global Economy*, WORLD ECONOMIC FORUM (Jan. 16, 2023), https://www.weforum.org/agenda/2023/01/enabling-free-flows-of-data-a-user-centric-approach/ [https://perma.cc/M27E-WXED].

59. EU-U.S. DATA PRIVACY FRAMEWORK , *supra* note 37.

if they self-certify their compliance with specific principles detailed within the DPF.[60] Once firms self-certify and publicly declare their adherence to the DPF, the U.S. Department of Transportation (DOT) and the FTC have the authority to enforce compliance with the DPF.[61] Notably, the FTC's enforcement capability flows from its Section 5 authority, as a company's failure to abide by the DPF principles would constitute an unfair or deceptive trade practice due to its public declaration of compliance.[62]

III. ANALYSIS

A. The Inadequate State of Consumer Privacy Regulation

The current U.S. approach provides a regulatory landscape that limits the possibility of strong consumer privacy protections. While the FTC enforces certain federal statutes related to consumer privacy and pursues general consumer protection under Section 5, the law limits its authority to specific sectors of the economy and the strength of its Section 5 enforcement actions.[63] One might then look to empowering consumers to protect themselves through a federal consumer privacy law with a private right of action, allowing consumers to sue companies in federal court. However, Supreme Court precedent on standing in the privacy context has created an onerous standard for plaintiffs that weakens the deterrence effect of a private right of action. Finally, these regulatory responsibilities should not remain solely with the states, as this scenario would likely create inconsistent requirements for companies which would lead to burdensome compliance requirements for businesses that collect consumer data.[64]

1. Regulatory Gaps in Federal Privacy Law

Under what is known as a "sectoral" approach, the U.S. regulates consumer privacy through a series of statutes that regulate specific areas related to consumer privacy.[65] This method of regulation takes a "harms-based" approach to privacy where the law generally allows the collection and

60. *Id.* at 28.

61. RACHEL F. FEFER & KRISTIN ARCHICK, CONG. RSCH. SERV., IF11613, U.S.-EU TRANS-ATLANTIC DATA PRIVACY FRAMEWORK 2 (2022).

62. EU-U.S. DATA PRIVACY FRAMEWORK PRINCIPLES, *supra* note 37 at 2.

63. Elizabeth R. Pike, *Defending Data: Toward Ethical Protections and Comprehensive Data Governance*, 69 EMORY L.J. 687, 711-12 (2020); Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51280 (Aug. 22, 2022) (recognizing that its Section 5 enforcement may be inadequate to deter companies since it cannot apply civil penalties for first-time violations).

64. Ev Kontsevoy, *New State-Wide Privacy Laws Could Have Unintended Consequences for Consumers and Businesses*, INFOSECURITY MAG. (Mar. 30, 2023), https://www.infosecurity-magazine.com/opinions/state-privacy-laws-consequences/ [https://perma.cc/3G4W-BNKH].

65. Frederic D. Bellamy, *U.S. Data Privacy Laws to Enter New Era in 2023*, REUTERS (Jan. 12, 2023, 10:21 AM), https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/ [https://perma.cc/L398-YZRH).].

use of consumer data but identifies specific sectors of the economy where these activities are restricted to protect consumers from a certain types of apparent harm.[66] For example, the Children's Online Privacy Protection Act (COPPA) identifies the online collection and use of data about children as a heightened privacy risk, and thus imposes more stringent standards on companies that know they are collecting data from children online.[67] As a result, consumer privacy regulation from the federal angle inherently limits itself to only protect consumer privacy from the risks and harms of data collection by companies where the activities of a given company fall within the scope of a given statute.

As such, consumer privacy protection takes the form of a statutory exception to the traditional American approach to encourage self-regulation by industry.[68] Regulators justified this method under the theory that self-regulation was the "least intrusive and most efficient" method to establish data protection principles.[69] However, this lens seems to view consumer privacy more as goodwill provided by the companies collecting and handling consumer data rather than a requirement for companies to refrain from harming consumers through the collection and use of their data. The FTC attempts to fill this gap by enforcing the prohibition of "unfair and deceptive" trade practices under Section 5. However, this amorphous language lacks clear privacy standards (indeed, it's not a privacy-focused regulation) and does not allow the FTC to apply strong enforcement actions.[70] As the economy becomes increasingly digitized, much of consumers' personal data will likely be collected and used outside the scope of federal statutes, which leaves regulators with a scant ability to deter the risk that entities create for consumers through aggregating their data.[71]

2. Weakness of Private Consumer Litigation in Federal Court

Under current jurisprudence, courts have found that most consumers fail to bring a proper cause of action for an alleged privacy violation because there is an inadequate theory of harm to the consumer.[72] While related to government surveillance as opposed to consumer privacy, the Supreme Court in *Clapper v. Amnesty International* interpreted a stringent standing requirement for all plaintiffs seeking to allege a privacy violation.[73] In this

66. *Id.*
67. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506.
68. FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 16 (1999).
69. *Id.* at 6.
70. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51280 (Aug. 22, 2022).
71. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/H3C9-BPGM].
72. *See, e.g.*, TransUnion LLC v. Ramirez, 594 U.S. 413, 433 (2021).
73. Clapper v. Amnesty Int'l, 568 U.S. 398, 414 (2013).

case, the plaintiffs alleged a constitutional violation due to the "objectively reasonable likelihood" of government surveillance of their communications.[74]

The Court ruled that the plaintiffs lacked standing because the alleged harm of unconstitutional government surveillance was speculative, since they did not have proof of actual surveillance.[75] In addition, the Court found that the plaintiffs did not have standing due to the costs incurred to avoid unconstitutional surveillance, since these costs arose from the same speculation of surveillance rather than concrete proof of surveillance.[76]

While not directly addressing consumer privacy, *Clapper* highlights the difficulty of alleging harm while litigating the collection and use of personal data. Courts have carried this scrutiny of privacy litigation to consumer privacy in cases such as *TransUnion v. Ramirez*.[77] There, a company aggregated consumer information and created erroneous data about certain consumers, including mislabeling one individual as a potential terrorist.[78] The plaintiffs brought a class action suit alleging a violation of the Fair Credit Reporting Act (FCRA).[79] The Court held that certain class members lacked standing, even though the company violated their statutory rights under FCRA, because there was no concrete harm associated with that violation.[80] However, the Court also found certain class members did allege adequate, concrete harm to confer standing because the company shared its erroneous data with third parties, and this caused the affected plaintiffs to suffer reputational harm with a "close relationship" to a defamation claim.[81]

These cases imply that courts will likely rule that a consumer-plaintiff lacks standing where they fail to allege the misuse of their data reflects a "close historical or common-law analogue."[82] Even where a statute confers consumer privacy protections and seeks to enforce them through a private right of action, courts will likely not view a violation of those protections as enforceable in itself. Consequently, consumer privacy regulation enforced through a private right of action likely does not confer enforceable protections under the Supreme Court's standing precedent.

3. Reliance on State Law Is Inadequate to Address Consumer Privacy

As of April 2024, nineteen states have enacted consumer privacy laws and numerous others are in the process of legislating their own.[83] One look at

74. *Id.* at 410.
75. *Id.* at 414.
76. *Id.* at 416.
77. *Ramirez*, 594 U.S. at 413.
78. *Id.* at 420.
79. *Id.* at 421.
80. *Id.* at 438.
81. *Id.* at 433.
82. *Id.* at 414.
83. Andrew Folks, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (Jan. 28, 2024) https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#enacted-laws [https://perma.cc/M2GR-2QB8].

the International Association of Privacy Professional's U.S. State Privacy Legislation Tracker shows the diversity of the current and proposed laws, which differ in the privacy rights conferred to consumers and the obligations imposed on businesses.[84] Inevitably, each state law will likely also differ in its important definitions (e.g., personal data), as well as the statutory interpretation of seemingly similar provisions. The transitory nature of online data collection and gathering will likely exacerbate this incongruence, as information seamlessly crosses over state boundaries in a matter of seconds. As a result, a consumer privacy protection regime based solely on state statutes is likely inadequate because it would create an uneven regulatory environment that places a substantial burden of compliance on companies. In addition, this would create major regulatory complexities for data transfers with markets that have standards like the GDPR, as states with inadequate data protection standards would cause the markets to prohibit data transfer to the U.S.

For example, an online business that collects consumer data from all American users will theoretically have to comply with the privacy law of each state, assuming an American from each state uses it. Since the business falls within the scope of each statute, it must understand the definitions, interpretations, and applications of each law. This scenario creates a major burden because the companies must spend time and resources learning about each law and assessing how to comply with all of them. While it may be reasonable to subject businesses to high standards for the collection and use of personal data, these complexities might end up harming consumer protection in the end, as the consumer would have to interpret a given company's understanding of their own labyrinthine regulatory situation to understand exactly how that company collects and handles their data.

B. The FTC Should Assume the Role of Promulgating and Enforcing General Federal Consumer Privacy Regulations

Due to its history of developing and enforcing privacy standards under current law, the FTC stands in the best position to create and enforce general consumer privacy standards. First, the FTC has gained authority as a privacy regulator from Congress's grant of statutory authority to shape privacy regulation in certain sectors.[85] Furthermore, the agency has developed expertise and substantive principles regarding privacy through its enforcement efforts.[86] Finally, the FTC has recognized its role in this area by initiating its rulemaking procedure regarding online commercial surveillance and data security.[87] With this authority, experience, and opportunity, the FTC should promulgate privacy regulations to provide comprehensive protection to U.S. consumers.

---

84. *Id.*
85. *See, e.g.*, 15 U.S.C.A. § 6804(a)(1)(C).
86. Solove & Hartzog, *supra* note 34, at 583.
87. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51280 (Aug. 22, 2022).

1. The FTC Serves as the De Facto Federal Privacy Regulator

E.U. member states enforce the GDPR through Data Protection Authorities.[88] In contrast and reflective of its sectoral approach, U.S. federal privacy regulation is dependent on the applicable statute.[89] As a result, there is no official administrative body solely responsible for enforcing federal privacy regulations. For example, the Health Insurance Portability and Accountability Act (HIPAA) creates a Privacy Rule that carries potential civil and criminal penalties.[90] The Department of Health and Human Services Office for Civil Rights carries out civil enforcement, while the Department of Justice manages criminal enforcement.[91]

While this may appear to imply there is no authoritative agency enforcing consumer privacy protections in the U.S., a comparison of the statutes and the history of FTC Section 5 enforcement actions shows that the FTC serves as the de facto federal privacy regulator.[92] First, a comparison of federal statutes that enforce consumer privacy standards reveals that the FTC is the most common regulator responsible for enforcement.[93] In addition, the FTC enforces consumer privacy as part of its broad mandate to prohibit unfair and deceptive trade practices under Section 5.[94] Consequently, the FTC sits in the best position to administer privacy regulations, as it has developed standards for regulating data privacy, possesses the ability to apply such standards under its Section 5 authority, and currently has the opportunity to promulgate its standards into express rules in its current rulemaking process.

As Solove and Hartzog explain, the FTC also received more legitimacy as the "lynchpin" of the enforcement mechanism that allows cross-border data transfer with the E.U.[95] At that time, E.U. regulators ruled that the U.S. did not have adequate levels of privacy protection, and E.U. law prohibited data transfers to such countries.[96] To protect the commercial benefits of the data transfers between these major markets, the U.S. and E.U. regulators entered into the Safe Harbor Agreement which allowed companies to transfer personal data from the E.U. if they agreed to comply with principles set out in the agreement.[97] With the FTC's pedigree as the regulator of a number of

88. *What Are Data Protection Authorities (DPAs)?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en [https://perma.cc/MMG5-F73W] (last visited Apr. 9, 2024).

89. STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., IF11207, DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION 1 (2022).

90. *See* 45 C.F.R. § 164 (2024); *see also* 42 U.S.C. § 1320d-5-1320d-6 (setting out potential civil and criminal penalties for violations).

91. *Id.*

92. Solove & Hartzog, *supra* note 34, at 583.

93. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 166-67 (International Association of Privacy Professionals, 6th ed. 2022).

94. *See* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 16 (1999).

95. Solove & Hartzog, *supra* note 34, at 604.

96. *Id.* at 603.

97. *Id.* at 604.

federal privacy statutes, along with its companies' privacy policies for online companies, the Safe Harbor Agreement made the FTC the main regulator for U.S. compliance as the U.S. lacked a formal data protection authority.[98]

Although the CJEU invalidated the Safe Harbor Agreement, its successor, the E.U.-U.S. Data Privacy Framework, retains this enforcement mechanism with the FTC at the helm.[99]

2. The FTC Has Attained Privacy Expertise and Developed Substantive Privacy Standards

With its role as the central privacy regulator and its broad, somewhat vague mandate under Section 5, Hartzog and Solove conclude that the FTC has effectively produced a body of precedent through its enforcement actions and settlements.[100] In particular, the legal community uses the FTC's published settlement agreements and statements as guidance as to how the FTC will interpret and apply Section 5 to different privacy situations.[101]

Hartzog and Solove identify four trends in FTC enforcement actions that show the FTC has been able to interpret Section 5 to strengthen consumer privacy protections beyond ensuring a company's compliance with the language in its privacy policy.[102] First, the FTC has evolved its general standards into more specific ones.[103] Second, it has introduced "norms and best practices" into its assessment of privacy practices.[104] Third, it has created baseline standards that companies must meet.[105] Finally, the FTC has mirrored common law principles to recognize "indirect" unfair or deceptive practices similar to contributory liability.[106]

With respect to the first trend, the FTC has developed some specific requirements for companies to avoid the general moniker of "unfair" or "deceptive."[107] Hartzog and Solove highlight this evolution through a review of FTC settlement decrees that declare certain data security practices as inadequate and interpret the statement "clearly and conspicuously" to require "specific text with hyperlinks."[108] Although these settlement decrees do not have a legal effect on other parties, they reveal that the FTC can develop and implement heightened privacy requirements in its enforcement, and regulated companies will accept them.

Under the second trend, Hartzog and Solove find that the FTC has introduced qualitative judgments about certain practices such as the

98. *Id.*
99. DEP'T OF COM., *supra* note 37, at 52.
100. Solove & Hartzog, *supra* note 34, at 620-21.
101. *Id.* at 626.
102. *Id.* at 649.
103. *Id.*
104. *Id.*
105. *Id.*
106. Solove & Hartzog, *supra* note 34, at 649.
107. *Id.*
108. *Id.* at 657-58.

"inadequacy" of notices.[109] For instance, a vague disclosure from a company about how they track consumer activity when they download certain software may constitute a deceptive trade practice if the FTC considers the disclosure inadequate to inform a consumer.[110] Also in this thread of FTC "jurisprudence," the agency has effectively incorporated industry standards into its assessment of data security practices, pursuing enforcement actions against companies that employ inadequate security measures.[111] In *FTC v. Wyndham*, the Third Circuit confirmed the FTC's authority to pursue enforcement against a company's unfair practices under Section 5 because they failed to meet "commercially reasonable methods for protecting consumer information."[112] This decision affirmed the Third Circuit's view that the FTC is able to incorporate certain qualitative standards in its assessment of industry practices without explicit reference in the FTC Act.

This reasoning goes hand-in-hand with the "baseline standards" required by the FTC as identified by Hartzog and Solove.[113] Specifically, they state the FTC "require[s] baseline security practices for all companies that deal with personal information and prohibits certain kinds of invasive information collection…regardless of the existence of a privacy policy."[114] This ability to enforce specific requirements for privacy and data security reveals that the agency has discretion under the FTC Act to incorporate new principles into consumer protection enforcement actions.[115] Indeed, Hartzog and Solove conclude that the FTC can use their approach to enforce developing norms and customs of consumer privacy as substantive rules.[116]

As technology changes how consumers interact with businesses in the digital space, the FTC has continued developing substantive standards around practices that affect consumer privacy.[117] One such phenomenon is the FTC's recognition of and action against the use of "dark patterns" by companies to obtain consumer consent.[118] Rohit Chopra (then, an FTC Commissioner)

---

109. *Id.* at 659.

110. *See* Complaint at para. 13, Sears Holdings Mgmt. Corp., F.T.C. No. C-4264 (Aug. 31, 2009) https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf [https://perma.cc/2VYF-TD3K] (finding the download of tracking software unfair or deceptive because the license agreement did not adequately disclose the extent of the tracking).

111. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241 (3d Cir. 2015).

112. *Id.*

113. Solove & Hartzog, *supra* note 34, at 661.

114. *Id.*

115. *See e.g.*, FED. TRADE COMM'N, 2020 PRIVACY AND SECURITY UPDATE 3-5 (2020), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf [https://perma.cc/U7KY-BBKM] (discussing the FTC's practice of requiring companies to implement comprehensive security program).

116. Solove & Hartzog, *supra* note 34, at 673.

117. *See, e.g.*, Final Complaint and Order at para. 1, Epic Games, Inc., F.T.C. No. C-4790 (Mar. 14, 2023) (alleging unfair practices due to company's use of "dark patterns" caused led consumers to incur charges without their express informaed consent).

118. Sean Kellogg, *How US, EU Approach Regulating 'Dark Patterns',* INT'L ASS'N OF PRIV. PROS. (Dec. 1, 2020), https://iapp.org/news/a/ongoing-dark-pattern-regulation/ [https://perma.cc/7FE7-FZP7] (last visited Apr. 9, 2024).

defined dark patterns as "design features used to deceive, steer, or manipulate users into behavior that is profitable for an online service, but often harmful to users or contrary to their intent."[119] While FTC actions have focused on the use of dark patterns to obtain customer consent to payment, scholars have shown that the same principle applies to consumer consent for privacy.[120] Even though these enforcement actions are not substantive regulations in themselves, the enforcement actions and subsequent Commissioner opinions reveal that the FTC has continued following the trends described by Hartzog and Solove by identifying certain substantive principles in its approach to consumer protection that implicate privacy.

3. FTC Rulemaking Authority and the Proposed Rule on Online Commercial Surveillance and Data Security

Outside of its ability to protect consumer privacy through prohibiting unfair and deceptive trade practices of specific companies under Section 5, the FTC also has the ability to use rulemaking to "address unfair or deceptive practices…that occur commonly."[121] This form of rulemaking is known as Magnusson-Moss Rulemaking Authority, and it establishes extra procedures such as a "reason to believe that the practices to be addressed by the rulemaking are 'prevalent.'"[122] Through this process, the FTC may create rules, known as trade regulation rules, which define specific practices that are unfair or deceptive and apply to an entire industry.[123] After rules are promulgated, they create civil penalties for anyone who violates the rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule."[124]

In August 2022, the FTC initiated its Magnusson-Moss Rulemaking Authority and published an advanced notice of proposed rulemaking to consider whether it should issue trade regulation rules relating to "commercial surveillance and lax data security practices" by companies.[125] According to

---

119. Press Release, FTC, Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc. 1 (Sept. 2, 2020) (on file with the Federal Trade Commission) https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf [https://perma.cc/W73C-H7LT].

120. Johanna Gunawan et al., Position Paper: Towards an Understanding of Dark Pattern Privacy Harms 1 (May 8, 2021), (on file with CHI Workshop) https://darkpatterns.ccs.neu.edu/pdf/gunawan-2021-chiworkshop.pdf [https://perma.cc/CF83-S6AB] (defining dark patterns as "interface designs that lead users towards outcomes that benefit the platform over users, or that steer users away from what they are intending to do).

121. *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/D4TX-UCL2] (last visited Sept. 29, 2024).

122. *Id.*

123. *Id.*

124. *Id.*

125. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51277 (Aug. 22, 2022).

the FTC, the practice of commercial surveillance involves the "collection, retention, aggregation, analysis, and onward disclosure of consumer data" to target consumers for various commercial purposes.[126] As evidenced by its enforcement actions against companies for unfair or deceptive privacy practices, the FTC recognized that there may be prevalent practices that permit trade regulation rules.[127] Specifically, the FTC points to the limitations of its current Section 5 enforcement capabilities, as its enforcement actions do not allow for civil penalties until an individual company violates Section 5 a second time.[128] Since new trade regulation rules would permit the FTC to seek civil penalties for first-time violators, it posits that new trade regulation rules will bolster consumer privacy protections by incentivizing companies to invest in privacy compliance to proactively avoid these penalties rather than retroactively reacting to enforcement actions.[129]

Recent Supreme Court jurisprudence may undermine the FTC's ability to interpret its Section 5 authority to promulgate these regulations. In *Loper Bright*, the Court overruled the long-standing *Chevron* doctrine, which required courts to defer to "permissible" agency interpretations where statutory language is ambiguous.[130] Moreover, under the major questions doctrine, the Court looks for more express authorization from Congress when an agency asserts authority on a matter of major "economic and political significance."[131] With the ubiquity of online commerce and the use of consumer data in the economy, it is likely that the Court would take such an approach to this question.

However, these decisions are unlikely to bar the FTC's authority to regulate commercial surveillance and data security. Magnusson-Moss rulemaking, as opposed to Administrative Procedure Act, expressly authorizes the FTC to promulgate rules that "define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce."[132] The main question then is whether the FTC may interpret certain commercial surveillance and data security practices as unfair and/or deceptive. The FTC likely can interpret Section 5 this way, as suggested by the Third Circuit in *Wyndham*, since the standard is a "flexible concept" that Congress intentionally left for development by the FTC.[133] This suggests that a court reviewing an FTC rule need not address the question of deference, as Congress expressly granted the duty of interpretation to the FTC, not the Court. As a result, a court would likely find that Congress did grant the FTC

126. *Id.* at 51273-74.
127. *Id.* at 51280.
128. *Id.*
129. *Id.*
130. *See* Loper Bright Enterprises v. Raimondo, 144 S. Ct. 2244, 2254 (2024)
131. *See* FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 159-160 (2000).
132. 15 U.S.C. § 57a(a)(1)(B).
133. *See* Wyndham, 799 F .3d at 243.

clear authority to implement them due to its broad discretion to regulate unfair and deceptive acts and practices in or affecting commerce.[134]

C. E.U.-U.S. Data Privacy Framework as a Standard for New Privacy Trade Regulation Rules

1. The E.U.-U.S. Data Privacy Framework

The E.U.-U.S. Data Privacy Framework is a mechanism to "facilitate transatlantic commerce by providing U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union."[135] The E.U. and U.S. built the Data Privacy Framework to continue reaping the commercial benefits of the Safe Harbor Agreement after it was invalidated by cases in Europe known as *Schrems I* and *Schrems II*.[136]

After Edward Snowden, a government contractor for the National Security Agency, revealed U.S. intelligence agencies regularly accessed troves of personal data, litigation from Austrian privacy advocate Max Schrems lead to the suspension of the legal framework for data transfers to the U.S. from the E.U..[137] The resulting case led the CJEU to invalidate the European Commission's adequacy determination, allowing data transfers to the U.S., which led to the creation of a new framework known as the E.U.-U.S. Privacy Shield.[138] Schrems's amended complaint resulted in yet another CJEU invalidation of the European Commission's adequacy determination of the Privacy Shield.[139]

The E.U.-U.S. Data Privacy Framework allows American companies to transfer personal data protected by the GDPR if they agree to be bound by the principles detailed within the Data Privacy Framework.[140] The FTC acts as the enforcer of the Data Privacy Framework under the logic that the companies voluntarily entering into the Data Privacy Framework represent that they adhere to it. Therefore, a deviation from the Framework would constitute an unfair or deceptive trade practice.[141] As required by the GDPR, the European Commission issued a decision on July 10, 2023 declaring that the E.U.-U.S. Data Privacy Framework provided an "adequate level of protection for personal data transferred...to certified organizations in the United States."[142]

---

134 *See* Douglas Ross, *How Loper Bright and the End to the Chevron Doctrine Impact the FTC*, PROMARKET. (Sept. 5, 2024), https://www.promarket.org/2024/09/05/how-loper-bright-and-the-end-to-the-chevron-doctrine-impact-the-ftc/ [https://perma.cc/6T7W-KPP5] (last visited Nov. 23, 2024).

135. DEP'T OF COM., *supra* note 37, at 1.

136. *Schrems I*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/article/schrems-i/ [https://perma.cc/2TTJ-VZNM] (last visited Sept. 29, 2024).

137. *Id*.

138. *Id.*

139. *Id.*

140. DEP'T OF COM., *supra* note 37.

141. *Id.* at 26.

142. Commission Implementing Decision EU 2023/1795, 2023 O.J. (L 231) 118, 119.

2. The Applicability of the E.U.-U.S. Data Privacy Framework Principles as Trade Regulation Rules

The Data Privacy Framework expresses seven Principles that participants must comply with to take advantage of the E.U.'s adequacy decision and receive personal data from E.U. data subjects.[143] These Principles are Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; Recourse, Enforcement, and Liability.[144]

Notice operates like a privacy policy requirement that directs participants as to what information the Data Privacy Framework requires them to communicate to consumers.[145] This reflects current standards of FTC enforcement that require adequate disclosure to consumers about their practices, but it specifies exactly what must be included at a minimum.[146]

Choice details the consent organizations must obtain from consumers for the use of their data.[147] However, the aspect of consent differs significantly from the FTC's domestic enforcement standards. While similar to their requirement of clear and conspicuous text detailing to consumers how to opt-out of consent, the Data Privacy Framework employs the GDPR's concept of sensitive data.[148] Under the Data Privacy Framework Standard, consumers must affirmatively consent to the collection and use of their sensitive data.[149]

Sensitive data is defined as "personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual."[150] This approach to sensitive data is known as opt-in consent, which the FTC does not necessarily require as a matter of its Section 5 enforcement.[151]

Accountability for Onward Transfer essentially creates an obligation of stewardship for the data transferor such that it must require any transferee to adhere to the Principles and enter into a contract that limits the use of the controlled data.[152] These purposes must adhere to the scope of the consent

143. DEP'T OF COM., *supra* note 37, at 4-8.

144. *Id.*

145. *Id.* at 4-5.

146. *Id.*; *see also* Complaint at para. 13, Sears Holdings Mgmt. Corp., F.T.C. No. C-4264 (Aug. 31, 2009) (alleging that the full extent of the software's tracking of consumers' Internet behavior would be material to consumers' decision to install the software, so the failure to disclose this was deceptive under the FTC Act). https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf [https://perma.cc/VTE7-LEZY].

147. DEP'T OF COM., *supra* note 37, at 5.

148. Solove & Hartzog, *supra* note 34, at 658; DEP'T OF COM., *supra* note 37, at 5.

149. DEP'T OF COM., *supra* note 37, at 5.

150. *Id.*

151. *The Difference Between Opt-In vs Opt-Out Principles In Data Privacy: What You Need To Know*, SECURE PRIV. (Feb. 1, 2024), https://secureprivacy.ai/blog/difference-beween-opt-in-and-opt-out [https://perma.cc/NG8Q-V2T9].

152. DEP'T OF COM., *supra* note 37, at 6.

provided by the consumer whose data is being processed.[153] These requirements generally exceed the standards enforced by the FTC in domestic Section 5 enforcement, as it generally allows the transfer of data without many limitations, as long as the entity does not misrepresent this use to consumers and gets adequate consent for the practice.[154]

The Security principle requires participants in the Data Privacy Framework to take "reasonable and appropriate" measures to mitigate the risks involved with processing personal data.[155] This approach runs parallel to the data security principles the FTC enforces under Section 5. The FTC has specifically required certain data security practices outside of any promise within a privacy policy.[156] This parallel suggests that the E.U. and FTC's approach to data security is parallel, as they agree a certain standard of data protection must exist for an organization to properly process consumer data regardless of what they promise that consumer.

Data Integrity and Purpose Limitation ensure participants in the Data Privacy Framework maintain accurate personal data and limit their use of the data to the purpose for which it is obtained.[157] It does not appear the FTC, in its domestic Section 5 enforcement, requires organizations to limit their use of data to such specific purposes. However, there is some congruence between the two regulatory frameworks where the FTC could take enforcement action against an organization for deceptive trade practices on the theory that the organization's privacy policy is too vague to properly notify a consumer of the purposes of their data use or any limits to their use of the data.[158] Moreover, the language in this Data Privacy Framework Principle to use "reasonable and appropriate measures" shows a similar method to FTC enforcement of creating baseline qualitative standards that incorporate and enforce industry norms without requiring any specific textual language detailing the requirements.[159]

Access requires members of the Data Privacy Framework to provide individuals with the right to access to the information about them and modify any information that is incorrect or improperly processed.[160] This consumer right likely is not part of the FTC "common law" of Section 5 enforcement outside of an organization's promise to provide that right in its privacy policy,

---

153. *Id.*

154. *See, e.g.*, *FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay $16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking*, FED. TRADE COMM'N (Feb. 22, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over [https://perma.cc/NBE8-73NX] (alleging Avast's data practices were deceptive for promising its products would protect consumers from online tracking while selling consumer information to third parties).

155. DEP'T OF COM., *supra* note 37, at 6.

156. Solove & Hartzog, *supra* note 34, at 661.

157. DEP'T OF COM., *supra* note 37, at 6-7.

158. Solove & Hartzog, *supra* note 34, at 659. *See* Complaint at para. 13, F.T.C. No. C-4264 (finding the download of tracking software unfair or deceptive because the license agreement did not adequately disclose the extent of the tracking).

159. Solove & Hartzog, *supra* note 34, at 661-62.

160. DEP'T OF COM., *supra* note 37, at 7.

but other American consumer protection statutes may provide a similar right. For example, the Fair Credit Reporting Act (FCRA) provision at issue in *TransUnion v. Ramirez* required the regulated entity to take reasonable steps to ensure they held accurate data about the individual.[161] As the U.S. recognizes this right of access in specific statutes, the FTC has not tried to enforce it as part of its general privacy regulations, so it is unlikely that the FTC might regard refusal of this right as inherently unfair or deceptive for all commercial entities.

Recourse, Enforcement, and Liability entail the mechanisms available to those affected when a participant in the Data Privacy Framework deviates from the Principles.[162] These Principles are improper for analysis and comparison to FTC Section 5 enforcement, as U.S. law inherently limits the FTC's enforcement ability under Section 5, and FTC Act enforcement does not provide for a private right of action for individuals to enforce the statute through litigation.[163]

3. Addressing the Potential Limitations of the Data Privacy Framework and FTC Authority

While the Data Privacy Framework contains strong core principles that the FTC should incorporate in its efforts to strengthen consumer privacy, there are some clear limitations inherent in enforcement power fundamental to the Framework. First, the Data Privacy Framework exists as a voluntary organization, so any heightened standards applied to American companies within this framework are justified by the companies' assent to the regulation. If the FTC seeks to promulgate any trade regulation rules outside of the Data Privacy Framework Principles, it is likely the FTC will need to justify the Principle on the grounds that it coheres with industry standards, norms, and best practices outside of its mere presence in the Data Privacy Framework.[164]

The solution to this issue likely exists within the Data Privacy Framework itself, since the businesses involved have agreed to follow the Principles to do business with the E.U. As a result, the Principles themselves could constitute acceptable industry standards for data processing, so it follows that the Principles are an acceptable standard to apply to businesses processing consumer data in general.

Second, the Data Privacy Framework recognizes the constitutional right of private companies that limits the ability of U.S. regulators to regulate data transfers that implicate the First Amendment.[165] The Data Privacy Framework requires organizations to defer to the First Amendment when balancing free speech and privacy interests related to a "U.S. person or

161. *See Ramirez*, 594 U.S. at 413.

162. DEP'T OF COM., *supra* note 37, at 7.

163. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51280 (Aug. 22, 2022); 15 U.S.C. § 45(b)-(n).

164. Solove & Hartzog, *supra* note 34, at 673.

165. DEP'T OF COM., *supra* note 37, at 9.

organization."[166] Under the First Amendment, a regulation that prohibits speech due to its content is unconstitutional unless the regulation is narrowly tailored to achieve a compelling state interest.[167] Applied to the context of data transfers, the Supreme Court held in *Sorrell* v. *IMS Health Inc*. that regulations barring specific entities from transferring data for specific commercial purposes can constitute an impermissible "content- and speaker-based" restriction on speech.[168] In addition, the First Amendment establishes freedom of the press, which the Supreme Court has interpreted to protect access to information in the public record such as a court proceeding.[169] Consequently, it is not impossible for the FTC to promulgate trade regulation rules based on the Data Privacy Framework Principles due to the First Amendment, but a court would likely bar the FTC's attempts to enforce the Principles in situations where the information in question was collected or processed in a manner that receives First Amendment protection.

While the First Amendment may limit certain contexts of consumer privacy regulation, a general privacy regulation would apply equally to all commercial entities covered by Section 5 and regulate the collection and processing of data for all uses by covered entities. Thus, this regulation would not constitute a content-based restriction like the Vermont law in *Sorrell* where a prohibition of data transfers for marketing purposes constituted a content-based restriction, since it prohibited the transfers for the underlying marketing purposes of the data transfer. Since the FTC can likely apply these principles as content-neutral consumer protection standards, the Data Privacy Framework Principles serve as the basis of trade regulation rules in their commercial surveillance and data security rulemaking efforts.

IV. CONCLUSION

The FTC should use its current rulemaking process on Online Commercial Surveillance to promulgate trade regulation rules based on the E.U.-U.S. Data Privacy Principles. This approach to the rulemaking process will allow the FTC to strengthen consumer privacy protections by incorporating stronger, more definite standards into its Section 5 enforcement. The presence of the principles as trade regulation rules will also facilitate better compliance by entities not already subject to the current, voluntary privacy framework, since they would now be subject to a civil penalty for a first offense.[170] In addition, the new trade regulation rules based on the Data Privacy Framework Principles would create a simpler path to compliance than unique, new rules, since many companies already participating in the program would not need to implement new compliance regimes at all.

---

166. *Id.*

167. *See* Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015).

168. Sorrell v. IMS Health Inc., 564 U.S. 552, 571 (2011) (holding a Vermont law prohibiting pharmacists from selling certain prescription information for marketing purposes constituted content-based and viewpoint-based regulation of protected commercial speech).

169. *See* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 491-92 (1989).

170. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51280 (Aug. 22, 2022).

While not all the Data Privacy Framework Principles may work through the rulemaking process, the FTC's past practice in its Section 5 enforcement suggests that it could incorporate certain practices into its new regulations. In particular, the FTC should promulgate a trade regulation rule based on a combination of the Notice, Accountability for Onward Transfer, and Purpose Limitation Principles. The FTC has shown that it can enforce a Section 5 violation for companies that insufficiently disclose their collection and use of personal data.[171] With this new standard, the FTC could make a rule that requires a notice of use in their privacy policy. Moreover, where the regulated entity's purpose or limitation of data use is not clear, the FTC could apply implied requirements of accountability for the transfer of the data and limits on the data use. Under such a theory, the FTC could find that the entity violated the trade regulation rule by unfairly or deceptively transferring personal data without accountability for its future use or using the data for an unreasonable purpose from the consumer's perspective.

171. Solove & Hartzog, *supra* note 34, at 661.