Harvard Journal of Law & Technology
Volume 37, Number 3 Symposium 2023

THE GREAT REGULATORY DODGE

Helen Nissenbaum, Katherine Strandburg** & Salomé Viljoen****

ABSTRACT

U.S. privacy law is in a renewed moment of regulatory possibility, with both Congress and the states considering sweeping consumer privacy laws. These new proposals to enact "omnibus" privacy protections could be couched as an antidote to the current U.S. privacy regime: a patchwork of sectoral privacy laws stitched atop the background of FTC consumer contract enforcement. However, this Essay maintains that a one-size-fits-all approach cannot successfully capture both privacy's value and its variability. Yet, it is clearly the case that the present-day sectoral regime in the United States suffers from significant shortcomings. These shortcomings allow behaviors that seem clearly to violate privacy to flourish, effectively gouging meaningful oversight from sectoral privacy laws. We call these "regulatory dodges." Understanding and addressing these dodges is essential to preserving the value of contextual privacy protection. We first focus on specific health (the Health Insurance Portability and Accountability Act of 1996[1] ("HIPAA")) and financial (the Gramm-Leach-Bliley Act[2] ("GLBA")) privacy regulations to elucidate two illustrative types of regulatory dodges. We then use the General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act[3] ("CCPA") (as amended by the Consumer Privacy Rights Act) to illustrate why omnibus regulation may not solve these problems. We conclude with proposals for designing more contextually sensitive, gap-free privacy law.

---

* Andrew H. & Ann R. Tisch Professor, Information Science, Director, Digital Life Initiative, Cornell Tech.

** Alfred Engelberg Professor of Law and Faculty Director, Information Law Institute, Now York University School of Law.

*** Assistant Professor of Law, Michigan Law School. The authors thank workshop participants at the DLI Seminar and the *Harvard JOLT*-UIowa IBL Symposium: Beyond the FTC for helpful comments and advice. In addition, the authors thank participants at the 2021 Privacy Scholars Conference for helpful comments on an earlier version of this Essay. Professor Strandburg acknowledges the generous support of the Filomen D. Agostino and Max B. Greenberg Research Fund. Professor Nissenbaum is grateful for research support from the John D. and Catherine T. MacArthur Foundation and the US National Science Foundation: SaTC grant CNS-1704527 and CNS-18015307. Finally, the authors thank Tom McBrien and Eddie Percarpio for invaluable research assistance.

1. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of the U.S. Code).

2. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 of the U.S. Code).

3. CAL. CIV. CODE §§ 1798.100–.199 (West 2023).

TABLE OF CONTENTS

I. INTRODUCTION

U.S. privacy law confronts a renewed moment of possibility. Following the European Union's enactment of the General Data Protection Regulation ("GDPR"),[4] numerous states are debating and enacting sweeping consumer privacy laws, with Congress considering similar proposals.[5] These new "omnibus" laws are often favorably contrasted

4. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 38–39 [hereinafter GDPR].

5. Brenna Goth & Skye Witley, *Data Privacy 'Panoply' Looms as States Move to Fill Federal Hole*, BLOOMBERG L. (Jan. 19, 2023), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X8ID0VLS000000?bna_news_filter=privacy-and-data-security#jcite [https://perma.cc/DNU8-77QQ] ("Broad privacy bills filed in eight states so far this year would, if enacted, add to laws in California, Virginia, Connecticut, Utah, and Colorado."). Omnibus or otherwise cross-contextual privacy bills being considered this congressional term include the Stop Spying Bosses Act, S. 262, 118th Cong. (2023) (Sen. Robert

with the current patchwork of sectoral privacy laws stitched atop the backdrop of the Federal Trade Commission's ("FTC's") consumer protection enforcement.[6] A one-size-fits-all omnibus approach is insufficient, however, to capture privacy's contextual variability, which is keyed not to individual preferences and "consent" but to disparate social spheres. Privacy regulation must embody contextual privacy norms that promote the functions, goals, and values of particular social domains.

Omnibus regulation alone is likely to be overly broad in some cases and overly narrow in others. Sectoral privacy regulations can complement omnibus laws by instantiating the plurality of information-sharing norms in different settings and relationships. The present U.S. sectoral regime has significant shortcomings, however, and intuitively apparent privacy violations are rampant. Companies leverage these shortcomings to dodge the spirit and letter of sectoral laws and thus violate contextual integrity. Addressing these "regulatory dodges" is essential to enhancing the efficacy of sectoral privacy protection.

As long as there has been law, some have sought to evade it. Corporate actors do so to minimize their regulatory costs and gain competitive advantage. Technologies and business practices invariably evolve in the shadow of governing legal rules.[7] We do not purport to (re)discover age-old concepts of regulatory arbitrage and evasion. Instead, we analyze how regulatory dodges emerge in a domain significantly transformed by digital technologies. This analysis can help us design better privacy laws.

Information assets are like stem cells: they can grow into a variety of commercially exploitable insights across a range of distinct commercial sectors, endowing companies with "predictive power" they can use across various settings.[8] Information companies are flexible business

---

Casey Jr.); UPHOLD Privacy Act of 2023, S. 631, 118th Cong. (2023) (Sen. Amy Klobuchar); Data Care Act of 2023, S. 744, 118th Cong. (2023) (Sen. Brian Schatz); Online Privacy Act of 2023, H.R. 2701, 118th Cong. (2023) (Rep. Anna Eshoo).

6. *See, e.g.*, Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy*, PRIV. + SEC. BLOG (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law [https://perma.cc/7RFV-8VCC] (detailing the gaps, complexities, redundancies, and inconsistencies of the sectoral approach and suggesting the United States should move to "at least a baseline omnibus privacy and data security law"); Saryu Nayyar, *Is it Time for a U.S. Version of GDPR?*, FORBES (Feb. 1, 2022), https://www.forbes.com/sites/forbestech-council/2022/02/01/is-it-time-for-a-us-version-of-gdpr [https://perma.cc/4JAW-MHMA] ("The U.S. federal government already regulates data protection and privacy on a nationwide basis, albeit only for specific industries. . . . [T]hese [sectoral] regulations, along with some of the specifics from the GDPR, are good starting points for developing an all-encompassing federal data protection and privacy law.").

7. *See* JULIE COHEN, BEYOND TRUTH AND POWER 2 (2019).

8. Katharina Pistor, *Rule by Data: The End of Markets?*, 83 L. & CONTEMP. PROBS. 101, 106 (2020); Roxana Vatanparast, *The Code of Data Capital: A Distributional Analysis of Law in the Global Data Economy*, 2021 JURIDIKUM 98, 108. For further treatment of predictive

entities; they can morph from providing advertising insights to health insurance profiles to financial services relatively seamlessly (with perhaps a strategic merger or acquisition).[9] As a result, the digital economy is particularly vulnerable to regulatory dodge.

Regulatory avoidance is also particularly troubling in the digital economy. Information and communication serve important infrastructural roles for commercial and non-commercial life. Dodges may introduce significant, network-wide competition concerns. Lax privacy rules for information infrastructures may threaten entities in other industries that rely on them. In such networked scenarios, it is difficult to trace adverse effects back to a particular instance of inappropriate flows of data. Given these challenges of opacity and structural accountability, individuals are especially reliant on effective regulation to protect them from information harm.

We first focus on specific health (the Health Insurance Portability and Accountability Act of 1996[10] ("HIPAA")) and financial (the Gramm-Leach-Bliley Act[11] ("GLBA")) privacy regulations to elucidate two illustrative types of regulatory dodge. We then use the GDPR and the California Consumer Privacy Act[12] ("CCPA") (as amended by the Consumer Privacy Rights Act) to illustrate why omnibus regulation may not solve the problems. We conclude with proposals for designing more contextually sensitive, gap-free privacy law.

II. BACKGROUND

A. Sectoral Approach

The US traditionally regulates privacy primarily sector by sector rather than with an overarching omnibus framework. The list of federal statutes provided in Solove and Schwartz's *An Overview of Privacy*

---

power, see Amanda Parsons & Salomé Viljoen, *Valuing Social Data*, COLUM. L. REV. (forthcoming 2024) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4513235 [https://perma.cc/ABY9-YSMR].

9. Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 589 (2021). For example, consider Meta's rollout of Meta Pay, a bid to leverage Meta's social media information to provide superior payments services, and vice versa. *Meta Pay*, META, https://pay.facebook.com [https://perma.cc/7KVE-R36D]. Or consider Alphabet subsidiary FitBit's partnership with United HealthCare to share activity data with the insurance company. Andrew Boyd, *Could Your Fitbit Data Be Used to Deny You Health Insurance?*, CONVERSATION (Feb. 16, 2017), https://theconversation.com/could-your-fitbit-data-be-used-to-deny-you-health-insurance-72565 [https://perma.cc/CU9L-L8M8].

10. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of the U.S. Code).

11. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 of the U.S. Code).

12. CAL. CIV. CODE §§ 1798.100–.199 (West 2023).

Law exposes the sectoral mosaic.[13] Some sectors have received considerable regulatory attention. The financial sector, for example, has attracted repeated legislation, such as the Fair Credit Reporting Act of 1970,[14] Bank Secrecy Act of 1970,[15] Right to Financial Privacy Act of 1978,[16] and the GLBA. Two federal statutes regulate health privacy: HIPAA and the Health Information Technology for Economic and Clinical Health Act of 2009, which are implemented in the HIPAA Privacy Rule.[17]

The lacuna in federal regulation is obvious: sectoral statutes miss a large swath of consumer data handled by innumerable companies, small and large. Some companies provide digital services directly to consumers. Others collect data while providing physical services or products. Still others, including data brokers, provide back-end services to consumer-facing companies. These kinds of companies are regulated by general consumer protection laws, the most important of which has been Section 5 of the FTC Act.[18] Section 5 prohibits "unfair and deceptive trade practices,"[19] which the FTC has interpreted primarily to require companies to adhere to their posted privacy policies and public statements.[20] The result is a regime of "notice and choice," which purports to give consumers "notice" of data practices in a privacy policy and a "choice" of whether and how to engage with a company.[21] In practice, this approach has allowed privacy policies to say virtually anything and enabled companies to pursue virtually any practices that conform to those policies. Study after study demonstrates that individuals are largely unable to negotiate, or even comprehend, privacy

13. DANIEL SOLOVE & PAUL SCHWARTZ, *An Overview of Privacy Law*, *in* PRIVACY LAW FUNDAMENTALS 1, 4–6 (2015).

14. 15 U.S.C. §§ 1681–1681x (2021).

15. Pub. L. No. 91-508, 84 Stat. 1114 (1970).

16. 12 U.S.C. §§ 3401–3423 (2020).

17. Pub. L. No. 104-191, 110 Stat. 1936 (1996); 45 C.F.R. §§ 164.500–.534 (2022) (implementing HIPAA).

18. 15 U.S.C. § 45(a)(1) (2021).

19. *Id.*

20. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 60–64 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/VE9B-7H5N]; Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405, 432 (2010).

21. Woodrow Hartzog & Neil Richards, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1197–98 (2017) (reviewing FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015)); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016); Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529 *passim* (2007); Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE. L. REV. 310, 329–31 (2020); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883–85 (2013).

policies.[22] As a result, given the FTC's limited enforcement resources, the vast array of actors not covered by sectoral privacy law has been virtually immune from federal regulation.

One response to gaps between sectoral privacy regulations and the notice and choice backstop has been to enact omnibus privacy laws that are, in theory, more broadly scoped than sectoral laws and stronger than notice and choice. In the ongoing debate about sectoral versus omnibus approaches, sectoral regulation supporters cite the importance of specific tailoring to the actors, information, and distinctive activities characterizing different sectors.[23] Omnibus regulation supporters counter that a sectoral approach is piecemeal and gap-filled, while only an omnibus approach can establish privacy protection as the default.[24]

Acknowledging the merits on both sides, we consider how to avoid both sorts of failings in designing privacy regulation. We agree wholeheartedly that privacy law must be contextual, but U.S. sectoral privacy law is severely challenged by what we call "the great regulatory dodge." Here, we describe the dodge, explain why it is problematic, and outline ways to design regulation that foils it. We argue that recent omnibus laws are insufficiently contextual while remaining overly reliant on notice and choice. Our concluding proposals favor a privacy regime with strong general standards for the form and substance of contextually appropriate information flows while encouraging sector-specific rules based on those standards.

B. Privacy as Contextual Integrity

Drawing on social theory, social philosophy, and law, Contextual Integrity Theory ("CI") conceives of social life as comprising distinct social domains ("contexts") such as commerce, education, finance, healthcare, civic life, family, and friends.[25] The defining features of a CI context are its ends, aims, or goals, which determine its contribution to society at large. Contexts also incorporate broader values, such as

22. Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL. F. 95, 143; Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO. COMMC'N & SOC'Y 128, 140–42 (2020); *see also* Solove, *supra* note 21, at 1883–86.

23. WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 549 (2016); PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 177 (1998); Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy,* 87 CALIF. L. REV. 751, 756–57 (1999) (reviewing PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996) and PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998)).

24. *See* Solove, *supra* note 6.

25. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 130–32 (2010).

equality, justice, or individual autonomy. For example, healthcare may be oriented around curing disease, alleviating pain, and preventing illness, and be committed to values of equity and patient autonomy. The precise composition of ends and values may differ from society to society and be controversial and contested *within* societies. For example, individuals might disagree about whether the goals of education are to enlighten or train, to teach rote skills or encourage creativity, or to generate workers or produce good citizens.

In a departure from predominant definitions of privacy as information control or secrecy, CI conceives of privacy as *appropriate* flow of information, meaning flow that conforms with contextual privacy norms.[26] Contextual privacy norms define acceptable data practices and may range from implicit and weak (e.g., social disapproval of friends betraying confidences) to explicit and embodied (e.g., professional rules protecting journalists refusing to name sources or requiring physicians to maintain confidentiality of health data). A complete statement of a contextual privacy norm provides values for five parameters: data subject, data sender, data recipient, information type (topic, attribute), and transmission principle.[27]

Actors (i.e., data subjects, data senders, and data recipients) are labeled according to contextual capacities or roles, such as physician, nurse, lab technician, biomedical researcher, or health insurance company in a healthcare context. Information types are labeled according to contextual ontologies, which may include symptoms, diagnoses, pathogens, or medication, in a contemporary healthcare context. Transmission principles are the conditions, or constraints, under which data about subjects flows from senders to recipients. Consent is just one such principle. Others include requirement, confidentiality, reciprocity, or, familiar to lawyers, "with a warrant." A rule based only on whether data is "sensitive" or only on whether a subject has consented is not only ambiguous and incomplete but is unlikely to hold true across all social contexts. Following the CI schema, the appropriateness of an information flow depends on all five parameters.

To remain relevant in a world characterized by unjust social relations and rapidly changing technologies, a normative conception of privacy must be able to adjust, neither simply bowing to disruptive flows nor digging in its heels despite disruption. CI's approach to evaluating informational norms and disruptive data practices is applicable to entrenched norms (e.g., rules and laws) or disruptive information practices. It probes: (1) whose interests are affected and how; (2) how contextual goals, purposes, and values are affected; and (3) how

26. We use the terms "information" and "data" interchangeably.
27. NISSENBAUM, *supra* note 25, at 140–47.

societal values, including fundamental liberties and rights, are affected.[28] CI thus explicitly highlights the critical relationship between information flows and contextual ends. While privacy is almost always seen as an individual interest, to be balanced against other interests, CI adopts the idea, introduced by Priscilla Regan, that privacy is a societal value.[29] In practice, the appropriateness of particular information flows often must be interpreted through legitimate governance institutions, both formal and informal.[30]

This discussion explains why a simplistic omnibus approach is unsatisfactory, potentially squandering privacy's regulatory moment on a regime that poorly fits the complex social relations that information flows reflect and enact. While omnibus laws attempt to import flexibility through notice and consent, that approach is unworkable in the modern world where it is impossible for individual data subjects to meaningfully assess the choices they are presented with. Equally important, a consent-based approach is normatively indefensible because it neglects privacy's societal role in promoting contextual functions, ends, and values; addressing collective action problems (e.g., public health); or addressing the interests of disfavored minorities.[31] This critique suggests the merits of the US sectoral vision. However, as we discuss below, sectoral laws are vulnerable to "dodges," in which information flows that implicate contextual goals and values escape regulation as a result of regulatory design flaws.

III. WHAT IS A DODGE?

We define a "regulatory dodge" to mean the use of legal affordances (in combination with technical means and corporate structures) to circumvent the spirit or letter of existing sectoral privacy regulation. We explore the anatomy of two types of "dodges" — "scoping" and "exceptions" dodges — illustrating them with case studies drawn from different sectors, healthcare and finance, regulated by different sectoral privacy laws. There are undoubtedly other categories of dodges that could be examined, but we believe these are both important and exemplary.

"Scoping dodges" exempt companies from regulations that seemingly ought to apply to them because their activities are similar to those of covered entities. Scoping dodges often arise when laws "scope" their

28. *Id.* at 10–11.

29. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 225 (1995).

30. Madelyn Rose Sanfilippo, Brett M. Frischmann & Katherine J. Strandburg, *Privacy and Knowledge Commons*, *in* GOVERNING PRIVACY IN KNOWLEDGE COMMONS 5, 5, 12–13 (Madelyn Rose Sanfilippo, Brett M. Frischmann & Katherine J. Strandburg, eds. 2021); Viljoen, *supra* note 9, at 610–11.

31. ANITA L. ALLEN, UNPOPULAR PRIVACY 99–121 (2011).

obligations around certain actor types, taking them to be reliable proxies for the activities that deserve regulation. Scoping dodges may be unanticipated at the time of drafting and emerge later due to social, institutional, and technological upheaval, when traditional roles are disassociated from relevant activities, as illustrated here in the healthcare context. Scoping dodges violate contextual integrity by regulating only some of the activities triggering similar privacy concerns in the targeted sector.

"Exception dodges" occur when companies covered by a privacy law focus on activities that come within exceptions to the law's obligations. While such legal exceptions are intentional, they become "dodges" when they produce unanticipated and undesired loopholes and distortions. Relevant activities may evolve over time or may be intentionally designed to fit within an exception. Exception dodges can distort business activities, sometimes to the point where the exception essentially swallows the rule, as we discuss below using a case study from the financial sector.

IV. FERTILITY APPS AND THE SCOPING DODGE

Downloaded by millions[32] and touted as the number one mobile product for women's health, fertility apps would seem to be good candidates for coverage by a sectoral law such as HIPAA. Yet, unless used under a doctor's supervision, they are primarily governed like other commercial mobile apps, not health services.[33] "Covered entities" under HIPAA's Privacy Rule include healthcare providers and those who provide direct services to these healthcare providers, as well as insurance companies.[34] Certain "business associates" are also subject to HIPAA regulation,[35] but health-related apps that operate direct-to-consumer escape HIPAA's coverage; as a result, at the federal level, fertility app privacy is regulated primarily by the FTC's enforcement of Section 5's ban on "unfair and deceptive trade practices."[36] This

32. *See* number of downloads detailed *infra* note 37.

33. The FTC governs commercial mobile apps under its Section 5 consumer protection authority. *See supra* note 18 and accompanying text.

34. *See* 45 C.F.R. § 160.103 (2020) (defining "covered entity").

35. *See id.*

36. *See* 15 U.S.C. § 45(a)(1) (2021). The FTC has begun to use an expansive interpretation of its Health Data Breach Notification Rule to impose fines on health app companies for not only data security incidents (as the Rule was traditionally used) but to also include unauthorized disclosures of personal health information. *See* Press Release, Fed. Trade Comm'n, FTC Warns Health Apps and Connected Device Companies to Comply with Health Breach Notification Rule (Sept. 15, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health-breach-notification-rule [https://perma.cc/4DNM-DHN2]; *see also* Jordan T. Cohen, Elizabeth F. Hodge & Lauren F. Gandle, *Health Apps Beware: FTC Clarifies Health Breach Notification Rule With*

unfortunate escape from legitimate sector-specific privacy regulation is a scoping dodge.

A. Fertility Apps

Some of the most popular fertility apps include Glow, Ovia, Flo, and Clue.[37] These apps market themselves as offering users greater access to, control over, and accuracy of prediction related to their fertility.[38] The apps offer a range of health and fertility-related services as well as different business models. Clue, for example, is available in both free and subscription (paid) versions, but emphasizes its non-freemium business model and their German location (i.e., subject to EU privacy law) as evidence of the company's credible commitment not to monetize or disclose user data.[39] Both Glow and Ovia Health go beyond period tracking to offer pregnancy and early parenting services.[40] Flo even tracks menopause.[41] Ovia offers its apps directly to consumers, but also has partnerships with employment benefits plans.[42] Partnership beneficiaries can sign in with their plan information to access premium tools and features including health coaching, personalized benefits

Significant Proposed Changes, LEXOLOGY (June 9, 2023), https://www.lexology.com/library/detail.aspx?g=60a3135c-9d25-45af-b03a-e505b6fca049 [https://perma.cc/R8P6-JMBX] (discussing the impact of the FTC's new enforcement strategies).

37. Glow claims over twenty-five million users worldwide. GLOW, https://glowing.com [https://perma.cc/U78Y-PYEM]; Ovia claims a community of over fifteen million users. *Ovia: Fertility, Cycle, Health,* APPLE APP STORE, https://apps.apple.com/us/app/ovia-fertility-cycle-health/id570244389 [https://perma.cc/T72N-YCHY]. Flo bills itself as the top period and ovulation tracker worldwide with over 250 million users. FLO, https://flo.health [https://perma.cc/Q2XF-KWRD]. Clue claims eleven million monthly active users. CLUE, https://helloclue.com [https://perma.cc/6QSX-JJDB].

38. Clue offers users a way to "live in sync with [their] cycle," CLUE, https://helloclue.com [https://perma.cc/6QSX-JJDB]; Flo states that one reason "millions of women are using Flo" is for its "accurate predictions," FLO, https://flo.health [https://perma.cc/Q2XF-KWRD]; Ovia Health promotes its algorithm as the "most accurate ovulation tracker and fertility tracker," claiming accurate predictions even for "women with irregular periods trying to conceive," *Ovia: Fertility, Cycle Health*, GOOGLE PLAY (July 18, 2023), https://play.google.com/store/apps/details?id=com.ovuline.fertility [https://perma.cc/5R5J-YW73]; Glow offers users a way to "take control" of their reproductive health, *Glow: AI Fertility Ovulation Tracker*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.glow.android [https://perma.cc/3WWG-86L7].

39. Audrey Tsang & Carrie Walter, *One Year Post-Roe: This Is What We Want Clue Users to Know*, CLUE (June 21, 2023), https://helloclue.com/articles/about-clue/one-year-post-roe-this-is-what-we-want-clue-users-to-know [https://perma.cc/U825-XVYF].

40. *Individuals*, OVIA HEALTH, https://www.oviahealth.com/apps [https://perma.cc/8ESE-BHK7]; GLOW, https://glowing.com [https://perma.cc/U78Y-PYEM].

41. *What is Flo?*, FLO, https://help.flo.health/hc/en-us/articles/4406825500052-What-is-Flo [https://perma.cc/LKG4-QAQ2] ("Flo is an AI-powered health app that supports women during their entire reproductive lives — from first menstruation to menopause.").

42. *Individuals*, OVIA HEALTH, https://www.oviahealth.com/apps [https://perma.cc/8ESE-BHK7]; GLOW, https://glowing.com [https://perma.cc/U78Y-PYEM].

content, and programs covering birth control tracking, endometriosis education, personalized health programs, and one-on-one coaching.[43]

Fertility apps can collect rather detailed and extensive data related to menstruation and female fertility. Apps allow users to track their cycles, weight, basal body temperature, cervical fluid changes, and results of ovulation and pregnancy tests.[44] They can track symptoms over time, such as head or body aches, daily moods or mood changes, sleeping patterns, energy levels, sex drive, and food cravings.[45] Some apps integrate with wearables, so users can sync app data with wearable-collected data on weight, sleep, and physical activity.[46] Glow, which covers pregnancy and early parenthood, can collect data on fetal development and newborn developmental milestones, breastfeeding habits and timing, and diaper changes.[47]

B. Fertility Apps and HIPAA

Given fertility apps' functions and how they are promoted, U.S. users might expect them to be governed by HIPAA's Privacy Rule, the primary federal law governing healthcare data. Instead, direct-to-consumer fertility tracking is primarily regulated under the FTC's Section 5 authority, though HIPAA may apply to usage under physician supervision or in partnership with an insurer.[48] For direct-to-consumer markets, these companies' privacy policies are virtually indistinguishable from those of myriad other consumer apps. This unfortunate gap in HIPAA's coverage results from its design.

HIPAA was intended to facilitate the use and portability of electronic health records. Congress directed the Department of Health and Human Services to promulgate privacy regulations because effective medical treatment depends on people's trust, and the "proliferation of electronic records" had increased the risk of unauthorized disclosures.[49] The resulting HIPAA Privacy Rule protects personal health

---

43. *Id.*

44. *See, e.g.*, *Ovia: Fertility, Cycle, Health*, *supra* note 37; *Flo Period & Pregnancy Tracker*, APPLE APP STORE, https://apps.apple.com/us/app/flo-period-pregnancy-tracker/id1038369065 [https://perma.cc/P22G-K7MU].

45. *Ovia: Fertility, Cycle, Health*, *supra* note 37; *Flo Period & Pregnancy Tracker*, *supra* note 44.

46. *Glow*, APPLE APP STORE, https://apps.apple.com/developer/glow/id734913506?l=en [https://perma.cc/2W8T-PBBR].

47. *Glow Baby: AI Newborn Tracker*, APPLE APP STORE, https://apps.apple.com/us/app/glow-baby-ai-newborn-tracker/id1077177456 [https://perma.cc/QFT8-VDND].

48. For example, HIPAA regulations may apply in the context of Ovia's partnership program. *See Partners*, OVIA HEALTH, https://www.oviahealth.com/channel-partners [https://perma.cc/WL3Y-GS72].

49. Morgan Leigh Tendam, Note, *The HIPAA-Pota-Mess: How HIPAA's Weak Enforcement Standards Have Led States to Create Confusing Medical Privacy Remedies*, 79 OHIO ST. L.J. 411, 413 (2018).

information ("PHI"), defined as any health status, treatment, or healthcare payment information that can be linked to an individual.[50] The Privacy Rule regulates the use and disclosure of PHI and establishes several patients' rights over health information.[51] With a few contextually defined exceptions, sharing PHI requires written consent from the patient and is governed by data minimization requirements.[52]

HIPAA's scope is limited, however. The Privacy Rule applies to "covered entities"[53] and to "business associates."[54] "Covered entities" include health plans, health care clearinghouses, and any "health care provider who transmits any health information in electronic form in connection with a [covered] transaction," meaning "financial or administrative activities related to health care."[55] "Health care provider" includes any "person or organization who furnishes, bills, or is paid for health care in the normal course of business."[56] "Health care" includes "care, services, or supplies related to the health of an individual."[57] The vast majority of doctors and hospitals are thus "covered entities." While fertility app companies arguably meet the definition of health care provider, they generally do not transmit PHI in connection with covered transactions.[58] Fertility app companies, possibly excepting those that partner with covered entities, escape the definitional clutches of both "covered entity" and "business associate." The resulting scoping dodge emerges from HIPAA's implicit assumptions about roles and information flows in the healthcare context.

C. The FTC's Health Data Breach Notification Rule

The American Recovery and Reinvestment Act of 2009[59] ("ARRA") "recognize[d] that there are new types of Web-based entities that collect or handle consumers' sensitive health information . . . [including] applications through which consumers can track and

50. 45 C.F.R. § 160.103 (2020).

51. *See* ROBERT BELFORT, WILLIAM S. BERNSTEIN, ALEX DWORKOWITZ, BRENDA PAWLAK & PO YI, A SHARED RESPONSIBILITY: PROTECTING CONSUMER HEALTH DATA PRIVACY IN AN INCREASINGLY CONNECTED WORLD 7 (2020).

52. Covered entities may disclose PHI without consent to facilitate treatment or payment or conduct healthcare operations, with law enforcement as required by law, and to comply with administrative agency requests. They may disclose limited PHI in hospital directories and for a few similar purposes unless patients object. 45 C.F.R. § 164.502 (2020).

53. 45 C.F.R. § 160.103 (2022).

54. *Id.*

55. *Id.*

56. *Id.*

57. *Id.*

58. *See* Hannah Norman & Victoria Knight, *Should You Worry About Data From Your Period-Tracking App Being Used Against You?*, KFF HEALTH NEWS (May 13, 2022), https://kffhealthnews.org/news/article/period-tracking-apps-data-privacy [https://perma.cc/TJ4A-CHLG]; see also *supra* note 55 and accompanying text.

59. Pub. L. No. 111-5, 123 Stat. 115 (2009).

manage . . . personal health records."[60] ARRA required the FTC to issue a temporary data breach notification rule covering such entities.[61] The FTC noted the gap created because "entities offering these types of services are not subject to the privacy and security requirements of" HIPAA[62] and promptly promulgated the Health Breach Notification Rule ("HBNR").[63] The broader regulatory enterprise then stalled, and the HBNR was essentially dormant.[64]

Recently, and controversially, the FTC has begun to enforce the HBNR expansively against health app companies.[65] While breach

60. Press Release, Fed. Trade Comm'n, FTC Publishes Proposed Breach Notification Rule for Electronic Health Information (Apr. 16, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/04/ftc-publishes-proposed-breach-notification-rule-electronic-health-information [https://perma.cc/KL5Z-22DH].

61. 16 C.F.R. pt. 318 (2022).

62. Press Release, Fed. Trade Comm'n, FTC Issues Final Breach Notification Rule for Electronic Health Information (Aug. 17, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/08/ftc-issues-final-breach-notification-rule-electronic-health-information [https://perma.cc/X8KZ-V9JN].

63. 16 C.F.R. pt. 318 (2020).

64. See Libbie Canter, Anna D. Kraus & Olivia Vega, *FTC Announces First Enforcement Action Under Health Breach Notification Rule*, INSIDE PRIV. (Feb. 2, 2023), https://www.insideprivacy.com/digital-health/ftc-announces-first-enforcement-action-under-health-breach-notification-rule [https://perma.cc/U8R4-ZQCW].

65. FTC has brought actions against GoodRx, a prescription service, and Easy Healthcare, the developer of another fertility app, for violating the HBNR by impermissibly sharing health data with advertisers. Complaint for Permanent Injunction, Civil Penalty Judgment, and Other Relief at 2–4, United States v. Easy Healthcare Corp., No. 23-cv-3107 (N.D. Ill. May 17, 2023); Press Release, Fed. Trade Comm'n, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising [https://perma.cc/66PX-WQLL]. These enforcement actions followed the FTC's September 2021 Policy Statement, which clarified that health apps fall within the scope of HBNR. *See infra* note 66. Yet the decision to bring these actions as violations of the HBNR has proven controversial. Dissenting Commissioner Christine Wilson complained that, "Rather than 'clarifying' the scope of the Rule, this Policy Statement in fact expands it – while contradicting existing FTC business guidance." CHRISTINE S. WILSON, DISSENTING STATEMENT OF COMMISSIONER CHRISTINE S. WILSON, POLICY STATEMENT ON BREACHES BY HEALTH APPS AND OTHER CONNECTED DEVICES 1 (2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/dissenting-statement-commissioner-christine-s-wilson-regarding-policy-statement-breaches-health-apps [https://perma.cc/P4F5-CX38]. Dissenting Commissioner Noah Phillips called the Policy Statement a "Rube Goldberg interpretation" both with respect to its treatment of health apps as "health care providers" and as to its expansive interpretation of "breach of security." NOAH J. PHILLIPS, DISSENTING STATEMENT OF COMMISSIONER NOAH JOSHUA PHILLIPS REGARDING THE POLICY STATEMENT ON BREACHES BY HEALTH APPS AND OTHER CONNECTED DEVICES 2–3 (2021), https://www.ftc.gov/system/files/documents/public_statements/1596328/hbnr_dissent_final_formatted.pdf [https://perma.cc/HGZ9-34ZY]. Perhaps recognizing the boldness of its interpretation, the FTC recently issued a notice of proposed changes to the HBNR. *See* FTC Health Breach Notification Rule, 88 Fed. Reg. 37819, 37822 (proposed June 9, 2023) (to be codified as amended at 16 C.F.R. pt. 318). And in its latest action against BetterHelp, a mental health service, the FTC did not include a count for violations of the HBNR for similar acts of sharing health information. Complaint at 17–19, BetterHelp, Inc., FTC Docket No. C-4796 (Mar. 2, 2023).

notification laws may ordinarily target "cybersecurity intrusions or nefarious behavior,"[66] the HBNR defines "breach of security" as any "acquisition of [personal health record] information without the authorization of the individual."[67] The FTC interprets this definition expansively, stating that a "breach of security" occurs when a health app "discloses sensitive health information without users' authorization."[68] Assuming the FTC's interpretation stands, however, the HBNR's "notification" remedy remains weak tea compared to HIPAA's more robust (if sometimes criticized) protection.

D. Privacy Policies and Fertility Apps

Fertility app companies' stated policies show sensitivity to privacy concerns. For example, Clue's co-founder wrote that "we do not want to build a business model that relies on sharing our users' attention or personal data with third parties" and that Clue's business model would be based on a paid premium version of its apps.[69] Clue "share[s] a minimal amount of data about our users with advertising networks (but we never share the menstrual or other health data you track in the app)" and allows users to opt out of "*any* data being shared for ad optimization."[70] Glow offers users the option to "[d]elete [their] 'Key Health Data' from [Clue's] servers[] but keep it on [their] personal device."[71] Some companies' websites have at times declared that their apps are voluntarily HIPAA compliant.[72]

Nonetheless, fertility tracking companies have often asserted strong rights to user data. Ovia's terms of use at one time granted the

---

66. FED. TRADE COMM'N, STATEMENT OF THE COMMISSION ON BREACHES BY HEALTH APPS AND OTHER CONNECTED DEVICES 1–2 (2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf [https://perma.cc/F8LS-CFD3] [hereinafter FTC POLICY STATEMENT] ("[T]he Commission reminds entities offering services covered by the Rule that a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule.").

67. 16 C.F.R. § 318.2 (2022).

68. FTC POLICY STATEMENT, *supra* note 66.

69. Ida Tin, *Making Money at Clue: Our Principles and Promises*, CLUE (July 16, 2018), https://helloclue.com/articles/about-clue/making-money-at-clue-our-principles-and-promises [https://perma.cc/SF47-82G8].

70. *Clue Privacy Policy*, CLUE (May 11, 2023), https://helloclue.com/privacy [https://perma.cc/Y4Y5-Q8YF].

71. *Glow Privacy Policy*, GLOW (June 17, 2023), https://glowing.com/privacy#your-choices [https://perma.cc/35JY-84Q9].

72. Erin Jones, *No, Health Data From Most Period-Tracking Apps is Not Protected Under HIPAA*, VERIFY (June 24, 2022), https://www.verifythis.com/article/news/verify/health-verify/period-tracking-apps-hipaa-privacy-rules-law-fact-check/536-bf44e08c-cc5f-4ee8-997a-c15e0060081a [https://perma.cc/9X66-N5GY] (Pam Dixon of the World Privacy Forum describes claims of HIPAA compliance as a "big red flag" that is a "meaningless phrase" for apps that are not covered entities).

company a royalty-free, perpetual, and irrevocable license to "utilize and exploit" de-identified personal information for scientific research and "external and internal marketing purposes" and to "sell, lease or lend aggregated Personal Information to third parties."[73] Like other entities, fertility app companies often include the same sort of vague, ambiguous, and even self-contradictory language in their privacy policies and terms of use. Glow claimed at one point that "[w]e do not sell or rent your personal data to third parties" and "[w]e do not profit from your personal information and do not share your information with advertisers" while also explaining that "[w]e may share your personal information as necessary . . . to tell you about products and services of interest to you."[74]

These companies also have not always abided by their lofty promises. In 2021, Flo Health settled FTC allegations that its app shared health information with third parties (including Facebook and Google analytics, AppsFlyer, and Flurry) after promising to keep such data private and only use it to provide services.[75] Similarly, Glow settled a complaint brought by the California Attorney General alleging violations of various California laws by failing to comply with its privacy policy.[76]

Most importantly, FTC privacy policy enforcement is at best a notice-and-choice regulatory regime. There is now a clear consensus among privacy experts and advocates that this approach fails on multiple fronts.[77] Moreover, while we may admire Ovia for voluntarily complying with HIPAA, Glow for offering the key health data deletion feature, and Clue for designing its business model not to rely on selling user data, such promises are unilateral and may be revoked at any time — with notice, of course.[78] Even the FTC's approach to the HBNR

---

73. Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?*, WASH. POST (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think [https://perma.cc/6Q5N-KM2E].

74. *Glow Privacy Policy*, GLOW (Mar. 31, 2020), https://glowing.com/privacy-20200331 [https://perma.cc/JQK6-5VMT]. Note that the language of these companies' privacy policies and terms of use changes frequently. Indeed, there were major changes during the writing of this Essay.

75. Complaint at 1–2, Flo Health, FTC Docket No. C-4747 (June 17, 2021); Decision and Order at 1, Flo Health, FTC Docket No. C4747 (FTC June 17, 2021) (memorializing the terms of the settlement).

76. Alex Pearce, *The California Attorney General's Settlement with Glow: A Wake-Up Call for Consumer Health App Developers*, JD SUPRA (Sept. 30, 2020), https://www.jdsupra.com/legalnews/the-california-attorney-general-s-71808 [https://perma.cc/AW8X-RE5V].

77. See *supra* note 22 for a sampling of the consensus empirical and normative views.

78. In fact, the FTC has found that companies can at times invoke HIPAA compliance to put consumers at ease in ways that the FTC alleges is deceptive. *See* Complaint at 14, BetterHelp, Inc., FTC Docket No. C-4796 (Mar. 2, 2023). An important exception here may be

requires only that app companies obtain user consent before sharing health data — another incarnation of notice and choice.[79]

Treating fertility apps as akin to other commercial apps is a scoping dodge. It misassigns new forms of healthcare services to an unsuitable privacy regime and misleads individuals who would expect a more contextually appropriate regime. While health tracking apps may also be constrained by omnibus consumer protection or health-specific state laws, there is no principled reason not to subject them to contextually appropriate health privacy regulation at the federal level.

E. Through a Contextual Integrity Lens

The term "scoping dodge" carries a normative judgment: fertility apps have escaped federal sectoral regulation when, in our view, it should cover them. Fertility app companies inhabit the healthcare context because they absorb and generate data substantively similar to that absorbed and generated within traditional healthcare settings; promote their expert services as the basis for clinical insights and healthcare decisions; and are in an asymmetric relationship with users analogous to that between healthcare provider and patient.

As noted, fertility apps collect wide-ranging biological and physiological data as well as health-related behavioral data.[80] At the same time, they tout their sophisticated methods for deriving insights from this data, in a manner that is similar to the practices of traditional healthcare providers, who collect and use information about patients'

Clue, which is based in Germany. Thiago, *What Is the GDPR and How Does It Affect Me?*, CLUE SUPPORT (Nov. 21, 2023, 7:35 AM), https://support.helloclue.com/hc/en-us/articles/360000751643-What-is-the-GDPR-and-how-does-it-affect-me [https://perma.cc/VBC9-TNDA]. Under the GDPR, Clue would likely not be able to simply unilaterally begin selling access to customer data, even if it did provide notice of its proposed plan to change its business model. Under the GDPR, mere notice of a changed policy is not sufficient. Freely given, specific, informed, and unambiguous consent must be given. GDPR art. 7, rec. 32 (detailing that processing personal data is generally prohibited, unless expressly allowed by law or the data subject consents to the processing).

79. The GoodRx complaint heavily emphasizes the company's failure to abide by its privacy promises, though it does include counts based on Section 5 of the FTC Act. *See* Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 20–26, United States v. GoodRx Holdings, Inc., No. 23-cv-460 (N.D. Cal. Feb. 1, 2023). In the case of BetterHelp, the FTC's proposed order bans the service from sharing health data for advertising purposes (with no consent loophole) and requires the company to pay $7.8 million to consumers whose health data had been shared with advertisers. BetterHelp, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 88 Fed. Reg. 15717, 15719 (Mar. 14, 2023); Press Release, Fed. Trade Comm'n, FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising (Mar. 2, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook [https://perma.cc/5SF5-JF5U].

80. *See supra* Sections IV.A–B.

physical condition for the purposes of analyzing their health status.[81] Flo boasts of using more than seventy fields of user data to derive "precise" AI-driven period and ovulation predictions.[82] Ovia advertises its algorithm's capacity to provide accurate ovulation and menstrual predictions while offering health coaching.[83] Glow describes itself as a form of "modern care" for fertility.[84]

Power asymmetries, based on differential levels of knowledge and expertise, mark physician-patient relationships. These imbalances have long motivated confidentiality obligations, from ancient texts such as the Hippocratic Oath to contemporary standards reflected in the HIPAA Privacy Rule. Fertility app companies stand in a similarly asymmetric relationship with users, who are acutely vulnerable to harm from inappropriate uses and dissemination of fertility-related data and inferences. Fertility data carries enormous personal and cultural significance. Early-stage fertility marks a moment of unique vulnerability. Not only do the vast majority of miscarriages happen during the first trimester,[85] but post-*Dobbs v. Jackson Women's Health Organization*,[86] this period corresponds to people's (drastically shrinking) window to legally terminate their pregnancies.[87] Inappropriate flows of fertility data can not only produce significant social and cultural stigma but also material risk from limits on employment or insurance opportunities as well as significant legal risk in a post-*Dobbs* world. Post-*Dobbs*, the risk of health data being used in some states to prosecute those suspected of terminating a pregnancy must be added to the litany of concerns.[88]

Fertility app services are part of the healthcare context. Regulating them like garden-variety commercial apps is unlikely to be contextually appropriate or sufficiently protective. Moreover, fertility app companies and the platforms that host them may be unconstrained by professional healthcare norms. Because early insight into when people may be pregnant is both intimate and commercially valuable, contextually

---

81. *See id.*

82. *See id.*

83. *See id.*

84. *See id.*

85. EMILY OSTER, EXPECTING BETTER 28 (2021) ("Pregnancy loss is very, very common [in the first 5 weeks]."); *id.* at 73–74 (describing how "[t]his rate declines quickly over the course of the first trimester, falling to between 1 and 2 percent by 12 weeks").

86. 597 U.S. 215 (2022).

87. Christine Hennenberg, *The Trade-Offs for Privacy in a Post*-Dobbs *Era*, WIRED (June 5, 2023), https://www.wired.com/story/the-trade-offs-for-privacy-in-a-post-dobbs-era [https://perma.cc/4X9W-WF93].

88. Margi Murphy, *Anti-Abortion Firms Lure Pregnant Teens Online, Save Their Data,* BLOOMBERG L., (June 27, 2022, 10:00 AM), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X2Q3CFFS000000?bna_news_filter=privacy-and-data-security#jcite [https://perma.cc/S9SL-CSAB]; Martin Kaste, *Nebraska Cops Used Facebook Messages to Investigate an Alleged Illegal Abortion*, NPR (Aug. 12, 2022), https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion [https://perma.cc/WY7G-7M87].

appropriate and effective privacy regulation is crucial. Otherwise, uninformed users will be harmed, while savvy users may decide not to connect fertility tracking records with other health information records or even avoid the apps altogether. Such evasive maneuvers are opportunity costs for societal health as well as for the individuals involved.

CI prescribes privacy rules designed to produce *appropriate* flows of data, taking into consideration stakeholder interests, fundamental ethical and political values, as well as contextual ends and values. The HIPAA Privacy Rule is tailored to the healthcare context: it encourages the free flow of data needed for diagnosis and treatment by ensuring that only parties involved with those (and similarly appropriate) aims have access to health data. Above, we pointed to the reasons why fertility apps should be conceived as contextual actors in healthcare and bound by contextual norms: as the saying goes, "If it looks like a duck, swims like a quick, and quacks like a duck, then it is probably a duck." Although fertility apps may not exactly fit the roles of traditional "covered entities," their data practices affect the interests of users and their purposes and values in similar ways.

Details of regulatory design for fertility apps are matters for debate among experts knowledgeable about the healthcare domain. Such analysis might suggest expanding the class of HIPAA-covered entities or devising bespoke privacy rules for health app companies, as was previously done for business associates. The ramifications of these choices are too far-reaching and complex to be left to the uninformed decisions of individual app users. Ultimately, while regulators will benefit from the insights of privacy experts, the experts most critical to this endeavor are those who grasp the data flows enabled by fertility app use and can envision how those data flows affect people, healthcare systems, and societies.

HIPAA's scoping dodge affects a wide range of health-related apps, perhaps most notoriously mental health apps.[89] For example, researchers have demonstrated that educational technology vendors (learning platforms, websites, apps, and software) for primary, secondary, and tertiary education, who explicitly claim to provide educational services, follow troubling data practices.[90] These online education

89. See *supra* note 65 and accompanying text for a discussion of the recent FTC actions against several healthcare apps.

90. *See* Elana Zeide & Helen Nissenbaum, *Learner Privacy in Massive Open Online Courses and Virtual Education*, 16 THEORY & RSCH. EDUC. 280, 291–94 (2018); Jake Chanenson, Jason Chee, Brandon Sloane, Navaneeth Rajan, Marshini Chetty, Amy Morrill et al., *Uncovering Privacy and Security Challenges in K-12 Schools*, 2023 CONF. ON HUM. FACTORS COMPUTING SYS., Apr. 2023, at § 7, https://bpb-us-w2.wpmucdn.com/voices.uchicago.edu/dist/1/2826/files/2023/02/CHI23_Chanenson_EdTech.pdf [https://perma.cc/CJ6B-8G3P]; Shaanan Cohney, Ross Teixeira, Anne Kohlbrenner, Arvind Narayanan, Mihir Kshirsagar, Yan Shvartzshnaider et al., *Virtual Classrooms and Real Harms: Remote Learning at U.S. Universities*, 17 SYMP. ON USABLE PRIV. & SEC. 653, 658 (2021), https://www.usenix.org/system/files/soups2021-cohney.pdf [https://perma.cc/DZ6S-ZSME].

vendors easily dodge the Family Educational Rights and Privacy Act, which is scoped to apply only to entities that receive Department of Education funding.[91]

V. PAYMENT APPS AND THE EXCEPTION DODGE

Payment apps, such as Venmo, Square, and Google Pay, are intermediaries to an increasing amount of highly revealing financial activity that paints a detailed picture of consumers' lives: what we earn and what, when, and where we buy. Not surprisingly, financial privacy is the subject of several federal statutes, including the GLBA. Though payment app companies are covered by the GLBA's privacy requirements, they often benefit from an "exception dodge" because contextually inappropriate information flows fall within an affiliated company exception.

A. Payment Apps

Digital payment systems facilitate payment between account holders and between consumers and businesses, and allow platforms' users to make in-system purchases. Venmo, launched in 2009, is a widely adopted payment system, handling $242 billion in transactions in 2022.[92] Square facilitates point-of-sale payment services between consumers and businesses, offering tablets and mobile phone plug-ins to facilitate card or mobile payments as well as a range of financial services to small businesses.[93] Google Pay, similar to other digital wallet and online payment platforms, allows users to make credit and debit card payments on Android devices and, with limited functionality, on iOS devices.[94] Merchants can add Google Payment services and link their rewards or loyalty programs, allowing users to store and access tickets, boarding passes, coupons, public transit cards, and even student IDs.[95]

These services also collect a great deal of data. Venmo collects transaction data, including payment sender, recipient, and a user-

91. 20 U.S.C. § 1232g(a) (2020).

92. *About Us*, VENMO, https://venmo.com/about/us [https://perma.cc/7R2N-ZXMV]; *Value of Payments Processed (TPV-Total Payment Volume) of Venmo from 1st Quarter 2017 to 2nd Quarter 2023*, STATISTA, https://www.statista.com/statistics/763617/venmo-total-payment-volume [https://perma.cc/7YTR-7FHG].

93. *About Us*, SQUARE, https://squareup.com/us/en/about [https://perma.cc/WW59-MZR6].

94. *About*, GOOGLE PAY, https://pay.google.com/about [https://perma.cc/78Y3-FV3Z].

95. *Google Pay for Business*, GOOGLE PAY, https://pay.google.com/about/business [https://perma.cc/6UZS-PRHV].

entered description of what the payment is for.[96] Square collects granular data from each transaction, including location, items purchased, purchase price, and credit card information.[97] As an intermediary, Square can assemble detailed longitudinal data on both customers and businesses across multiple Square-facilitated transactions. Square shares data with third parties for a variety of purposes, including advertising.[98] Google Pay collects registration information (e.g., credit card number, bank account number, and taxpayer ID number), information obtained from third parties (including credit bureaus and transacting parties), and transaction information (e.g., transaction date and time, parties, method of payment, and a description of goods purchased).[99] Registration information is associated with users' Google accounts, and Google Pay's privacy policy incorporates "any information listed in the Google Privacy Policy."[100]

B. Payment Apps and the GLBA

The GLBA imposes broad but shallow privacy obligations on financial institutions through its Privacy Rule, which bans the disclosure of nonpublic personal information ("NPI") to "nonaffiliated third parties" (entities outside common corporate ownership) without first providing the consumer or customer a privacy notice.[101] A GLBA-covered "financial institution" engages in activities "that are financial in nature or incidental to such financial activities, as determined by Section 4(k) of the Bank Holding Company Act of 1956."[102] Section 4(k)'s definition includes "[l]ending, exchanging, transferring, investing for

96. *Privacy Statement*, VENMO, https://venmo.com/legal/us-privacy-policy [https://perma.cc/9QE6-WQEZ].

97. *Privacy Notice for Buyer Features and Square Pay*, SQUARE, https://squareup.com/us/en/legal/general/buyer-features [https://perma.cc/UHX7-MBH2]; *Privacy Notice for Users Who Do Not Apply or Sign Up for a Square Account or Other Services*, SQUARE, https://squareup.com/us/en/legal/general/privacy-no-account [https://perma.cc/8VAN-KKHP]; *Privacy Notice for Square Sellers and Website Visitors*, SQUARE, https://squareup.com/us/en/legal/general/privacy [https://perma.cc/L76R-L9MC].

98. *Privacy Notice for Buyer Features and Square Pay*, *supra* note 97; *Privacy Notice for Users Who Do Not Apply or Sign Up for a Square Account or Other Services*, *supra* note 97; *Privacy Notice for Square Sellers and Website Visitors*, *supra* note 97.

99. *Google Payment Privacy Notice*, GOOGLE (Mar. 28, 2022), https://payments.google.com/payments/apis-secure/u/0/get_legal_document?ldo=0&ldt=privacynotice&ldl=en [https://perma.cc/U95J-PUSD].

100. *Id.* Thus, if Google's privacy policy mentions that it collects search history data subject to user permissions, that information is also covered under Google Pay's policy. This greatly expands the information covered by Google Pay's privacy policy and is a widespread and standard industry practice.

101. 15 U.S.C. §§ 6801–6809, 6821–6827 (2022); 16 C.F.R. pts. 313, 314 (2022).

102. FDIC, FDIC CONSUMER COMPLIANCE EXAMINATION MANUAL VIII-1.2 (2021) https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-1-1.pdf [https://perma.cc/28FZ-7J5Z] (discussing 15 U.S.C. § 6809(3)(A) (2021)).

others, or safeguarding money or securities."[103] The GLBA directs the relevant agency to interpret "financial activities" in light of the statute's purposes and of changes in the marketplace or in technology for delivering "financial services."[104] This purpose-driven approach means that the GLBA covers not only obvious actors such as banks, securities brokers, insurance underwriters, and finance companies, but also other entities that provide financial services.[105] While the FTC interprets the GLBA's "financial institutions" to be those "significantly engaged" in financial activities,[106] the GLBA's coverage remains quite broad; even universities have been deemed "financial institutions" because they administer federal student loan programs.[107]

The GLBA regulates the treatment of consumers' nonpublic personal information, where "consumers" are those who use a financial product or service for personal or household purposes.[108] Nonpublic personal information is information that is not publicly available or used in connection with solicitation or provision of a financial product or service.[109] According to the Consumer Financial Protection Bureau, NPI may include seemingly public personal information (such as name, phone, and address) obtained through cookies or combinations of public information in a nonpublic list.[110] Thus, a financial institution's list of depositors would be considered "nonpublic" because of the connection with the institution.

Because "financial institution" is functionally defined (i.e., around activities that are financial in nature, not a predetermined set of entities), there is little question that payment apps are covered by the

---

103. 12 U.S.C. § 1843(k)(4) (2020).

104. 15 U.S.C. § 6804(a)(1)(A) (2020).

105. Bank Holding Company Act, 12 U.S.C. §§ 1841–1852 (2021). See, in particular, 12 U.S.C. § 1843(k)(4)(A)–(E) (2021).

106. Enforcement of the GLBA Privacy Rule was subsequently transferred to the Consumer Financial Protection Bureau. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203 § 1093(4)(A), 124 Stat. 1376, 2095–97 (2010) (codified as amended at 15 U.S.C. §§ 6801–6827).

107. James W. Runcie & Ted Mitchell, *GEN-15-18 Subject: Protecting Student Information*, U.S. DEP'T OF EDUC., OFF. OF FED. STUDENT AID (July 29, 2015) ("In addition to other provisions within the SAIG Agreement, FSA requires institutions to comply with the Gramm-Leach-Bliley Act."); Ted Mitchell, *GEN-16-12 Subject: Protecting Student Information*, U.S. DEP'T OF EDUC., OFF. OF FED. STUDENT AID (July 1, 2016) ("As noted earlier, each institution's PPA includes a provision that the institution must comply with the provisions of the GLBA.").

108. "Customers," defined as those who have an ongoing business relationship with a financial institution, are owed somewhat greater obligations. 12 C.F.R. § 1016.3(e)(2) (2020).

109. CONSUMER FIN. PROT. BUREAU, GLBA PRIVACY EXAMINATION MANUAL 4 (2016), https://files.consumerfinance.gov/f/documents/102016_cfpb_GLBAExamManualUpdate.pdf [https://perma.cc/9NDH-MMYG].

110. *Id.*

GLBA's Privacy Rule and handle consumers' NPI.[111] There is no scoping dodge. Instead, problems arise from the rule's exception for affiliated companies.[112] The GLBA Privacy Rule generally prohibits financial institutions from disclosing NPI to "nonaffiliated third parties" (outside common corporate ownership) unless the institution supplies a "clear and conspicuous" privacy notice meeting certain requirements[113] and provides an opportunity to opt out of disclosure to such parties.[114] The institution must provide its privacy policy and notify consumers of their right to opt out, giving them a reasonable opportunity to do so (often thirty days), before sharing.[115] Financial institutions may disclose NPI to nonaffiliated parties *without* an opt-out opportunity only when the disclosure is necessary to effect, administer, or enforce a transaction (e.g., an audit of credit information or the administration of a rewards program)[116] or other specified, contextually appropriate purposes,[117] reminiscent of the routine disclosures permitted by HIPAA in the healthcare context.

The exception dodge arises because, as described above, the GLBA Privacy Rule only regulates NPI flowing to entities outside the corporate umbrella; it does not impose any regulatory requirements onto information flows between financial institutions and "affiliated third parties" under a common ownership umbrella.[118] Today, this exception creates a large swath of unregulated flows of NPI that has potentially profound implications for financial privacy in the shadow of market concentration.

---

111. Again, "financial institution" is broadly defined — any institution that engages in activities "that are financial in nature or incidental to such financial activities, as determined by Section 4(k) of the Bank Holding Company Act of 1956." 15 U.S.C. § 6809(3)(A) (2021). Financial institutions under that Act include the usual suspects like banks, securities brokers and dealers, finance companies, and mortgage bankers, but the Act also covers nonbank entities that provide financial services like lending, exchanging, transferring, investing, or safeguarding money or securities — even travel agents. *See* Bank Holding Company Act, 12 U.S.C. § 1841–1852 (2021). See, in particular, 15 U.S.C. § 1843(k)(4)(A)–(E) (2021). Financial services also include the "evaluation or brokerage of information that the [financial] institution collects in connection with a request or an application from a consumer for a financial product or service." FDIC, *supra* note 102. *See* Decision and Order at 5, PayPal, Inc., FTC Docket No. C-4651 (May 23, 2018) (consent order) (permanently enjoining PayPal to comply with the GLBA, thus demonstrating that mobile payment platforms are covered under the scope of the GLBA's definition of a financial institution).

112. 16 C.F.R. § 313.3(m)(1) (2022) (exempting "affiliates" from the definition of "nonaffiliated third party").

113. 16 C.F.R. § 313.6(b) (2020).

114. *Id.* § 313.10. Disclosure of certain account number information for marketing purposes is regulated more stringently. *See id.* § 313.12.

115. *Id.* §§ 313.7, 313.10(3).

116. *Id.* § 313.14(b).

117. *Id.* § 313.13 (exempting sharing of information with "a third party" who "perform[s] services for you or functions on your behalf"); *id.* § 313.15 (providing for other specific circumstances exempted from the rule).

118. *See* 15 U.S.C. § 6802(a) (2021). "Affiliate" is defined in 15 U.S.C. § 6809(6) (2021).

When enacted in 1999, GLBA primarily contemplated the activities of large traditional financial institutions.[119] The bill repealed key sections of the Glass-Steagall Act that had prohibited financial holding companies from acting as a combination of investment bank, commercial bank, and insurance company, and erected conflict-of-interest barriers against an "officer, director, or employee" of a securities firm also serving as an "officer, director, or employee" of a member bank.[120] These changes encouraged the consolidation of firms across core financial services such as investment banking, commercial banking, and insurance.[121]

Whatever one thinks of this outcome, the GLBA's enactors did not contemplate a future in which the GLBA would govern digital companies for whom producing financial transaction data and linking it with other data sources is a primary focus. The GLBA Privacy Rule's affiliated entity exception now exempts whole swathes of financial information flowing beyond the financial context.

C. Exception as Dodge

Companies benefit from an exception dodge when they can change market configuration to "shift" previously regulated data sharing activity into an exception. While the sharing may nominally fit within the exception, we call "Dodge!" when social and technological evolution has distorted an exception's coverage in problematic ways. When financial data sharing patterns shift so that major pathways fall within an exception, regulatory requirements become vestigial, appended to an exception that has swallowed the rule. Such an exception may also incentivize business strategies that exacerbate the problem.

The GLBA's exception for disclosures to affiliated third parties makes sense in the traditional banking sector that was the core concern of the law. It frees banks from having to provide notices each time financial data is transferred between affiliated corporations that provide distinct banking services. In the digital economy, however, this exception encompasses potentially inappropriate data flows extending beyond the financial context.

---

119. The law was meant to allow large financial entities to further consolidate. The GLBA followed the 1998 merger of Citicorp (a bank holding company) with Traveler Group (an insurance company) to form Citigroup — a violation of the Glass-Steagall Act that required the Federal Reserve give Citigroup a temporary waiver. Arthur E. Wilmarth, Jr., *Citigroup: A Case Study in Managerial and Regulatory Failures*, 47 IND. L. REV. 69, 71–74 (2014). The GLBA was passed the next year to legalize these kinds of mergers. LISSA BROOME & JERRY MARKHAM, THE GRAMM-LEACH-BLILEY ACT: AN OVERVIEW 1 (2001), https://web.archive.org/web/20120217055223/http://www.symtrex.com/pdfdocs/glb_paper.pdf.

120. *Id.* at 1–3; 12 U.S.C. § 78 (1998), *repealed by* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

121. *See* BROOME ET AL., *supra* note 119, at 1.

Digital financial services exist within an ecosystem of mega-mergers and concentrated service provision. Google Pay is part of Google, LLC, which is in turn part of Alphabet Inc., whose many subsidiaries include Firebase (for analytics), DoubleClick (for advertising), Waymo, Verily Life Sciences, and Google DeepMind.[122] Google Pay may share financial information with any of these entities, who may use it for "everyday business purposes,"[123] thus linking users' payment information to their other activities throughout the web and mobile ecosystems. Users' purchasing information is especially valuable to companies like Google that derive their revenue from advertising, providing insight into which advertising strategies result in purchases.

Other digital financial services also trend toward consolidation across diverse services. PayPal, for instance, owns (among others) Venmo, Xoom (which facilitates bank transfers), Honey (which gathers data on coupons), and Braintree (a data sharing toolkit that does analytics and shares payment data with third parties to improve advertising).[124] Square has several affiliates and services, including Weebly (the e-commerce version of Square), Square Financial Services (a banking subsidiary), Afterpay (an installment-payment platform), and Square Capital (small business loans and other financial services).[125]

---

122. *Firebase*, PITCHBOOK, https://pitchbook.com/profiles/company/54523-18#overview [https://perma.cc/YJZ4-79DS]; Louise Story & Miguel Helft, *Google Buys DoubleClick for $3.1 Billion*, N.Y. TIMES (Apr. 14, 2007), https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html [https://perma.cc/S49G-6WYW]; Anna Domanska, *An A to Z List of Companies Owned by Alphabet Inc.*, INDUS. LEADERS (Jan. 12, 2022), https://www.industryleadersmagazine.com/an-a-to-z-list-of-companies-owned-by-alphabet-inc/ [https://perma.cc/G26K-DASX].

123. *Google Payment Privacy Notice*, *supra* note 99.

124. In 2012, Venmo was acquired by Braintree, which had been acquired by PayPal in 2013. *PayPal Braintree*, PAYPAL, https://www.braintreepayments.com/products/braintree-extend [https://perma.cc/6388-YUPF]. PayPal settled FTC claims that Venmo's privacy settings and notices were inadequate under both FTC Act Section 5 and the GLBA's privacy provisions. Complaint at 13–15, PayPal, Inc., FTC Docket No. C-4651 (May 23, 2018) (listing the allegations against Venmo); Decision and Order at 1, PayPal, Inc., FTC Docket No. C-4651 (May 23, 2018) (memorializing the settlement agreement between PayPal and the FTC).

125. The parent company changed its name from Square to Block, Inc. in 2021. Block, Inc., Current Report Pursuant to Section 13 or 15(d) of The Securities Exchange Act of 1934 (Form 8-K) (Dec. 10, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/1512673/000119312521354007/d270905d8k.htm [https://perma.cc/G6W2-NMF5]; *Square Updates Second Quarter and Full Year 2018 Guidance*, SQUARE (June 4, 2018), https://squareup.com/us/en/press/square-updates-second-quarter-and-full-year-2018-guidance [https://perma.cc/N6L3-86B5] (announcing Square's acquisition of Weebly); *Introducing Square Banking, a Suite of Powerful Financial Tools for Small Businesses*, SQUARE (July 20, 2021), https://squareup.com/us/en/press/introducing-square-banking [https://perma.cc/75DN-S8MP] (announcing Square's banking services and its bank Square Financial Services beginning operations in March 2021); *Block, Inc. Completes Acquisition of Afterpay*, BLOCK (Jan. 31, 2022), https://investors.block.xyz/news/news-details/2022/Block-Inc.-Completes-Acquisition-of-Afterpay/default.aspx [https://perma.cc/5TRZ-MLWQ]; *Square Capital: Expanding Access*, SQUARE, https://squareup.com/us/en/capital/access [https://perma.cc/XA6S-ELXR].

Square also offers its own analytics engine for itself and for businesses using the platform.[126]

In a less concentrated economy, entities performing such disparate services would be separate, and data sharing between them would be subject to GLBA's notice and opt-out rights. The "regulation-free zone" created by the GLBA's exception for affiliated third parties encourages consolidation of disparate data-producing activities under a single corporate umbrella and allows companies to freely combine financial information with other information. Financial data generated via Google Pay, for example, may be freely combined with search history data, location data, or data generated by any other Alphabet service. This undercuts the GLBA's power to impose privacy standards for digital financial services. Even if the GLBA's affiliate exception is not a primary driver of consolidation in the technology sector, it reinforces that tendency and exacerbates its privacy-eroding effects.[127]

The GLBA's Privacy Rule applies in principle to applications such as Venmo, Square, and Google Pay. But in light of the market concentration, the sustained merger activity, and high degree of back-end integration in the digital economy, one is hard pressed to identify data flows that actually trigger the Rule's requirements. As a result, consumers are constructively deprived of their (already relatively meager) GLBA privacy rights for digital financial services. Consumers, researchers, and policymakers are also deprived of meaningful information about how consumer financial data is flowing and being used in the digital economy.

D. Lessons from the Payment App Case Study

Unlike HIPAA's scoping dodge problem, the GLBA's exception dodge issue is not widely recognized, in part because the GLBA's notice and opt-out requirements are weak tea. Our analysis is not a defense of the GLBA's paltry requirements, however, but a lesson about sectoral privacy regulation design. While the GLBA successfully avoids a scoping dodge because its scope is keyed to financial activity rather than traditional financial institutions, its affiliate exception opens a yawning gap in coverage.

Affiliate data flow exceptions are common in settings beyond finance. But corporate affiliation is no longer — if it ever was — a proxy

126. *Square Analytics*, SQUARE, https://squareup.com/us/en/point-of-sale/features/dashboard/analytics [https://perma.cc/Y799-W5EA].

127. This replicates on a smaller, inter-firm scale the argument others have made about the GDPR. Namely, that the law not only regulates privacy and data processing, but also sets compliance standards that eases inter-bloc commerce among European Union member states (and raises regulatory barriers to international commerce with non-bloc states). Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 810 (2019).

for common social context. Affiliate exceptions advantage large conglomerate entities, encourage market concentration, and magnify the competitive advantage large companies already draw from data aggregation. While data's flexibility increases the commercial value of cross-context aggregation, linking data across contexts and using it for divergent purposes raises significant privacy concerns. Consider the recent revelation of Amazon Ring's partnerships with over four hundred local law enforcement agencies.[128] Exempting such affiliations — and the resulting data flows — from scrutiny would shield flows that raise serious privacy concerns.

Problematic exception dodging is not limited to "affiliate" exceptions alone. Exceptions become dodges whenever they unexpectedly allow cross-context data sharing without appropriate normative constraints. For instance, the commonplace "public" data exception may allow commercialization of nominally publicly available data — such as court records and land registries — without privacy obligations, despite evidence that people often base their privacy expectations on the context in which data was collected.[129]

VI. SECTORAL AND OMNIBUS REGULATION: PITFALLS AND WAYS FORWARD

If sectoral privacy laws facilitate "dodges," perhaps we should prefer omnibus privacy regulation. But unless they provide standards for context-sensitive tailoring by judges and agencies, omnibus laws will amount to one-size-fits-all regimes, permitting contextually inappropriate information flows, erecting barriers to contextually appropriate flows, or both.

In response to the contextual needs of healthcare, for example, HIPAA enshrines a complex set of transmission principles varying with the particular actors, purposes, and information involved. It permits unauthorized disclosures for contextually routine purposes such as treatment, payment, and healthcare operations (with exceptions for psychotherapy notes) and mandates disclosures for Department of

128. Colin Lecher, *Amazon's Ring Offered a Footage Request System to More Than 400 Law Enforcement Agencies*, VERGE (Aug. 28, 2019 4:51 PM), https://www.theverge.com/2019/8/28/20837510/amazons-ring-partnerships-police-departments-map [https://perma.cc/9GEY-6D3E]; Jason Kelley & Matthew Guariglia, *Ring Reveals They Give Videos to Police Without User Consent or a Warrant*, ELEC. FRONTIER FOUND. (July 15, 2022), https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant [https://perma.cc/8W6Y-FLQV].

129. Kirstin Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J.L. & TECH. 111, 139–41 (2018); Abraham Bell & Gideon Parchomovsky, *Of Property and Information*, 116 COLUM. L. REV. 237, 241–44 (2016) (discussing the role of registries in the relationship between property and information access).

Health & Human Services compliance monitoring.[130] HIPAA allows some disclosures, such as listing minimal information in a facility directory and providing relevant information to family caregivers, under informal processes that rely heavily on professional judgment.[131] With narrow exceptions, the Rule forbids the sale and use of health information for advertising unless a detailed written "authorization" process is followed, and covered entities may not condition treatment or benefits on such authorization.[132] In these and other ways, the HIPAA Privacy Rule raises *and lowers* barriers to information flow depending on contextual norms.

Now consider two well-known omnibus privacy laws: California's CCPA (as modified by the Consumer Privacy Rights Act) and the EU's GDPR. Each imposes various requirements, many focusing on notice and transparency, relating to the collection, use, and disclosure of personal information.

The CCPA requires that a business's collection, use, and disclosure of personal information be reasonably necessary and proportionate to achieve the purposes for which it was collected or processed, or for another compatible disclosed purpose.[133] It does not, however, impose many restrictions on those disclosed purposes. Consumers' power to directly affect a business's use and disclosure of their information comes primarily from Section 1798.120's right to opt out of sale of personal information for valuable consideration and of "sharing" for cross-context behavioral advertising[134] and Section 1798.121's right to limit the use and disclosure of "sensitive" information collected or processed for the purpose of inferring characteristics about a consumer.[135] Both of these provisions default to allowing companies to do what they wish unless consumers proactively assert their rights, in contrast with HIPAA's default prohibition of the sale of health information or its use in (most) marketing unless explicitly authorized.[136] The CCPA is thus watered down in comparison to HIPAA's context-specific provisions.

---

130. "[T]he Privacy Rule requires a covered entity to obtain a patient's authorization prior to a disclosure of psychotherapy notes for any reason, including a disclosure for treatment purposes to a health care provider other than the originator of the notes." *Does HIPAA Provide Extra Protections for Mental Health Information Compared With Other Health Information?*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Sept. 12, 2017), https ://www.hhs.gov/hipaa/for-professionals/faq/2088/does-hipaa-provide-extra-protections-mental-health-information-compared-other-health.html [https ://perma.cc/7KWR-LSUP].

131. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 6 (2003).

132. 45 C.F.R. §§ 164.501, 164.508(a)(3) (2022).

133. CAL. CIV. CODE §§ 1798.100(a)(1), 1798.140(e) (West 2023).

134. *Id.* § 1798.120.

135. *Id.* § 1798.121(d).

136. If a communication is "marketing," then the communication can occur only if the covered entity first obtains an individual's consent. 45 C.F.R. §§ 164.501, 164.508(a)(3)

The GDPR's default is different. Under the GDPR, personal data may be processed only under limited circumstances, most notably with purpose-limited consent or when "necessary" to the "legitimate interests pursued by the controller or by a third party, except where . . . overridden by the interests or fundamental rights and freedoms of the data subject."[137] "Legitimate interest" and other alternative justifications are not available for "special categories" of data, including health data, where the default is to require "explicit consent" that is "freely given" and services cannot ordinarily be denied for refusal to consent.[138] The GDPR's default for health data is thus similar to HIPAA's authorization requirement for many uses and disclosures. But HIPAA does not require consent for routine medical information flows required for treatment.[139] In short, a one-size-fits-all explicit consent requirement would be inappropriate in the medical context.

In practice, neither jurisdiction actually applies omnibus rules to health data. The CCPA exempts HIPAA-covered entities, as well as entities covered by California's Confidentiality of Medical Information Act ("CMIA"),[140] from its requirements.[141] Unlike HIPAA, California's CMIA was recently amended to cover many health apps[142] and was a primary basis for the California Attorney General's complaint against Glow.[143] The GDPR exempts health data disclosures (similar to those allowed by HIPAA) from its blanket requirement of express consent for "special categories."[144] Like HIPAA, the GDPR thereby avoids erecting barriers to standard and appropriate flows of healthcare

---

(2022). For a general review of how the Privacy Rule treats sale and marketing with health data, see *Marketing*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Dec. 3, 2002), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html [https://perma.cc/Q36H-S5BM].

137. GDPR art. 6.

138. GDPR art. 9, recital 32; *see also id.* recital 53. It is still not entirely clear how the "legitimate interest" justification applies to targeted advertising even where sensitive data is not involved. *See, e.g.*, Clothilde Goujard, *Facebook, Instagram Face Norwegian Ban from Tracking Users for Ads*, POLITICO (July 17, 2023), https://www.politico.eu/article/facebook-instagram-norway-ban-track-users-ads [https://perma.cc/AP4L-73L2].

139. 45 C.F.R. § 164.506 (2020).

140. CAL. CIV. CODE § 56 (West 2023).

141. *Id.* § 1798.145(c)(1)(A)–(B) (West 2023). The CMIA's requirements for a valid authorization are similar to those under HIPAA. *Compare* CAL CIV. CODE § 56.11 (West 2023) (listing the requirements for valid authorization under CMIA), *with* 45 C.F.R. § 164.508 (2020) (listing the requirements for valid authorization under HIPAA).

142. CAL. CIV CODE § 56.06(b) (West 2023); *Attorney General Bonta Emphasizes Health Apps' Legal Obligation to Protect Reproductive Health Information*, STATE OF CAL. ATT'Y GEN. (May 26, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-emphasizes-health-apps-legal-obligation-protect [https://perma.cc/V6VL-TSEF].

143. Complaint for Injunctive, Civil Penalties, and Other Equitable Relief at 2, California v. Upward Labs, No. CGC-20-586611 (Cal. Super. Ct. Sept. 17, 2020) (alleging that information such as "medications, fertility test results, past and upcoming medical appointments, complete medical records, and ovulation-cycle calculations" is CMIA "medical information").

144. GDPR art. 9(3).

information. The GDPR's health data exemption does not cover direct-to-consumer health apps, however; they remain subject to the "special categories" explicit consent standard. If the main concern about health app data is disclosure for marketing, this may be roughly equivalent to HIPAA's consent requirement for marketing uses. Nonetheless, it is unlikely that the GDPR's exceptions manage to anticipate every situation in which explicit consent is an inappropriately high barrier to flows of "special category" data.

In sum, neither California nor the EU actually applies an omnibus rule to health data. Both, albeit differently, define sectoral rules. And both succeed in avoiding the "scoping dodge" that plagues HIPAA: California by bringing health apps (at least mostly) under its state medical privacy law and the EU by setting a stringent default rule for "sensitive" data and creating a sectoral exception that permits some contextually appropriate flows. The health data case demonstrates both the fallacy of the one-size-fits-all omnibus dream and the fact that scoping dodges are not inevitable in sectoral privacy law.

Our payment app analysis also illuminates the omnibus privacy law question. The CCPA and GDPR illustrate dramatically different possibilities for omnibus regulation. The CCPA imposes relatively weak limitations on information flow and use, giving consumers only a limited right to opt out of information sales and sharing for cross-contextual behavioral advertising and of certain uses of "sensitive" data.[145] The GDPR, on the other hand, requires legal justification for all data processing, though consent is nearly always an acceptable basis.[146]

The CCPA and GDPR are potentially both more and less restrictive than the GLBA. The CCPA does not cover payment apps (it exempts entities covered by the GLBA),[147] but if it did, the CCPA's opt-out regime would probably cover data sharing with affiliates — though it would apply only to "selling" or "sharing" for cross-contextual behavioral advertising.[148] Whether this compromise would improve on the GLBA is a question for contextual experts. And because financial information is not a "special category" under the GDPR, legal bases for sharing it (with affiliates or non-affiliates) include not only consent[149] but also "necessities" such as "legitimate interests pursued by the controller or by a third party, except where . . . overridden by the interests

145. *See California Consumer Privacy Act*, STATE OF CAL. ATT'Y GEN. (May 10, 2023), https://oag.ca.gov/privacy/ccpa#sectionf [https://perma.cc/4KYR-E274]; CAL. CIV. CODE §§ 1798.120–.121 (West 2023).

146. GDPR art. 6(1).

147. CAL. CIV. CODE § 1798.145(e) (West 2023).

148. *Cf.* CAL. CIV. CODE § 1798.145(i)(2) (West 2023).

149. Consent is defined as "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." GDPR art. 4. Consent is further specified in GDPR art. 7.

or fundamental rights and freedoms of the data subject."[150] Thus, the default rule varies according to the intended use, and it is not always possible for data subjects to opt out of sharing. Whether this is good is again a contextual question.

Omnibus laws such as the CCPA and GDPR generally impose significant requirements for notice, transparency, correction, deletion, obtaining valid consent, and the like. Complying with such duties may be overly burdensome in some circumstances. Both statutes limit their scope in response. The CCPA covers only "businesses" that handle large amounts of money or data.[151] The GDPR is scoped broadly, exempting "personal or household activity," leaving the question of whether there are other contexts in which privacy is more appropriately governed by informal norms and private arrangements than by potentially onerous legal requirements.[152]

Omnibus data privacy laws can also themselves fall prey to regulatory dodges: the CCPA applies only to "businesses" of a certain size,[153] creating the potential for a scoping dodge for smaller but privacy-invasive companies. Omnibus privacy laws also have to cover so much (and invite lobbying from so many sectors), that they may end up with watered-down, lowest-common-denominator provisions. Omnibus laws can also erect unnecessary and potentially costly barriers to contextually appropriate information flows and uses. In sum, omnibus approaches can mask or paper over regulatory design questions that are critical to contextual integrity.

A broad-based law need not be one-size-fits-all. Omnibus laws can accommodate contextual tailoring, either by including contextually specific derogations (as the GDPR does for healthcare) or by imposing flexible standards. The GDPR's legitimate interest basis is a step in this direction, but its emphasis on individual, rather than contextual or social, balancing is insufficient. Moreover, extant omnibus laws are uniformly overly dependent on consent, which is an important transmission principle, but often ineffective and certainly not universally appropriate.[154]

---

150. GDPR art. 6(1)(f).

151. CAL. CIV. CODE § 1798.140(d) (West 2023).

152. GDPR art. 2(2). On governing privacy via informal norms and other arrangements, see generally Madelyn Sanfilippo, Katherine J. Strandburg & Brett M. Frischmann, *Privacy as Knowledge Commons Governance*, *in* GOVERNING PRIVACY IN KNOWLEDGE COMMONS 268, 278–81 (Madelyn Rose Sanfilippo, Brett M. Frischmann & Katherine J. Strandburg eds. 2021).

153. CAL. CIV. CODE § 1798.140(d) (West 2023).

154. Article 9 allows EU or member state laws to remove consent as a legitimate basis for processing "special categories" of data. GDPR art. 9. There is, however, no recognition that individual consent may be an inappropriate basis for processing other types of data in some circumstances.

VII. GETTING OUT OF DODGE

Designing contextually sensitive but comprehensive privacy regulation is tricky. What can be done? Privacy regulation designers should employ CI's analytical framework: classifying information flows according to the roles of sender, recipient, data subject, and information type before considering the transmission principle most appropriate to the context. Designers should also explicitly consider who should assess the appropriateness of particular information flows and uses. Depending on the context and specific setting, legitimate governance bodies might range from legislatures to expert agencies to professional bodies to private communities to informal social norms.

A. Functional Sectoral Privacy Regulation

Sectoral privacy regulation should be drafted functionally to apply to entities and activities that involve the relevant sorts of contextual information flows. In principle, the overall scope of sectoral privacy regulation should be designed so that the "rules-in-use"[155] resulting from the contextual suite of applicable laws, regulations, professional requirements, and informal norms results in (mostly) contextually appropriate information flows. A contextually functional approach is a step in this direction.

In the fertility app case, the scoping dodge occurs because HIPAA's Privacy Rule defines covered entities based on now-outdated assumptions about the institutional structure of the healthcare system. While HIPAA's definition of "health care provider" is functional and potentially flexible, its limitation to entities that electronically transmit health information in connection with certain transactions seems odd from today's perspective.[156] While most traditional healthcare providers fall within the Privacy Rule's scope, this limitation's unanticipated effect is to exclude direct-to-consumer health app companies from the Privacy Rule's scope.

The GLBA defines covered entities functionally, but its affiliate exception is framed in terms of corporate status, ignoring the now-common possibility that affiliated entities might operate in disparate contexts. Regulators should state exceptions functionally so that contextually similar information flows are subject to the same

155. Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, NOBEL PRIZE LECTURE 408, 414 (Dec. 8, 2009), https://www.nobelprize.org/uploads/2018/06/ostrom_lecture.pdf [https://perma.cc/BA3V-N5S5].

156. However, this definition does have statutory roots. HIPAA's rulemaking mandate refers to "standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in Section 1173(a) of the Social Security Act." Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (1996).

transmission principles. The instinct that undergirds restrictions on sharing personal data with "third parties" should be seen for what it is — a proxy for concern about sharing that violates contextual information norms. Illegitimate sharing is not magically transformed into appropriate flow when one company buys another.

B. Omnibus Privacy Regulation

To design omnibus regulation with contextual integrity in mind, several approaches are possible.

An omnibus law could act as a gap-filler to sectoral laws. Many recent state privacy laws have this flavor, exempting at least some activities covered by sectoral privacy laws.[157] Backstop exemptions leave any dodge problems of the exempted sectoral laws in place, however, and may create additional dodges. Cases applying the Illinois Biometric Information Privacy Act's[158] ("BIPA's") GLBA exemption to university remote proctoring illustrate this point.[159] While exempting university proctoring from BIPA might make sense, it is strange to do so because universities are considered "financial institutions" under the GLBA. The problem arises because BIPA's GLBA exemption fails to recognize that universities perform myriad functions in different contexts.

An omnibus law could also set a constraining "floor" upon which sectoral laws erect higher privacy protections. This approach also has its weaknesses: privacy norms sometimes *encourage* appropriate personal information flows rather than discourage inappropriate flows.[160] The temptation is to rely on notice and consent to permit contextually appropriate flows, but this simply resurrects well-known problems with consent as a universal transmission principle. This could be mitigated, or replaced, by incorporating agency-vetted safe harbors based on best practices instead. The safe harbor approach is similar to the sectoral law exemption approach (and would similarly require careful monitoring of the scope of the safe harbor) but is generally employed in arenas where it is presumed that private sector expertise — often in the form of industry associations — or community organizations can do a better job than government in developing best practices. Assuming such robust community-based development, safe harbors could allow adaptation to technological and social changes, encourage context-specific norm

157. Indeed, the CCPA operates this way. *See supra* Part IV (discussing the CCPA).

158. 740 Ill. Comp. Stat. 14/1–99 (2023).

159. *See, e.g.*, Christopher Brown, *DePaul Defeats Biometric Privacy Lawsuit Over Online Proctor*, BLOOMBERG L. (Nov. 4, 2022), https://news.bloomberglaw.com/privacy-and-data-security/depaul-defeats-biometric-privacy-lawsuit-over-online-proctor [https://perma.cc/WEP6-8MYX].

160. For example, patients may share intimate information with a therapist because they know all sessions are private.

development, and provide sensitivity to sub-contexts or local norm variations. However, their obvious Achilles heel is vulnerability to industry capture — especially where privacy regulators vetting the best practices lack sectoral expertise.

Alternatively, an omnibus law could focus on cross-contextual issues. Laws such as the Wiretap Act[161] and the Electronic Communications Privacy Act[162] and, more recently, biometrics or face recognition regulations are of this ilk.[163] Indeed, many omnibus privacy laws seem aimed primarily at cross-contextual targeted advertising or profiling. If, however, today's omnibus privacy laws are aimed primarily at regulating information flows for targeted advertising, their heavy focus on notice and consent is ill-suited for that purpose, given their demonstrated ineffectiveness and high transaction costs.

Of course, standards can be difficult for regulated entities to understand, since they leave some questions uncertain and indeterminate. Here, however, sectoral regulations could standardize outcomes for repeat players in important contexts, while leaving room for courts to recognize and regulate new types of information flows within existing contexts using the standard. Courts could be expected to defer to informal norms and local governance in many other instances.

Finally, and we think preferably, an omnibus law could incorporate a general CI standard to be fleshed out by judges and agencies, thus avoiding both unregulated gaps and one-size-fits-all rules. A well-drafted context-based standard would allow judges and regulators to account for technological and social evolution, as well as for situations in which the norms, goals, and values of more than one context need to be taken into account. The basis for the GDPR's legitimate interests approach is standards-like, but it is not quite the contextual-integrity-based standard that we have in mind because it employs an overly individualistic balancing that is not sufficiently context-sensitive. Moreover, the GDPR employs consent as an all-purpose justification. Indeed, for data that falls under Article 9's "special categories," the legitimate interests justification is unavailable and consent reigns supreme. But consent is ineffective, burdensome, and simply not a universally appropriate transmission principle.

---

161. 18 U.S.C. §§ 2510–2523 (2021).

162. 18 U.S.C. §§ 2510–2523, 2701–2713, 3121–3127 (2021).

163. 18 U.S.C. § 2510 (2021) (prohibiting the unauthorized, nonconsensual interception of "wire, oral, or electronic communications" by government agencies as well as private parties); Pub. L. No. 99-508, 100 Stat. 1848 (1986) (extending protection to transmissions of communication from telephone calls to electronic data via computer); *see also* Illinois Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1–99 (2023); Washington Facial Recognition Law, WASH. REV. CODE §§ 43.386.010–.901 (2023). These are cross-contextual in the sense that protection afforded to information flows does not depend on the social context in which information is being shared.

A contextual-integrity-based omnibus law could provide a universally applicable standard while allowing agencies to develop sectoral regulations that might even incorporate appropriately vetted safe harbors. Sectoral regulation would concretize the CI standard for common situations in important contexts. Outside of such explicitly regulated areas and in situations of evolving or overlapping contexts, judges could apply the CI standard in common law fashion, considering evidence regarding contextual norms, values, and goals, just as tort law takes factors such as custom into account. Many types of evidence would be relevant, such as informal norms, industry practice, surveys of citizens and consumers, and professional ethics guidelines.

Of course, standards introduce uncertainty that can be difficult for regulated entities to manage. But they also provide opportunities to develop more substantive, contextually sensitive bodies of privacy law. Sectoral regulations could standardize outcomes for repeat players in important contexts, while leaving room for courts to recognize and regulate new types of information flows within existing contexts under the broad standard. Courts could be expected to defer to informal norms and local governance in many instances, allowing for context-specific norm development and flexibility to technological change. In sum, an omnibus law based on a contextual standard can incorporate the best of both worlds.