RING THE ALARM: AN ANALYSIS OF THE FTC'S HEALTH BREACH NOTIFICATION RULE

Alexis Tatum†

ABSTRACT

In 2024, the Federal Trade Commission updated and enforced the once-dormant Health Breach Notification Rule (HBNR) relating to privacy violations by health information technology disruptors that are not regulated under Health Insurance Portability and Accountability Act (HIPAA). The FTC's modernized definitions of terms like "breach of security" and "health care provider" are significant and helpful changes to reflect the world consumers face, rather than limiting enforceable privacy protections to technology that existed over a decade ago. However, the agency's inconsistent enforcement and subsequent changes to the Rule have opened the regulation to heightened procedural scrutiny. In an era of criticism of federal agency authority and increasing judicial restraints on federal agency actions, the FTC's enforcement of the Health Breach Notification Rule demonstrates a potential path towards clear, effective, and meaningful privacy law enforcement that encourages businesses to protect the privacy of individual consumers.

TABLE OF CONTENTS

DOI: https://doi.org/10.15779/Z388P5VC1G

† Alexis Tatum, J.D., University of California, Berkeley School of Law, Class of 2025. Many thanks to Allison Schmitt, Wayne Stacy, Erik Stallman, Gaurav Lalsinghani, Andra Cernavskis, and Michelle D'Souza for their guidance, support and encouragement.

I. INTRODUCTION

These days, it is very convenient for consumers to manage, record, and understand their health conditions from their homes and personal devices. Consumers can track their heart rate, blood oxygen levels, and sleep by wearing a smartwatch. Consumers can choose from dozens of phone applications designed to track menstrual cycles, ovulation, and fertility with increasing levels of specificity. Virtually any American can bargain shop for prescription and over-the-counter medications such as diabetes test strips, nicotine patches, and birth control pills in exchange for an input of personal health information to companies like GoodRx.[1]

1. *How Do I Find and Use Coupons for Over-The-Counter Medications and Medical Supplies?*, GOODRX, https://support.goodrx.com/hc/en-us/articles/360000677866-How-do-I-find-and-use-coupons-for-over-the-counter-medications-and-medical-supplies (last visited Feb. 12, 2025); *see also GoodRx Terms of Use*, GOODRX, https://support.goodrx.com/hc/en-us/articles/115005225563-GoodRx-Terms-of-Use (last accessed May 3, 2025). GoodRx offers prices and coupons for many popular over-the-counter medications, including Zyrtec, aspirin, vitamins, Claritin, and nicotine patches. The company also advertises discounted medical supplies and devices like test strips, needles, and meters. The information required for a GoodRx account to access these discounted items includes a user's date of birth, prescription information, home or billing addresses, and more.

Now more than ever, direct-to-consumer (D2C) products help inform consumers' personal health decisions without the safeguards of a doctor's office or a hospital, where the collection of consumer information is federally regulated by the U.S. Department of Health and Human Services (HHS).[2] Americans began using telehealth services for physical and mental health at unprecedented levels during the COVID-19 pandemic, and that telehealth use remained significantly higher than pre-COVID levels in 2024.[3] The dominance of D2C healthcare has created new ways for consumers to track and manage their health themselves, including the ability to request consumer-initiated lab testing without the guidance or authorization of a doctor.[4] D2C healthcare is also extremely profitable—in April 2020, D2C healthcare was already a $700 billion industry.[5] While D2C healthcare provides consumers with convenience and greater accessibility, the industry is largely unregulated by the federal government and businesses face requirements to adhere to typical standards of transparent communication and patient privacy. As a result, sensitive data, including social security numbers, biometric profiles, test results, and insurance information, is not protected by HHS regulations when shared with D2C healthcare companies.

HHS can only enforce the provisions of the Health Insurance Portability and Accountability Act (HIPAA) in traditional health care provider settings.[6] Many people mistakenly assume that the HIPAA regulations apply to all people or entities that have access to an individual's health information, but HIPAA's regulations do not cover many D2C providers because they are not traditional health care providers, as defined by HIPAA.[7] As consumers take

2. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index. html (last visited May 3, 2025).

3. Oleg Bestsennyy, Greg Gilbert, Alex Harris & Jennifer Rost, *Telehealth: A Quarter-Trillion-Dollar Post-Covid-19 Reality?*, MCKINSEY & CO. (July 9, 2021), https://www.mckinsey.com/industries/healthcare/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality; *see also* Michael Kalinowski, *Telehealth Testing and Direct-to-Consumer Lab Testing Give Patients a Prominent Seat at the Healthcare Table*, LIGOLAB (Sept. 13, 2024), https://www.ligolab.com/post/telehealth-and-direct-to-consumer-testing-give-patients-a-prominent-seat-at-the-healthcare-table. Today, most states allow consumers to order some (or all) of their laboratory tests directly without the involvement of a physician. This is an example of how the telehealth industry has grown rapidly since the COVID-19 pandemic.

4. *See* Kalinowski, *supra* note 3.

5. Adam B. Cohen, Simon C. Matthews, E Ray Dorsey, David W. Bates & Kyan Safavi, *Direct-To-Consumer Digital Health*, THE LANCET (Apr. 2020), https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30057-1/fulltext.

6. *Summary of the HIPAA Privacy Rule*, *supra* note 2.

7. *See generally* PAUL M. SCHWARTZ & DANIEL J. SOLOVE, PRIVACY LAW FUNDAMENTALS 79 (International Association of Privacy Professionals, Inc., 7th ed. 2024).

more control of their health choices, the information used to make those decisions is used for purposes far beyond their control. Until 2023, GoodRx allegedly shared consumer prescription information and other identifying information with third-party advertising platforms for purposes that were never shared with consumers.[8] This kind of unauthorized disclosure of sensitive consumer information often leads to data breaches, exposures, and leaks that publicize and compromise important consumer information. In 2023, the Identity Theft Resource Center reported an unprecedented number of such incidents, amounting to more than three thousand different breaches.[9] A majority of Americans on both ends of the political spectrum think there should be more government regulation of what companies can do with customers' personal information in light of steadily increasing privacy concerns over the past decade.[10]

In the case of the GoodRx breach, consumers' personal health privacy was violated by GoodRx's broken promises. The company told its users that it would "never" share personal information with advertisers or other third parties, then allegedly did just that for several years, unbeknownst to millions of GoodRx customers.[11] GoodRx users had no options for direct recourse because this sort of injury does not currently create a cause of action that can be redressed in court.[12] As demonstrated by the Supreme Court's decision in *TransUnion LLC v. Ramirez*, a company's violation of its privacy policies is not enough of an injury to provide a consumer with standing to sue, absent a showing of further harm such as the theft of credit information.[13]

---

8. *See generally* Complaint Against GoodRx for Permanent Injunction, Civil Penalties, and Other Relief, United States v. GoodRx Holdings, Inc., No. 23-cv-460 (N.D. Cal. Feb. 1, 2023).

9. *2023 Data Center Report*, IDENTITY THEFT CTR. (2024), https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (last visited Dec 20, 2024).

10. *See* Michelle Faverio, *Key Findings About Americans and Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/ ("Some 78% of Democrats and 68% of Republicans think there should be more government regulation of what companies can do with customers' personal information.").

11. GoodRx Complaint, *supra* note 8, at ¶ 3.

12. *See, e.g.*, Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (holding that plaintiffs could not maintain suit against Northwest Airlines for breach of its privacy statement because it was not a contract). Similarly, the GoodRx Terms of Service do not constitute a contract for which individual plaintiffs could raise a breach of contract claim against GoodRx.

13. Schwartz, *supra* note 7, at 418. ("Health information is considered by many to be among the most private information . . . . Pursuant to its authority under the Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, the Department of Health and

In 2023, the Federal Trade Commission (FTC) took the unusual step of filing an enforcement action against GoodRx for its data practices, citing the Health Breach Notification Rule (HBNR), which the agency had not invoked in over a decade.[14] For the first time, the FTC stepped in to address the reckless exposure of consumer data and breach of their private health data by enforcing a once-abandoned federal rule targeting the failure to protect sensitive consumer data as an illegal "unfair or deceptive trade practice."[15] Despite widely documented concerns about digital privacy, especially in the health care context, Congress has rarely produced legislation that acknowledges and protects against these privacy violations.[16] The HBNR is the result of only a small set of privacy laws ever passed by Congress.

The FTC's investigation and enforcement resulted in GoodRx hiring a vice president of Data Privacy, creating written standards of data maintenance and security, and ceasing its disclosures to third parties.[17] Since this first action, the FTC has committed to enforcing the HBNR against vendors of personal health records "with vigor."[18] In 2024, the Commission finalized updates to "modernize" the Rule in support of this mission to protect sensitive health data for consumers, who often lack any meaningful opportunity to limit the use of their personal information when they solicit goods or services related to their health.[19]

The FTC's decision to enforce the once inoperative HBNR and later update the Rule to clearly demonstrate its scope and compliance requirements is exactly the type of flexible action the Commission should take to avoid agency rules becoming ignored, inconsistently enforced, or outdated. While critics suggest that the FTC's updates to the Rule are an unauthorized

---

Human Services promulgated regulations under HIPAA. The ensuing framework . . . provides a minimum level of protection for all states.").

14. Lesley Fair, *First FTC Health Breach Notification Rule Case Addresses GoodRx's Not-So-Good Privacy Practices*, *Federal Trade Commission*, https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices (last visited Mar. 17, 2025).

15. GoodRx Complaint, *supra* note 8, at ¶ 9.

16. *See generally U.S. Privacy Laws*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/privacy-laws/united-states/ (last visited Feb. 12, 2025) (The most recent privacy-related statutes passed by Congress were passed in the 1990s and do not address digital consumer privacy).

17. GoodRx Complaint, *supra* note 8, at ¶ 59.

18. Fed. Trade Comm'n, Remarks by Chair Lina M. Khan on the Health Breach Notification Rule Policy Statement Commission File No. P205405 (Sep. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596360/remarks_of_chair_lina_m_khan_regarding_health_breach_notification_rule_policy_statement.pdf.

19. Health Breach Notification Rule, 89 Fed. Reg. 47028 (May 30, 2024) (16 C.F.R. § 318).

expansion of agency power, the Commission's actions are well within their statutory authority and necessary to address the myriad of unauthorized invasions of health privacy that American consumers face today. Congress outlined a specific privacy concern when it contemplated that D2C health information technology not covered by HIPAA would eventually play a larger role in the lives of Americans and that it would need effective regulation to avoid disastrous erasure of health information privacy. To address this concern, Congress authorized the Commission to create a Rule responsive to those concerns.[20] In an era of attacks on federal agency power, the FTC should balance the aggressive approach to protecting consumers from fraught health privacy concerns with maintaining its legitimacy as an institution. When the FTC enforces the HBNR, it should take special care to respect due process and work with Congress to provide recommendations, insights, and progress reports to encourage Congress to pass more notice-and-comment privacy rulemaking statutes. Congress should produce more legislation authorizing privacy rules like the Health Breach Notification Rule to (1) provide agencies the necessary flexibility to address privacy violations when new, disruptive D2C businesses that escape regulation arise, (2) allow agencies a clearer and faster process to respond to privacy harms caused by businesses to consumers, and (3) re-emphasize the legitimacy of the FTC and other agencies tasked with protecting consumers' privacy interests.

The ability to review and update privacy rules promulgated by the FTC is one of the few options the federal government has to ensure that the law catches up with technological disruptors that often enter the market and spend years avoiding preexisting regulations that should apply to them. For example, the FTC's modernized definition of terms like "breach of security" is a significant and helpful change to reflect the world consumers face presently, not the world as it was in 2009, because the new definition reflects how privacy experts describe breaches today.[21] The HBNR should be strongly enforced,

20. American Recovery and Reinvestment Act (ARRA), Pub. L. No. 111-5, § 13410 (2009).

21. *See, e.g.*, WOODROW HARTZOG & DANIEL SOLOVE, BREACHED!: WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 5 (Oxford University Press 2022) ("Data breaches, by which we mean the unauthorized exposure, disclosure, or loss of personal information, are not only more numerous; they are more damaging."); *see also* National Institute for Standards and Technology Computer Security Resource Center, https://csrc.nist.gov/glossary/term/breach (last visited Feb. 12, 2025) (defining breach as "[t]he loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose.").

and its enforcement should be recognized as an example of impactful privacy law that acknowledges and protects consumer interests.

This Note explores the FTC's HBNR as a meaningful and effective method of regulating an increasingly pervasive data economy in the health information technology sector. Part II discusses the Rule in the context of the FTC's other congressionally mandated data privacy rules and the Commission's policy focus on protecting consumer privacy under the direction of Chair Lina Khan from 2021 to January 2025. Part III examines the odd and arguably controversial enforcement and promulgation history of the Rule from its inception in 2009 to its 2024 revision and related enforcement actions. Finally, Part IV will suggest improvements to the largely positive impact of the Rule on federal data protection, demonstrated by heightened privacy protections, notice, and opportunities for consent that resulted from the FTC's enforcement of the Health Breach Notification Rule.[22] These improvements protect consumers seeking to maintain their privacy while taking a more convenient, informed part in their health choices by using D2C health services and products.

II. BACKGROUND

Over the course of the agency's history, the FTC has become the premier agency for regulating information privacy. Section II.A outlines where the FTC gets general authority to enforce information privacy laws and policies and explains the history and function of the HBNR. Sections II.B and II.C discuss the significance of breach notification rules as a method of privacy protection and the role of the HBNR in the FTC's broader information privacy protection regime, most of which consists of breach notification rules.

A. GENERAL FTC AUTHORITY TO REGULATE INFORMATION PRIVACY

The FTC has the authority to promulgate rules under two statutes: the Federal Trade Commission (FTC) Act and the Administrative Procedure Act (APA).[23] The FTC Act provides the agency with broad authority but requires complex processes to promulgate substantive rules protecting consumers. Alternatively, the APA provides a series of straightforward rulemaking processes, including the notice-and-comment rulemaking procedure.[24]

22. *See, e.g.*, *GoodRx* Complaint, *supra* note 8; at ¶ 115; *see also* Complaint against EasyHealthcare, Inc. for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. EasyHealthcare, Inc., No. 1:23-cv-3107 (N.D. Ill. May 17, 2023).

23. Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (1914); Administrative Procedure Act (APA), 5 U.S.C. §§ 551–559 (1946).

24. 5 U.S.C. § 553 (1976).

1. The FTC's Authority Under the Federal Trade Commission Act

The Federal Trade Commission was established in 1914 to police the problem of "bigness" through regulating monopolies and large businesses that achieved their "bigness" from unfair and deceptive trade practices.[25] The agency's statutory authority to achieve this mission is largely encompassed in the FTC Act, which prohibits unfair and deceptive trade practices, and the Clayton Act, which prohibits unlawful corporate mergers and acquisitions, among other anticompetitive business arrangements.[26] The Commission's ability to protect consumer interests specifically originated in the Wheeler-Lea Act of 1938, in which Congress amended § 5 of the FTC Act to include "unfair and deceptive acts or practices in or affecting commerce" and "unfair methods of competition" as illegal activity that the Commission could specifically define and proscribe rules to regulate.[27] This development drastically expanded the scope of FTC power from an agency primarily focused on issues of unfair competition between businesses to an agency tasked with investigating and enforcing fair business practices for consumers and competitors alike.[28] Over time, the FTC focused on invasive advertising practices and business communications to consumers as an area ripe with unfair and deceptive trade practices.[29] Because today's businesses use consumers' personal data to advertise, and advertising is a category of business practices that the FTC has historically regulated, data privacy falls into the FTC's purview.[30]

The FTC utilizes § 5 of the FTC Act in part by promulgating and enforcing rules, which Congress authorized in § 6 and § 18 of the FTC Act.[31] Section six provides the Commission with authority to "make rules and regulations for the purpose of carrying out the provisions of this subchapter" and is cited by the FTC for its authority to regulate competition law.[32] Section six rulemaking authority is limited to procedural rules enforcing specific provisions within the FTC Act.[33]

The FTC's exclusive authority for issuing substantive rules with respect to unfair or deceptive trade practices is found in § 18 of the FTC Act, also

25. *See generally* Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 ANTITRUST L.J 1 (2003).

26. *See* FTC Act, *supra* note 23; *see also* Clayton Antitrust Act, 15 U.S.C. §§ 12–27 (1914).

27. *See* FTC Act § 45(a) (also referred to as) Wheeler-Lea Act, Pub. L. 75-447.

28. CHRISTOPHER HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW & POLICY 36–39 (Cambridge University Press, 2016).

29. *Id.*

30. *See id.* at 58–59.

31. 15 U.S.C. § 46(g); 15 U.S.C. § 57(a).

32. 15 U.S.C. § 46.

33. *Id.*

referred to as the Magnuson-Moss rulemaking authority.[34] Here, Congress specifically provided the Commission with broad authority to promulgate substantive rules to protect consumers from unfair and deceptive trade practices. When Congress amended the FTC Act in 1975 to include § 18, the legislative body recognized that, to be effective, the FTC needed flexibility to respond to the inevitability of new problems that would otherwise escape regulation, demonstrating Congress's intent to protect consumers from activity escaping regulation.[35]

Section eighteen empowers the Commission to "promulgate trade regulation rules, which define with specificity acts or practices that are unfair or deceptive acts or practices in or affecting commerce."[36] The statute allows the FTC to establish trade regulations that "may include requirements prescribed for the purpose of preventing such acts or practices."[37] Notably, § 18 allows the FTC to enforce substantive rules with civil penalties and injunctions under § 5 of the FTC Act.[38] The ability to promulgate rules under § 18 that effectuate Congress's ban on unfair or deceptive business practices theoretically allows the FTC to produce structural effects on the market to better reflect a balance between business's ability to reach consumers and each consumer's right to not be deceived or treated unfairly in the name of targeted advertising.

With great enforcement power, however, comes great procedural requirements.[39] In Title II of § 18, Congress detailed a unique agency rulemaking procedure complete with advance notices and public hearing requirements. The FTC's § 18 rulemaking authority is unique because it has more stipulations than what is required of agency rules by the APA and is a much lengthier rulemaking process that historically takes several years to complete.[40] Section eighteen authority has gone unused by the FTC for

34. 15 USC § 57(a); *see also* HOOFNAGLE, *supra* note 28, at 55. ("Title II [of the Magnuson-Moss Warranty Act] codified a framework for the Agency to draft "interpretive rules and general statements of policy" defining specific practices as unfair or deceptive.").

35. *See* HOOFNAGLE, *supra* at 28, at 55.

36. 15 U.S.C. § 57(a); *see also* 16 C.F.R. § 1.8 (interpreting the nature, authority, and use of trade regulations by the FTC under 15 U.S.C. 57(a)).

37. 15 U.S.C. § 57(a).

38. *Id.*; *see also* HOOFNAGLE, *supra* note 28, at 101. Existing trade regulations are codified in the Code of Federal Regulations and have the binding authority of civil law once promulgated.

39. *FTC Privacy Rulemaking: The Steps to Get There*, IAPP, https://iapp.org/media/pdf/resource_center/ftc_privacy_rulemaking_infographic.pdf (last visited May 3, 2025.).

40. *See* 5 U.S.C. § 553; *see also* 15 U.S.C. § 57. While the APA only requires agencies to initiate a rule, provide a Notice of Proposed Rulemaking (NPR) and a public comment period before finalizing a regulatory rule, § 18 requires additional steps, including publishing an

decades, largely because of how long it would take the FTC to finalize a rule. As a result, the FTC has never promulgated a privacy rule even though the agency technically has the authority to do so under § 18.[41] In August 2022, the FTC began the process of adopting a wholly new trade regulation rule, the Commercial Surveillance and Data Protection rule under § 18.[42] If successful, it would be the first time the FTC has promulgated a § 18 Rule in modern day.[43]

2. FTC's Authority Under the Administrative Procedure Act

Like every other federal agency, the FTC can create substantive rules that have the effect of law under § 553 of the Administrative Procedure Act.[44] While the statute outlines multiple ways to formulate, propose, and finalize a rule, the most commonly employed method of promulgating an agency rule is the notice-and-comment rulemaking process.[45] The FTC follows the notice-and-comment rulemaking procedures by issuing a notice of proposed rulemaking, providing opportunity for public comment, then developing and publishing a final rule.[46] Congress typically instructs the agency to use the notice-and-comment rulemaking process when it grants an agency authority to enforce a particular statute.[47] The FTC promulgated the HBNR through the notice-and-comment rulemaking process in accordance with a statutory mandate from Congress, as well as several other privacy rules.[48]

Advanced Notice of Proposed Rulemaking (ANPR) in the Federal Register, providing advanced notice to Congress, and informal hearings before a new FTC rule can be developed and published.

41. *See* CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB1083, FTC CONSIDERS ADOPTING COMMERCIAL SURVEILLANCE AND DATA SECURITY RULES (2022) ("The [Commercial Surveillance and Data Security Rules] ANPRM is also noteworthy because it would be the first time in decades that the FTC has adopted a wholly new "Trade Regulation Rule" (TRR) (i.e., a rule adopted under Section 18 of the FTC Act).").

42. *See id.*

43. *Id*; *see also* Kurt Walters, *Reassessing the Mythology of Magnuson-Moss: A Call to Revive Section 18 Rulemaking at the FTC*, 16 HARV. L. & POL'Y REV. 519, 531–32 (2022) (Following intense backlash and critiques of the FTC's rules promulgated under § 18, Congress passed legislation that restricted the FTC's ability to utilize the substantive rulemaking process. Consequently, the FTC has not successfully promulgated a rule under § 18 since the 1980's).

44. 5 U.S.C. § 553.

45. *See* TODD GARVEY, CONG. RSCH. SERV., R41546, A BRIEF OVERVIEW OF RULEMAKING AND JUDICIAL REVIEW, 2–5 (2017).

46. *Notice-and-Comment Rulemaking*, Admin. Conf. of the U.S., Information Interchange Bulletin No. 014 (2021).

47. *See, e.g.*, Children's Online Privacy Protection Act of 1998 (COPPA), 16 C.F.R. § 312. (15 U.S.C. § 6505) authorizing the FTC to promulgate the COPPA Rule.

48. *See* Pub. L. 111-5, *supra* note 20.

B. WHY BREACH NOTIFICATION RULES?

Most of the few statutory privacy regulations passed by Congress, including the HBNR, are breach notification rules.[49] Data or security breach notification laws require entities that possess sensitive individual user data, normally for business purposes, to notify individuals and other parties when an unauthorized access or use of their personal data occurs.[50] These rules, frequently used on both the state and federal level, allow individuals an opportunity to mitigate risks associated with the breach of their privacy and to incentivize businesses to strengthen their data security practices before a breach of security occurs.[51] Because data breach laws are drafted and enforced in a variety of ways, their efficacy varies. Generally, breach notification laws decrease the number of injuries that result from breaches, such as identity theft.[52] Although there is currently no comprehensive federal breach notification statute, all fifty states have some sort of breach notification statute for businesses that vary in scope and remedies, in addition to sector-specific federal rules such as the Gramm-Leach-Bliley Act (GLBA), which regulates the financial services industry.[53]

These breach notification requirements are a response to real concerns held by consumers today. The International Association of Privacy Professionals surveyed 4,750 individuals across nineteen countries and found that nearly seventy percent of consumers globally are either somewhat or very concerned about their privacy online.[54] In 2019, Pew Research Center reported that roughly six out of ten Americans believe it is not possible to go through daily life without having their data collected, and seventy-nine percent of Americans said they are not too or not at all confident that companies will admit mistakes and take responsibility if they misuse or compromise personal

49. *See, e.g.*, COPPA Rule, 16 C.F.R. § 312; *see also* GLBA Standards for Safeguarding Customer Information Rule (GLBA Safeguards Rule), 16 C.F.R. § 314. Each of these rules are breach notification methods of consumer privacy protection: HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 164. The HBNR and HIPAA rules are the only federal breach notification rules related to health.

50. *Id.*

51. *See generally* GINA STEVENS, CONG. RSCH. SERV., RL34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS (2010).

52. *See generally* Aniket Kesari, *Do Data Breach Notification Laws Work?*, 26 N.Y.U. J. LEGIS. & PUB. POL'Y 173–237 (2023).

53. *Security Breach Notification Laws: 50-State Survey*, JUSTIA (Jan. 15, 2025), https://www.justia.com/consumer/identity-theft/security-breach-notification-laws-50-state-survey; *see also* 16 C.F.R. § 314, *supra* note 49.

54. Müge Fazlioglu, *IAPP Privacy and Consumer Trust Report*, IAPP (Mar. 2023), https://iapp.org/resources/article/privacy-and-consumer-trust-summary.

information.[55] While breach notification rules do not entirely erase the possibility of breaches of consumer privacy, they at least require consumers to receive information about these breaches and further encourage preventative measures that deter violations of consumer trust.

C. COMPARING THE HBNR TO OTHER FEDERAL BREACH RULES

While there is no federal breach notification statute, the HBNR is one of a few breach notification rules employed by U.S. federal agencies to protect sensitive information, all of which focus primarily on information related to health, finance, and children's privacy.[56] Each Rule was developed to enforce statutory mandates from Congress to protect consumers' sensitive data in the normal course of business.[57] Federal agencies were authorized to create each statutory breach notification rule in HIPAA, the HITECH Act as part of the Recovery and Reinvestment Act, the Gramm-Leach-Bliley Act (GLBA), and the Children's Online Privacy Protection Rule (COPPA).[58] Four of the six statutory breach notification rules are enforced by the Federal Trade Commission.[59] The FTC Health Breach Notification Rule is the first in a series of updates to existing statutorily authorized privacy rules first promulgated in the late 1990s.[60] In November 2023, the FTC announced final updates to the GLBA Safeguards Rule, which require financial institutions to provide additional consumer notices in the event of a breach.[61] Similarly, in December 2023, the FTC proposed amendments to the COPPA Rule to "respond to changes in technology and online practices, and where appropriate, to clarify and streamline the Rule."[62]

---

55. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information.

56. *See, e.g.*, the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule promulgated and enforced in part by the FTC, *supra* note 49.

57. *Id.*

58. *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S. C. § 1320d-9; *see also* Pub. L. 111-5, *supra* note 20; Gramm-Leach-Bliley Act (GLBA), Pub. L. 106-102, 113 Stat. 1338; Children's Online Privacy Protection Act of 1998 (COPPA) (15 U.S.C. 6505).

59. *See* STEVENS, *supra* note 51, at 10–12. The FTC's authority to enforce these rules has made the FTC the primary administrative agency responsible for most federal consumer privacy protection.

60. *See, e.g.*, the COPPA Rule, *supra* note 49.

61. *Id.*

62. *See supra* note 49.

III. THE FTC'S HEALTH BREACH NOTIFICATION RULE

The FTC's HBNR has an atypical enforcement history that has caused confusion and concern about the scope of the Rule. Section III.A outlines the statutory origins and original promulgation of the HBNR. Section III.B explains the FTC's inconsistent enforcement of the HBNR, including the FTC's first two HBNR enforcement actions against GoodRx and Easy Healthcare.

A. STATUTORY ORIGINS AND ENFORCEMENT HISTORY

The FTC's Health Breach Notification Rule is an extension of privacy protections established by HIPAA.[63] Passed in 1996, HIPAA establishes guidelines by which personally identifiable health information should be protected from unconsented disclosure by traditional health care providers such as clinics, hospitals, nursing homes, doctors' offices, health care insurance providers, billing services, and employer-sponsored health plans.[64] The statute provides the Department of Health and Human Services the authority to enforce privacy rules against traditional healthcare providers with civil and criminal penalties.[65] The HIPAA privacy rules do not apply to nontraditional D2C health service providers, such as the data collected by an Apple Watch, an app that tracks menstrual cycles, or a consumer's prescription history from a telemedicine platform.[66] While an obstetrician's office is required to ensure effective protection of personal health information related to a patient's fertility, D2C providers had no such requirement to ensure secure information collection and storage practices. Thus, the FTC HBNR was authorized by the HITECH Act to complement the existing privacy and security rules in HIPAA, promulgated and enforced by HHS.[67] Congress recognized that

63. *See generally* Health Breach Notification Rule, 89 Fed. Reg. 47028 (May 30, 2024) (16 C.F.R. § 318).

64. *See* 42 U.S.C. § 1320d-9 (1996).

65. 42 U.S.C. § 1320(j) (1996).

66. *See* HIPAA Summary, *supra* note 2 ("The [HIPAA] Privacy Rule . . . appl[ies] to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities")."). These are all "traditional" healthcare providers that the public expects to be covered by HIPAA.

67. *See* Pub. L. 111-5, § 13410, *supra* note 20; *see also* CLINTON T. BRASS, CAROL HARDY VINCENT, PAMELA J. JACKSON, JENNIFER E. LAKE & KAREN SPAR, CONG. RSCH. SERV., R40537, AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009 (P.L. 111-5): SUMMARY AND LEGISLATIVE HISTORY (2009) ("the HITECH Act includes a series of privacy and security provisions that amend and expand the current federal standards under the Health Insurance Portability and Accountability Act (HIPAA). Among other things, it establishes a breach notification requirement for health information that is not encrypted. . . .").

people would be skeptical of the digitalization of their records because of the presumed increased risk of security breaches by hackers or poor management practices.[68] As a result, Congress held several hearings on a health information and privacy statute, which ultimately culminated in the HITECH Act, implemented as Title XIII of the 2009 Recovery Act.[69] Each of these rules contains a breach notification as a method of protecting privacy.[70] This Section outlines the significance of breach notifications, the FTC's "modernized" HBNR, and how the Rule is enforced.

1. 2009 Promulgation

In 2009, Congress passed the American Reinvestment and Recovery Act ("Recovery Act") to reinvigorate the national economy following the 2008 financial crisis.[71] As part of Congress's years-long effort to update health systems and adopt health information technology that reduces the difficulties faced by patients and their physicians accessing paper health records, Congress passed the Health Information Technology for Economic and Clinical Health ("HITECH Act").[72] The HITECH Act was enacted as Title XIII of the Recovery Act.[73] The statute expanded the scope of the HIPAA Privacy and Security Rules and authorized the promulgation of the FTC Health Breach Notification Rule.[74] Notably, several members of Congress and panelists before them expressed doubts about the HIPAA rules being effective in protecting patient privacy due to their lack of enforcement.[75] In particular, members of Congress noted that since the promulgation of the HIPAA Privacy Rule, the HHS Office of Civil Rights (OCR) received over thirty thousand complaints of alleged violations of the Rule,[76] but no penalties were issued on any of those complaints.[77] As Congresswoman Hilda Solis commented, "[t]he OCR, as you know, is already overburdened by existing

68. *See generally* John H. Cochran, *Investing in Health IT: A Stimulus for a Healthier America*, 13 PERMANENTE J. 65–70 (2009).

69. *See, e.g.*, *Fourth in a Series on Health Care Information Technology: Hearing Before the Subcomm. on Health of the H. Comm. on Ways and Means*, 109th Cong. (April 6, 2006).

70. *See generally* Stevens, *supra* note 51, at 10–12.

71. ARRA, *supra* note 20; *see also* BRASS ET AL., *supra* note 67.

72. *Id.*

73. ARRA, *supra* note 20.

74. BRASS ET AL., *supra* note 20.

75. *See* Devin McGraw, *Discussion Draft of Health Information Technology and Privacy Legislation Before the H. Comm. on Energy and Com.*, CTR. FOR DEMOCRACY & TECH. (June 4, 2008); *see also* statement by House Representative Henry Waxman: (" . . . the Administration has not imposed a single civil fine under the Federal Medical Privacy Rule, despite over 30,000 complaints of violations since the rule has been in effect.").

76. McGraw, *supra* note 75.

77. *Id.*

privacy complaints, and consequently complaints related to discrimination, language access, and racial and ethnic health disparities are not being adequately addressed in my opinion."[78] In light of the poor enforcement of the HIPAA rules and the acknowledgment of new potential D2C health services, Congress authorized the FTC to create the Health Breach Notification Rule with an eye towards improved enforcement.

Rather than amend the HIPAA statute to broaden the scope to whom the statute would apply, Congress authorized the FTC to promulgate a new rule to maintain relative flexibility in the health technology space.[79] This approach allowed Congress to address the growing concern about vendors of personal health records that may not provide a health service, such as vendors that provide online repositories of sensitive health data for personal use by the consumer.[80] Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of sensitive, identifiable personal health information, updates the existing HIPAA rules, and enables the promulgation of the HBNR.[81] Since 2009, the FTC and HHS have continued to collaborate to promote uniformity in health and health technology privacy rules by announcing guidance together.[82]

While the FTC's HBNR and the HIPAA breach rules may seem redundant on their face, Congress specified that the FTC's ability to enforce regulations of health data was necessary due to a growing gap in HIPAA's coverage of certain emerging health technologies, especially services and products that use health information but do not involve doctors, hospitals, or health insurance.[83] Congress was aware of this discrepancy and the OCR's limited ability to effectively enforce existing rules when it updated the HIPAA Privacy and Security rules and authorized the FTC to promulgate another health privacy rule in the HITECH Act. During a Senate floor hearing on the Recovery Act, Senator Whitehouse defended the inclusion of the HITECH Act and its privacy provisions:

---

78. *Id.*

79. Health Breach Notification Rule, 89 Fed. Reg. 47028, 47029 (May 30, 2024) (16 C.F.R. § 318).

80. *FTC Issues Final Breach Notification Rule for Electronic Health Information*, FED. TRADE COMM'N (Aug. 17, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/08/ftc-issues-final-breach-notification-rule-electronic-health-information.

81. Health Breach Notification Rule, 89 Fed. Reg. 47028, 47029.

82. *See, e.g.*, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, FED. TRADE COMM'N (July 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

83. *See generally* Discussion Draft of Health Information Technology and Privacy Legislation Before the H. Comm. on Energy and Com., *supra* note 76.

> [W]e all know that health information technology is ultimately about patients. Patients must trust and participate in the health information technology revolution if it is going to reach its full potential. Therefore, the Recovery bill includes a number of vital privacy protections to ensure the security and the confidentiality of electronic patient records. These protections include changes in notification policy if there is an unauthorized acquisition or disclosure of health information. It includes the establishment of privacy officers in HHS regional offices, new restrictions on the sale of health information, improved enforcement of violations to privacy law and other strong provisions. I am well aware that privacy is a controversial and highly charged area of debate. I think it is important we all view the privacy provisions in this bill as the beginning and not the end of our national discussion about health care privacy. These provisions will require oversight and, perhaps over time, adjustment. I look forward to this ongoing challenge and remain committed to being engaged in it. But for now, this is a good, strong privacy package. It has, I think, solid agreement in this building.[84]

Congress viewed the HBNR as necessary because it recognized both the need for digital health recordkeeping and the growing existence of direct-to-consumer health information technology. The provisions of the HITECH Act were meant to advance the use of such technology, but not at the expense of consumers' privacy.[85]

On August 24, 2009, the Federal Trade Commission issued the Final HBNR to officially implement the provisions in the HITECH Act, as instructed by Congress. The Rule applies to vendors of personal health records and related third parties that are not covered by HIPAA, which provides a similar Rule applicable to certain "covered entities" and "business associates" traditionally recognized or associated with healthcare providers.[86] The FTC provided very few examples of vendors of personal health records when it announced the Final Rule, but noted that devices like blood pressure cuffs or pedometers, whose readings consumers can upload into their personal health records, are examples.[87] The HBNR outlines steps that vendors of unsecured "personal health record" (PHR) identifiable health information are required to take in light of a "breach of security" as defined by the statute.[88] The main

84. 155 CONG. REC. S1474–S1614. S1510–12 (2009) (statement of Sen. Sheldon Whitehouse).

85. *Id.*

86. HIPAA Security Rule, 45 C.F.R. § 164.304 (2003); 45 C.F.R. § 164.308 (2003); 45 C.F.R. § 164.310 (2003).

87. *See FTC Issues Final Breach Notification Rule*, *supra* note 80.

88. 16 C.F.R. § 318.2 (2024).

steps in the statute include notifying each affected individual, the Federal Trade Commission, and in some cases, the media.[89] As noted in § 13407(g)(2)of the HITECH Act, the HBNR is meant to be temporary until Congress enacts new legislation "establishing requirements for notification in the case of a breach of security."[90] Any violation of the Rule may be treated by the FTC as an unfair or deceptive trade practice subject to civil penalties as outlined by § 5 of the FTC Act.[91] Following the enactment of this legislation, the health care industry began implementing the use of health information technology and digital health records.[92]

In addition to authorizing the HBNR, the Recovery Act instructed the FTC and the HHS to produce a study on potential privacy, security, and breach notification requirements.[93] But the agencies never produced the study, and the Rule was not enforced once in the first eleven years following its promulgation.[94] The lack of enforcement over the decade does not appear to be intentional; a review of the agency's annual report shows that the FTC was focused on pharmaceutical mergers, price inflation generally, the real estate market, and a multitude of other pertinent topics at the time.[95] Direct-to-consumer health apps and related devices were hardly in existence and did not raise significant HBNR enforcement concerns in 2009, but they quickly gained expansive commercial popularity over the following decade. For example, one of the most popular D2C healthcare products among US consumers is fitness trackers. The first major digital activity tracker with a connected app, the Fitbit Tracker, was released in 2009, followed by the Apple Watch in 2015.[96] Since 2010, Fitbit has sold over 143 million devices worldwide and counted around 128 million registered users in 2023, while an estimated thirty-eight

89. 16 C.F.R. § 318.5 (2024).

90. *See* Pub. L. 111—5, *supra* note 20, § 13407(g)(2). ("If Congress enacts new legislation establishing requirements for notification in the case of a breach of security, that apply to entities that are not covered entities or business associates, the provisions of this section shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.").

91. 15 U.S.C. § 45(a).

92. *See From Paper to Digital: The History of Healthcare Communication*, KNO2, (Aug. 15, 2024), https://kno2.com/from-paper-to-digital-the-history-of-healthcare-communication/ ("The HITECH Act of 2009 provided significant financial incentives for the adoption of [electronic health records] . . . Interoperability was a key component of [the incentive] criteria, driving further advancements in data exchange capabilities.").

93. *See* ARRA, *supra* note 20, at 42 U.S.C. § 17953.

94. *See* Fair, *supra* note 14.

95. FTC Annual Report, 2009, https://www.ftc.gov/sites/default/files/documents/reports_annual/annual-report-2009/2009ftcrptsv_0.pdf.

96. Peter Rubin, *How Fitbit Started the Wearables Craze That Got Us All Moving*, WIRED (Sep. 15, 2018), https://www.wired.com/story/how-fitbit-got-us-all-moving/.

million people owned an Apple Watch by 2023.[97] Despite this rapid expansion of health technology, the FTC did not enforce the HBNR against these devices until several years later.

B. 2020–2024 ENFORCEMENT AND UPDATES

Following a routine decennial review of the Rule in 2020,[98] the FTC issued a Policy Statement announcing the agency's intent to enforce the dormant Rule and putting businesses on notice to comply with the Rule.[99] The Statement clarified that the Rule was originally created to ensure that businesses or entities that are not covered by HIPAA because they are not "health plans," "healthcare providers," "healthcare clearinghouses," or specific "business associates" of "covered entities" nevertheless "face accountability when consumers' sensitive health information is compromised."[100] The Statement did not explain why the Rule was not enforced in the first ten years of its existence, but noted that "the explosion in health apps and connected devices makes its requirements concerning them more important than ever."[101] With this Statement, the Commission stated for the first time that developers of health applications and connected devices are covered by the Rule. The Statement did not yet suggest that the Commission intended to change the language of the Rule. The Policy Statement was only intended to "clarify the scope of the Rule, and place entities on notice of their ongoing obligation to come clean about breaches."[102] The Commission also cited business guidance and an interactive tool that had been previously used to put nontraditional vendors of "personal health records" on notice of their responsibility in light of a "breach of security."[103]

The Statement was approved by a 3-2 vote, across party lines—the two Republican Commissioners both dissented from the Statement, citing procedural concerns with what they viewed as an unauthorized expansion of

97. Statista Research Department, Fitbit-Statistics & Facts, STATISTA (Oct. 16, 2024), https://www.statista.com/topics/2595/fitbit/#topicOverview; *See also* David Curry, *Apple Statistics (2025)*, BUS. OF APPS, https://www.businessofapps.com/data/apple-statistics/ (last visited May 3, 2025).

98. *See* Retrospective Review of FTC Rules and Guides, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/rulemaking/retrospective-review-ftc-rules-guides (finding that since 1992, the FTC has conducted a review of existing Rules every 10 years).

99. *Statement of the Commission on Breaches by Health Apps and Other Connected Devices*, FED. TRADE COMM'N (Sep. 15, 2021).

100. *Id.*

101. *Id.*

102. *Statement of the Commission on Breaches by Health Apps and Other Connected Devices*, *supra* note 99.

103. *Id.*

FTC authority.[104] Because Congress did not explicitly intend for the Health Breach Notification Rule to cover technology like fitness trackers and health apps, the Republican Commissioners argued that the agency was expanding the scope of the Rule beyond the HITECH Act to include these health-related products.[105] However, if the FTC left the HBNR unenforced, the Rule would remain frozen in time and become a superfluous copy of the HIPAA rules. The FTC's enforcement of the HBNR properly captures the sorts of technologies that Congress had the foresight to imagine, even if it could not name them specifically in 2009. Digital records inevitably lead to new methods of accessing and organizing information, and it was reasonable to expect that consumers would be able to directly access this health information. The FTC's enforcement action against GoodRx demonstrates an application of the Rule that reflects Congress's intent in passing the HITECH Act.

1. GoodRx Enforcement Action

Two years after the Policy Statement, the Commission decided to enforce the 2009 Rule for the first time against GoodRx, a consumer-focused digital healthcare platform.[106] In the original February 1, 2023 complaint, submitted to a federal district court on the same day as the subsequent stipulated order, the Department of Justice brought the lawsuit "upon notification and on behalf of the [FTC]" for violations of § 5 of the FTC Act and the HBNR.[107]

The FTC alleged that GoodRx violated the statute and the Rule by engaging in deceptive and unfair trade practices and noted that GoodRx had 55.4 million users.[108] GoodRx's deceptive and unfair trade practices included actions such as violating its own privacy policy's promise that it would not share sensitive user information and sharing user data without notice or consent to advertising targeting platforms.[109] The sensitive health information at issue included GoodRx users' prescription medications and personal health conditions.[110] Notably, though it was not mentioned in the complaint or accompanying press release, this information would include birth control

104. *See* Dissenting Statement of Commissioner Christine S. Wilson Regarding the Policy Statement on Breaches by Health Apps and Other Connected Devices, FED. TRADE COMM'N MATTER NO. P205405 (Sep. 15, 2021).

105. *Id.*

106. *See generally* Goodrx Complaint, *supra* note 8.

107. 15 U.S.C. § 45(a)(1); *see* C.F.R. § 318; GoodRx Complaint, *supra* note 8, at 1.

108. *See generally* GoodRx complaint, *supra* note 8.

109. *Id.* at ¶ 38.

110. *Id.* at ¶ 8.

prescriptions and abortion pills.[111] Additionally, the Commission alleged that GoodRx's inaction, including a failure to implement sufficient policies or procedures to prevent the improper disclosure of sensitive health information and a failure to notify users of breaches, constituted unfair and deceptive practices.[112]

The FTC was first notified of GoodRx's data privacy practices by a *Consumer Reports* article in early 2020.[113] Within a month of the *Consumer Report* article, GoodRx created a new position, Vice President of Data Privacy, to oversee and coordinate the company's data privacy efforts and to limit data sharing.[114] The company also created an internal, written policy governing third-party data sharing.[115] Despite these changes, the FTC continued to investigate GoodRx to ensure its compliance with the Rule and eventually brought an enforcement action because the company continued to share personal health information with Facebook and other third-party platforms, in violation of the HBNR, until at least November 2020.[116] While the company quickly announced that Consumer Reports' "feedback" led them to update their policies in February 2020, the FTC found that GoodRx continued to violate the Rule by transmitting personal health information to Facebook pixel, a coding feature that allows Facebook to measure, optimize and build targeted ad campaigns, as late as November 2020.[117]

The FTC and GoodRx quickly reached a settlement agreement,[118] and a stipulated order granting the FTC's requested relief was issued by the United States District Court for the Northern District of California.[119] The settlement agreement included a $1.5 million civil penalty for GoodRx and a stipulated

111. Sarah Gupta, *5 Steps to Getting Birth Control Without Seeing a Doctor*, GOODRX (Mar. 1, 2024), https://www.goodrx.com/conditions/birth-control/heres-how-to-get-birth-control-without-a-doctors-prescription.

112. Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. GoodRx Holdings, LLC, No. 3:23-cv-460, (N.D. Cal. Feb. 1, 2023).

113. Thomas Germain, *GoodRx Saves Money on Meds—It also Shares Data with Google, Facebook, and Others*, CONSUMER REPORTS (Mar. 6, 2020), https://www.consumerreports.org/health/health-privacy/goodrx-saves-money-on-medsit-also-shares-data-with-google-facebook-and-others-a6177047589/.

114. GoodRx Complaint, *supra* note 8.

115. *Id.* at ¶ 57.

116. *Id.* at ¶ 63.

117. *Id.* at ¶¶ 56–5, 63.

118. *See* HOOFNAGLE, *supra* note 28, at 111–12. Most FTC enforcement actions end in settlements. While this series of FTC actions is atypical, this settlement agreement is not.

119. Germain, *supra* note 113.

order that imposed "a flat-out prohibition on GoodRx sharing user health data with applicable third parties for advertising purposes."[120]

GoodRx released its own press release, stressing that the company did not admit any wrongdoing and generally disagreed with the FTC's "novel" enforcement of the HBNR.[121] GoodRx also stated that "the requirements detailed in the settlement will have no material impact on our business or on our current or future operations," but the FTC's continued investigation resulted in direct and immediate changes to how GoodRx handles personal health information.[122] Though the Consumer Report article played a significant part in highlighting GoodRx's privacy practices, the FTC's enforcement of the Health Breach Notification Rule effectively forced the company to honor its promise to consumers.

Additionally, GoodRx took issue with the FTC complaint's focus on the company's use of advertising tracking pixels, which are commonly used by many websites.[123] This, however, does not change the fact that the advertising tracking technology offers no meaningful opportunity for user consent and uses personal, identifiable information of consumers for purposes well beyond the services GoodRx offers.[124] The company also failed to notify consumers that their information could or would be used for anything other than finding affordable medical offerings.[125] This unauthorized disclosure of information, according to the FTC's interpretation of the 2009 Health Breach Notification Rule, is a violation of the Rule and an unfair or deceptive trade practice.[126]

2. Easy Healthcare (Premom App) Enforcement Action

On May 17, 2023, the FTC announced that it had settled its second enforcement action of the Health Breach Notification Rule against Easy Healthcare, the company behind an ovulation tracking and fertility health app,

120. *Id.*; *see also* Fair, *supra* note 14.

121. *GoodRx Response to FTC Settlement*, GOODRX, (Feb. 1, 2023), https://www.goodrx.com/corporate/business/goodrx-response-to-ftc.

122. *Id.*

123. *Id.*

124. *See* Rita Ganz, *Understanding GDPR Compliance of Tracking Pixel Declarations Using Privacy Filter Lists*, SWISS FED. INST. OF TECH. (ETH) ZURICH (Feb. 18, 2022); *see also* FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FED. TRADE COMM'N (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

125. Goodrx Complaint, *supra* note 8, at ¶ 7.

126. *See generally* GoodRx Complaint, *supra* note 8.

Premom.[127] The FTC's initial complaint largely mirrored the February complaint against GoodRx, stressing that the company had violated its own privacy policy by sharing users' personal health data with third parties for advertising without user notice and consent and failed to implement written policies to address breach concerns created by the third-party usage.[128] In particular, Easy Healthcare allegedly failed to encrypt data that it shared with third parties or notify consumers of the unauthorized disclosures.[129] In the settlement, Easy Healthcare agreed to a $100,000 civil penalty and agreed to certain compliance reporting practices and requirements.[130] Easy Healthcare's Response to the FTC settlement was not specific and did not directly address the allegations in the complaint or stipulated order.[131]

3. Comparing the FTC's First Two HBNR Enforcement Actions

The FTC's first HBNR enforcement actions against GoodRx and Easy Healthcare highlight interesting developments in the FTC's approach to enforcing information privacy protections under the direction of former Chair Lina Khan. First, both enforcement actions address poor data security practices, such as the failure to notify users that third parties have access to their data, as unauthorized disclosures constituting "breaches of security" under the definitions provided in the HITECH Act and the agency's 2009 Rule.[132] This is an atypical conception of a security breach in a data privacy context because, historically, the term typically applies to cybersecurity hacks by an outside third party, rather than the intentional disclosure of sensitive information by the company authorized to collect the information for a consumer service.[133] This approach to data privacy violations centers the consumer, by identifying the business collecting consumer information as the

127. *See generally* Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corporation, No. 1:23-cv-3107 (N.D. Ill. June 22, 2023).

128. Complaint for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corporation, No. 1:23-cv-3107 (N.D. Ill. May 17, 2023).

129. *Id.* ¶ 32.

130. *See* Easy Healthcare Complaint, *supra* note 128.

131. *Easy Healthcare's Response to the FTC Settlement*, PREMOM (May 17, 2023), https://premom.com/ftc-response/.

132. Pub. L. 111–5, *supra* note 20.

133. *See Security Breach Definition*, CAMBRIDGE DICTIONARY (2024), https://dictionary.cambridge.org/us/dictionary/english/security-breach (defining a security breach as "a failure in a system that is intended to protect a person, building, organization, or country against threats such as crimes or attacks." This definition assumes an outside party always causes the breach).

perpetrator of the violation when they disclose sensitive information without authorization from consumers.

Second, both actions were enforced against companies handling sensitive health data related to reproductive health, fertility, and abortion access. These actions were enforced within a year of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, which overturned *Roe v. Wade* and eliminated the constitutional right to abortion.[134] Given this timing, the FTC's enforcement actions can reasonably be seen as responsive to the *Dobbs* decision and subsequent state actions taken to criminalize abortion.[135] At least thirteen states have outlawed abortion entirely, and another twelve states have enacted laws or policies that restrict or prohibit access to abortion care.[136] The FTC's enforcement actions under the Health Breach Notification Rule limit the likelihood of data leaks from private businesses publicizing whether someone sought or obtained an abortion. Such information, once obtained by states that criminalized abortion after *Dobbs*, could be used to prosecute people for health choices that they reasonably expected to remain private. The HBNR privacy protection is legally sound beyond the abortion context, but the decision to enforce the protection for the first time against purveyors of sensitive reproductive health information is an unusual development for the FTC, which has historically been considered apolitical.[137] In October 2024, the House Committee on Oversight and Accountability published a staff report alleging that FTC Chair Lina Khan "has consistently betrayed the obligation of the Commission to be an independent, bipartisan agency" through a slew of Democratic policies.[138] Remarkably, the report did not mention the FTC's "political" enforcement of a facially neutral rule on a hot-button issue as an example of Chair Khan's break from the FTC's "mandate of nonpartisanship, impartiality, and independence."[139]

Finally, both actions preceded any updates to the Health Breach Notification Rule, which were introduced and finalized a year after these settlements. The fact that each enforcement action and settlement occurred before the HBNR was modified is significant because the settlements indicate

134. *See generally* Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).

135. *After Roe Fell: Abortion laws by State*, CTR. FOR REPROD. RTS. (2024) https://reproductiverights.org/maps/abortion-laws-by-state/.

136. *Id.*

137. *See* HOOFNAGLE, *supra* note 28, at 9–11.

138. *Oversight Committee Releases Staff Report Finding FTC Chair Khan Abused Authority to Advance the Biden-Harris Administration's Agenda*, U.S. HOUSE COMM. ON OVERSIGHT & ACCOUNTABILITY 4 (Oct. 31, 2024), https://oversight.house.gov/wp-content/uploads/2024/10/HCOA-Majority-Staff-Report-FTC-Investigation.pdf.

139. *Id.* at 16.

that the Rule was sufficiently enforceable before the FTC updated the Rule in 2024. The Commission referenced insights from the two businesses when it decided to update the Rule. The updates clarify the scope and associated definitions of the Rule to provide covered businesses and entities with clear, direct notice. The update to the Rule was reasonable because businesses, law firms, privacy experts, and consumer protection organizations remained uncertain about the applicability of the HBNR following the FTC's 2021 Policy Statement announcing the intention to enforce the Rule.[140]

4. 2024 Updates to the Health Breach Notification Rule

Following the FTC's first-ever HBNR enforcement action in 2023, the updated Health Breach Notification Rule was finalized in May 2024 ("Final Rule").[141] The notice-and-comment period of updating the HBNR also provided affected businesses with an opportunity to comment on and raise their concerns about the FTC's future enforcement of the rule. Among other things, the updates (i) clarified what it means for a vendor of PHR to draw PHR identifiable health information from multiple sources, (ii) revised the definition of breach of security to clarify that a breach of security includes data security breaches and unauthorized disclosures, and (iii) extended the Rule's timing requirement for notifying the FTC of a breach of security.[142] These amendments addressed concerns raised in more than one hundred comments submitted during the Rule's notice-and-comment period before the Final Rule was announced.[143] The changes also add clarifying language to help businesses know whether they are expected to comply with the Rule, and specific

140. Mariah Bellamoroso, *FTC Signals Move Towards Tighter Data Privacy for Healthcare Apps*, HARV. J. L. & TECH. (Nov. 6, 2021), https://jolt.law.harvard.edu/digest/ftc-signals-move-towards-tighter-data-privacy-for-healthcare-apps.

141. 16 C.F.R. § 318, *supra* note 19.

142. *See* Health Breach Notification Rule, 89 Fed. Reg. 47028, 47029 (May 30, 2024) (16 C.F.R. § 318). The full suite of amendments to the 2024 HBNR (1) clarify the Rule's scope, including its coverage of developers of many health applications ("apps"); (2) clarify what it means for a vendor of personal health records to draw personal health record (PHR) identifiable health information from multiple sources; (3) revise the definition of breach of security to clarify that a breach of security includes data security breaches and unauthorized disclosures; (4) revise the definition of PHR related entity; (5) modernize the method of notice; (6) expand the content of the notice; (7) extend the Rule's timing requirement for notifying the FTC of a breach of security; and (8) improve the Rule's readability by clarifying cross-references and adding statutory citations, consolidating notice and timing requirements, articulating the penalties for non-compliance, and incorporating a small number of non-substantive changes.

143. *Id.*

requirements for how to do so.[144] In particular, the FTC clarified that only PHR-related entities are subject to the HBNR, and they include entities offering products and services through any online service, including mobile applications, if they access or send unsecured PHR identifiable health information.[145] Third parties that may access unsecured PHR in their course of business are not PHR-related entities simply because they have access to sensitive information.

IV. ANALYSIS

This Part explains the FTC's subsequent updates to the HBNR following its first two enforcement actions and highlights the significance of the HBNR as an effective privacy provision. Section IV.A outlines the primary criticisms of changes to the HBNR, including the updated definitions of "breach" and "health care providers." Sections IV.B and IV.C consider the critiques of updated definitions in the 2024 HBNR and highlight the significance of the HBNR's enforcement amidst the proliferation of D2C health care options. Section IV.D examines the potential impact of a recent Supreme Court holding that curtails some federal agency enforcement capabilities. Finally, Section IV.E suggests improvements for further enforcement of the HBNR and takeaways from the HBNR that can create an effective and more cohesive federal privacy framework.

A. CRITICISMS OF THE 2024 HEALTH BREACH NOTIFICATION RULE

After the Final Rule was promulgated, Republican Commissioners Melissa Holyoak and Andrew Ferguson published another dissent regarding the new HBNR, citing concerns about the substance, scope, and the FTC's authority to enforce the Rule.[146] In particular, they raised concerns that the Rule exceeds the commission's statutory authority by broadening the definitions Congress provided in the HITECH Act.[147] This criticism fails to recognize the congressional acknowledgment in 2009 that new technologies would continue to emerge and escape privacy regulation, and that the FTC was entrusted with the responsibility to promulgate a Rule that avoids that outcome. The updated definitions do not create punitive measures against covered health care

144. *See* Health Breach Notification Rule, 89 Fed. Reg. 47028, 47044 (May 30, 2024) (16 C.F.R. §. 318).

145. *Id.*

146. Fed. Trade Comm'n, Statement of Commissioner Melissa Holyoak, Joined by Commissioner Andrew Ferguson on the Health Breach Notification Rule, File No. P205405 (Apr. 26, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/p205405_hbnr_mhstmt_0.pdf.

147. *Id.*

providers under the HBNR—they clarify which entities are expected to comply with the Rule now that so many exist and remain in high demand after the COVID-19 pandemic.[148]

The dissent also noted that the Rule imposes affirmative obligations on companies to notify their service providers if they are covered by the Final Rule, regardless of whether they experienced an external breach.[149] This affirmative obligation is a minimal addition to other disclosures that businesses typically share with third parties; it only requires that third parties are put on notice that at least some of the data to be shared across companies includes sensitive PHR information.[150] Furthermore, the Rule only requires further action in the event of intentional, unauthorized disclosures of user information to capture more than external cyber hacks to reflect an updated understanding of breaches as they relate to individual users, rather than defining breach only from the perspective of the business housing the private information.[151] Data privacy experts today define a breach generally as "the unauthorized exposure, disclosure, or loss of personal information."[152] This updated definition reflects changes in the data privacy industry and accurately reflects the sort of privacy risks that consumers face today. In addition to criminal intrusions onto company data, a company entrusted with sensitive consumer health information can violate consumer privacy expectations by sharing that unencrypted information with a third-party advertiser or data broker.

Finally, the Commissioners argued that the Rule puts companies at risk of perpetual non-compliance and may undermine institutional integrity by artificially broadening its scope without clarity. In particular, they argue that unclear definitions of terms like "health care provider" cause confusion about who the Rule applies to.[153] Congress defined providers as "a provider of medical or other health services" and "any other person furnishing health care services or supplies," which encompasses both HIPAA-covered entities and entities that would only be regulated by the HBNR.[154] The new HBNR specifies which entities are non-HIPAA covered "healthcare providers" in part by whether or not they house unsecured PHR identifiable health information,

148. *See generally* Bestsennyy, *supra* note 3. Many Americans turned to telehealth providers for mental and physical health during the height of the COVID-19 pandemic, when most states had imposed stay-at-home orders and enforced quarantine requirements.

149. Holyoak, *supra* note 146.

150. Health Breach Notification Rule, 89 Fed. Reg. 47028, 47044 (May 30, 2024) (16 C.F.R. § 318).

151. *Id.*

152. *Id.*

153. Holyoak, *supra* note 146.

154. Pub. L. 111-5, *supra* note 20.

simplifying which businesses must comply with the HBNR.[155] Furthermore, these semantic concerns are a natural and well-anticipated part of regulating a rapidly changing industry. After all, Congress intended for consumers to learn of breaches of their unsecured PHR identifiable health information that fall outside HIPAA; the changes to the definitions in the HBNR help ensure consumers will receive the notification Congress intended.[156] To the extent that the FTC cannot provide a Rule that perfectly defines every possible violator, the agency can use other administrative tools, such as policy statements and notices, to further draw the line between a tangential health connection and a covered "health care provider" for purposes of the Rule and its enforcement.

B. SIGNIFICANCE OF THE 2024 HBNR "BREACH OF SECURITY" DEFINITION

Perhaps the most significant change in the 2024 HBNR ("modernized Rule") is that the HBNR makes an intentional, unauthorized disclosure by an entity a "breach of security" and a violation of the Rule.[157] For example, GoodRx and Easy Healthcare's decisions to share information with third-party ad platforms without notice to consumers are violations of the HBNR.[158] Historically, experts in privacy law have defined "breaches of security" as issues raised when an entity experiences a hack or some other nefarious seizure of information by an unknown or unapproved third party.[159] Many privacy experts, researchers, policy advocates, and even state lawmakers recognize that a breach of information privacy, as it relates to an individual user, extends beyond this traditional model.[160] Even the HITECH Act defines the term "breach" generally as the "unauthorized acquisition, access, use, or *disclosure* of

155. 16 C.F.R. § 318.2.

156. Health Breach Notification Rule, 89 Fed. Reg. 47028, 47034 (May 30, 2024) (16 C.F.R. § 318).

157. 16 C.F.R. 318.2 (2024); *see also* Health Breach Notification Rule, 89 Fed. Reg. 47028, 47029 (May 30, 2024) (16 C.F.R. § 318) ("The Commission further clarified that health apps and other products experience a "breach of security" under the Rule when they disclose users' sensitive health information without authorization; a breach is "not limited to cybersecurity intrusions or nefarious behavior.").

158. *See supra* Part II.

159. *See* CAMBRIDGE DICTIONARY, *supra* note 134.

160. *See, e.g.*, *Data Breaches*, NAT'L ASS'N OF ATT'YS GEN., https://www.naag.org/issues/consumer-protection/consumer-protection-101/privacy/data-breaches/ ("A data breach can be defined as the unlawful and *unauthorized* acquisition of personal information that compromises the security, confidentiality, or integrity of personal information." (emphasis added)).

protected health information which compromises the security or privacy of such information."[161]

The new breach definition in the HBNR better fulfills the goals of breach notification rules; it is a stronger measure to curtail poor data practices that are not the result of traditional cybersecurity, like phishing or hacking. This definition also centers around the stakeholders who suffer the most harm when a breach occurs: the individual whose sensitive health information was disclosed for any number of uses without their permission. The FTC has fulfilled its congressional mandate in the HITECH Act by creating an enforceable sectoral privacy rule that addresses historical and contemporary understandings of security breaches. By promulgating and enforcing the HBNR with this breach definition, the FTC holds businesses accountable for their privacy practices that allow for breaches of consumer privacy to happen, including decisions to share identifiable information without the approval or knowledge of the consumer.

C. SIGNIFICANCE OF THE ENFORCEMENT ACTIONS

In addition to being one of only a few entities empowered to protect consumers' data privacy, the FTC is one of the only sources of privacy jurisprudence at all, especially for federal privacy regulations.[162] As discussed by U.S. privacy law scholars Daniel Solove and Woodrow Hartzog, "in practice, the FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or any common law tort."[163] Most, if not all the aforementioned jurisprudence consists of settlement agreements rather than case law, leaving observers without a workable information privacy doctrine.[164] Solove and Hartzog argue that the FTC's decades of settlement agreements for privacy violations should be treated as common law to highlight certain norms and standards that are considered baseline privacy protections.[165] While FTC settlement agreements are the primary source of standards and expectations of consumer privacy, these actions are often too case-specific to provide meaningful recommendations for future cases.[166]

161. 42 U.S.C. § 17921(1)(A) (emphasis added).

162. *See supra* Section II.A.

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

164. *Id.*

165. *Id.* at 625.

166. *See, e.g.*, Easy Healthcare Stipulated Order, *supra* note 22. The settlement does not require a federal court to reach a conclusion as to whether the company's behavior is definitely

Regardless of whether the FTC's settlement agreements can or should be treated as common law, it remains clear that little precedent exists for federal privacy enforcement, and the FTC's more robust enforcement of the Health Breach Notification Rule can help further develop a significant body of privacy policies and law. However, robust enforcement is unlikely in the next four years due to a change in presidential administrations and FTC Chairs. In 2025, President Donald Trump appointed Andrew Ferguson to replace Lina Khan as Chair of the FTC.[167] Ferguson dissented from the FTC's updates to the HBNR, so it is unlikely that the FTC will continue to enforce the HBNR under Ferguson's leadership.[168]

The FTC's failure to enforce the HBNR over the next four years would have a significant effect on consumers because the agency would effectively eliminate a rare federal protection and remedy from business practices that expose consumers to harm. In many cases, consumers have no choice but to rely on the FTC to enforce the HBNR because they otherwise lack the individual ability to redress digital privacy injuries.

In 2021, the Supreme Court "significantly undermined the effectiveness of many privacy laws" by nullifying certain private rights of action due to a lack of standing.[169] In *TransUnion LLC v. Ramirez*, the Court held that a subset of a class of plaintiffs lacked Article III standing to sue a credit reporting agency for violations of the Fair Credit Reporting Act because they failed to demonstrate that their privacy injuries were concrete.[170] Specifically, their asserted harm was not similar to any harm "traditionally recognized as providing a basis for a lawsuit in American courts" and lacked a close historical or common law analogue for the asserted injury.[171] This ruling makes enforcing privacy rights increasingly difficult because "traditionally recognized" is a vague legal standard, and it most likely means that privacy lawsuits dealing with technology are much less likely to find standing in court since they do not have a long historical analogue that the Court is willing to recognize.[172]

---

a violation of the HBNR as the FTC alleges. This, in effect, leaves the FTC's application of the HBNR uncontested as applied to these facts, without expanding upon the FTC's rationale.

167. *Andrew N. Ferguson Takes Over as FTC Chairman*, FED. TRADE COMM'N, (Jan. 22, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/andrew-n-ferguson-takes-over-ftc-chairman.

168. *See supra* Section IV.A.

169. Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of TransUnion, LLC v. Ramirez*, 101 B.U. L. REV. ONLINE 62, 62 (2021); *see also* TransUnion LLC v. Ramirez, 594 U.S. 413 (2021). This holding limited many consumers' standing to sue for infringements of their privacy.

170. *TransUnion*, 594 U.S. 413 (2021).

171. *Id.*

172. *See* Solove, *supra* note 169.

After *TransUnion*'s Court-induced limitation on the ability of consumers to bring private lawsuits to assert and enforce their data privacy rights, consumers must rely on rules enforced by federal agencies, primarily the FTC and HHS, to enforce their data privacy rights. At the same time, all federal agencies face concerns about the ability to impose their rules with the force of law, especially after *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.* was overturned in 2024, ending the discretion that federal agencies enjoyed when interpreting ambiguous statutes based on their particular expertise.[173] Section IV.D considers the impact of the *Loper Bright* decision on the FTC's interpretation of the HBNR. When actively enforced, the FTC Health Breach Notification Rule provides a path for consumer relief and prevention of privacy harms that they themselves cannot raise in a court of law.

Additionally, the Commission's ability to enforce the Health Breach Notification Rule allows for more immediate changes in company conduct and self-governance. Through civil penalties and court-approved injunctions on unfair and deceptive business practices, the FTC's enforcement of the HBNR brings about a direct change for consumers. The combination of investigations, penalties, notification requirements, and public settlements causes businesses facing enforcement actions to make responsive changes to comply with the law and avoid future liability. These immediate actions include hiring data privacy professionals, establishing an internal system to avoid unnecessary and unauthorized disclosures of information to third parties, and routine review of the company's privacy practices.[174] The HBNR's ability to cause immediate and direct change to business behaviors that improve the consumer experience aligns with the FTC's general mission to combat bigness and its negative effects on the public.

Finally, though the FTC always requires that no more than three members of the Commission belong to the same party, the Rule's enforcement history until 2024 highlights a different political divide arising in the typically apolitical agency.[175] There is an underlying politicism in the fact that the first two enforcement actions were against companies that were careless with access to and disclosure of personally identifiable reproductive health information. While many onlookers have noticed that the agency has been criticized as politically extreme under former Chair Lina Khan, few have highlighted the

173. Loper Bright Enters v. Raimondo, 603 U.S. 369 (2024).

174. *See, e.g.*, GoodRx Settlement, *supra* note 113.

175. *See* Winerman, *supra* note 25, at 59; *see also* Will Weissert & Christopher Rugaber, *Trump Fires 2 Democrats on the Federal Trade Commission, Seeking More Control over Regulators*, ASSOCIATED PRESS (Mar. 18, 2025) (showing that in the first 100 days of the second Trump administration, the FTC has become even more politicized when President Trump fired Democratic commissioners Alvaro Bedoya and Rebecca Kelly Slaughter without cause).

significance of the FTC's HBNR enforcement as an example of the agency's political motives.[176] The FTC's protection of reproductive health privacy after the Supreme Court struck down the federal right to abortion further demonstrates the significance of the harms that consumers face when their digital privacy is compromised. Whereas privacy actions on behalf of individual consumers often lack a concrete harm that provides standing to bring a lawsuit, the political divide on reproductive health produces a significant risk of concrete harm when data is leaked that confirms, for example, that a resident of an anti-abortion state accessed the abortion pill through an online provider like GoodRx.[177] Given the likelihood that Ferguson's FTC will not enforce the HBNR with nearly as much rigor, if at all, it is not yet clear how this underlying politicization in the FTC will further change the agency's approach to privacy enforcement.

D. *LOPER BRIGHT* CONCERNS

Considering the Court's recent decision in *Loper Bright Enterprises v. Raimondo*, every federal agency, including the FTC, faces potential restrictions on its ability to promulgate and enforce rules if it relies too heavily on the agency's interpretation of an ambiguous statute ("*Chevron* deference").[178] While the FTC is sure to face continued legal objections to how it enforces certain rules, the Commission is well within its statutory duty to enforce the HBNR, even without *Chevron* deference, by interpreting the statute creating the HBNR. The statute authorizing the Rule is not ambiguous, but the updated Rule may be subject to review as to whether enforcement of the "modernized" language goes beyond the scope of authority that Congress intended. Newly installed Chair Ferguson agrees with this sentiment, as demonstrated by his dissent from the Final Rule, but this alone does not put the Rule at risk of elimination, especially because the FTC can simply choose not to enforce the HBNR without more instruction from Congress.

A comparison of the HBNR to the FTC's recent Noncompete Rule and its legal challenges provides an illustrative example of why the updated HBNR is likely not a breach of agency authority. On April 23, 2024, the FTC finalized the Noncompete Rule, which "adopts a comprehensive ban on new noncompetes with all workers," including senior executives.[179] The Rule was set to become effective in September 2024, but in August, a federal judge in

176. *See, e.g.*, House Oversight and Accountability Committee Report, *supra* note 138.

177. *See, e.g.*, Texas Heartbeat Act (Texas Health & Safety Code §§ 171.201–171.212) (authorizing private citizens to sue various stakeholders for violating or assisting in the violation of the state's restrictive anti-abortion laws).

178. GoodRx Settlement, *supra* note 113.

179. FTC Noncompete Rule, 16 C.F.R. §§ 910, 912.

the Northern District of Texas blocked the Rule with a nationwide injunction by siding with Ryan, LLC, a Dallas, Texas-based tax services provider and related co-Plaintiffs.[180] The FTC argued that the challenged Rule was within its authority to establish rules related to "unfair methods of competition" under § 6 and that noncompete agreements are unfair methods of competition under § 5 of the FTC Act.[181] Furthermore, the FTC based the promulgation of the Rule on its findings and conclusions after years of investigation, public hearings, and review of academic studies.[182] The district court rejected this argument and concluded that the FTC exceeded its statutory authority because the Commission's ability to promulgate rules concerning unfair methods of competition does not explicitly include the authority to create *substantive* rules regarding unfair methods of competition.[183] As a result, the Noncompete Rule as a method of combating an unfair method of competition is not enforceable by the FTC because it is a substantive and not procedural rule, thus exceeding the FTC's rulemaking authority in this area of law and policy.[184] The district court concluded that this result is further supported by the fact that § 6(g) rulemaking authority does not have a penalty provision, while § 18 does.[185]

Conversely, the HBNR finds initial authority in § 18 of the FTC Act, which in turn authorizes civil penalties in § 5.[186] The rulemaking authority in § 18 applies to the creation of substantive rules dealing with unfair or deceptive practices—not unfair methods of competition.[187] Furthermore, Congress specifically instructed the Commission to create and enforce the Health Breach Notification Rule in the HITECH Act.[188] Congress expressly delegated the enforcement of the provisions in § 13407 to the Commission. Under these circumstances, the court would review a challenge to the Rule by recognizing the constitutional delegation and "ensuring the agency has engaged in reasoned decision-making."[189] In the process of updating the HBNR, the Commission updated the Rule in an effort to honor Congress's mandate by clarifying the

180. Ryan, LLC v. Fed. Trade Comm'n, 746 F. Supp. 3d 369, 370 (N.D. Tex. Aug. 20, 2024).

181. 15 U.S.C. § 57(a).

182. *Ryan, LLC*, 746 F. Supp. 3d at 377.

183. *Id.* at 384 ("By plain reading, Section 6(g) of the Act does not expressly grant the Commission authority to promulgate substantive rules regarding unfair methods of competition" because it only allows the FTC to "make rules and regulations for the purpose of carrying out the provisions of this subchapter. 15 USC § 46(g).").

184. *Id.*

185. *Ryan, LLC*, 746 F. Supp. 3d at 385.

186. *See supra* Part II.

187. 15 U.S.C. § 57(a).

188. *See supra* Part II.

189. *Loper Bright*, 603 U.S. at 395.

Rule's scope and several definitions, and providing more time to comply with the notice requirement of the Rule following a breach.[190] Additionally, the House Judiciary Committee reviewed the FTC's proposed amendments to the HBNR in its FTC oversight meeting and expressed no concerns with the Rule before its finalization.[191]

Finally, there is an additional significant distinction between the FTC's Noncompete Rule and the HBNR. In its final dismissal of the Noncompete Rule, the district court stated that "the Rule imposes a one-size-fits-all approach with no end date, which fails to establish a 'rational connection between the facts found and the choice made.'"[192] In contrast, the HBNR is directed to a specific audience of vendors of personal health records that are not covered by HIPAA, as Congress determined, and the Rule has a statutory research and guidance in the HITECH Act.[193] Because the FTC had express, statutory authority to promulgate and enforce the HBNR, it is much less likely to face the scrutiny that the Noncompete Rule did. Furthermore, the HBNR is unlikely to face scrutiny because it is unlikely to be significantly enforced in the foreseeable future.

E. SUGGESTED IMPROVEMENTS TO HBNR ENFORCEMENT GUIDANCE AND PRACTICES

The following improvements would help the FTC fend off challenges to its authority and related resistance to its HBNR enforcement actions, which are ultimately meant to promote compliance and reduce injuries to consumers caused by a business's unfair or deceptive trade practices. These suggested improvements include further defining nontraditional health care providers for the purposes of the HBNR and exploring less aggressive administrative remedies in edge cases.

1. Distinguishing Between Traditional and Nontraditional Health Care Providers and Related Definitions to Provide Fair Notice

Many of the definition changes in the modernized Rule to terms related to health were intended to capture non-HIPAA health care providers.[194] Similarly, the Commission noted that it intentionally retained or added catchall terms that do not expand the original Rule's breadth but instead address existing

190. *See* 16 C.F.R. § 318, *supra* note 13.

191. Rules of Practice for Adjudication Proceedings, Vol. 88, Fed. Reg. 18382 (2023) (12 C.F.R. § 1081).

192. *Ryan, LLC*, 746 F. Supp. 3d at 388.

193. Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 300jj; ARRA, *supra* note 20, at § 13405.

194. 16 C.F.R. § 318.2.

health technology "to ensure the Rule's language can accommodate future changes in technology."[195] Many of these changes follow logically from the proliferation of mobile phone health apps, which did not exist in 2009 when the HBNR was promulgated but nonetheless were clearly intended by Congress to be covered by the Rule.[196] The Rule sets an ambiguous standard for edge cases that make the Rule susceptible to challenges to its enforcement. When it is unclear whether an entity is a vendor of personal health records and therefore subject to compliance with the HBNR, the threshold inquiry is whether "an app, website, or online service must provide an offering that relates more than tangentially to health."[197]

This standard could cause enforcement issues in the future because the malleable standard is not predictable or clear enough when it comes to online or digital services that are arguably related to health. For example, in the same year that the FTC issued two enforcement actions against GoodRx and Easy Healthcare, the FTC also secured a settlement against BetterHelp, an online mental health counseling service.[198] The FTC alleged that BetterHelp engaged in deceptive trade practices by promising users that their information, including their mental health status and data from intake questionnaires used to match users with therapists, would remain private but shared unauthorized, identifiable personal health records with third parties for targeted advertising purposes.[199] However, the Commission did not invoke the HBNR in its complaint challenging BetterHelp's practices, though it seems that the deceptive behavior violated the 2009 Rule and the 2024 Rule by engaging in the same activities as other non-HIPAA covered health providers like GoodRx and Easy Healthcare. A month before the 2024 Final HBNR was announced, the FTC settled two more enforcement actions against an alcohol addiction treatment company, Monument, and a subscription-based telehealth platform, Cerebral.[200] In both cases, the FTC made consistently similar claims of "breach of security" and issued injunctions that banned both businesses from disclosing consumers' health information for targeted advertising purposes.[201]

195. Health Breach Notification Rule, 89 Fed. Reg. 47028, 47035 (May 30, 2024) (16 C.F.R. § 318).

196. *Id.*

197. *Id.*

198. Complaint, In the Matter of BetterHelp, Docket No. C-4796 (July 14, 2023).

199. *Id.*

200. *See generally* Complaint for Permanent Injunction; Civil Penalty Judgment, and Other Relief, United States v. Monument, Inc., No. 1:24-cv-01034, (D.D.C. 2024); Complaint, United States v. Cerebral, Inc., No. 1:24-cv-21376-XXXX (S.D. Fla. Apr. 15, 2024).

201. *Id.*

The enforcement actions resulted in quickly updated privacy policies in both companies, but neither enforcement action invoked the HBNR. Such inconsistent enforcement of the HBNR opens the FTC's enforcement up to more criticism and minimizes the FTC's ability to enforce a necessary privacy provision. This inconsistent enforcement also wastes opportunities to clarify the scope of D2C healthcare providers covered by the HBNR by not explicitly noting that the Rule applies to these entities or explaining why it does not. It is unclear why the FTC, in its aggressive enforcement of consumer privacy against these three D2C health-related companies, did not seek enforcement actions under the new Health Breach Notification Rule with clarified definitions and an extended period to comply.[202] The FTC should take steps to clarify discrepancies and maintain consistent enforcement of the HBNR to effectively put the affected businesses on notice and to provide Congress with a clean record of enforcement actions that can help inform other privacy notification statutes.

2. Administrative Hearings and Cure Notices as Measures to Respect Due Process

When an agency enforces a regulation or a statute, it must adhere to a fair notice standard of "ascertainable certainty," which has been endorsed by several circuits.[203] The standard provides that fair notice exists if a regulated party reviewing an agency regulation or statement "would be able to identify, with 'ascertainable certainty,' the standards with which the agency expects parties to conform."[204] While the FTC provided both a Policy Statement[205] before enforcing the HBNR and published a Notice of Proposed Rulemaking[206] before the 2024 Rule was issued and enforced, the rulemaking and enforcement timeline still raises some concerns about notice, a fundamental requirement of due process.[207] For example, in the HBNR's very short enforcement history, it has not been enforced consistently. When the FTC brought actions against D2C healthcare providers BetterHelp, Cerebral, and Monument for failure to protect consumers' health information, it did not

202. 16 C.F.R. § 318.4.

203. *See, e.g.*, Gen. Elec. Co. v. Env't Prot. Agency, 53 F.3d 1324, 1329 (D.C. Cir. 1995).

204. *Id.*

205. *See* 2021 Policy Statement, *supra* note 99.

206. FTC Health Breach Notification Rule Notice of Proposed Rulemaking, 16 C.F.R. § 318.

207. U.S. CONST. amend. V ("No person shall . . . be deprived of life, liberty, or property, without due process of law.").

allege an HBNR violation.[208] Each of these enforcement actions was settled just months before the updated Rule took effect on July 29, 2024. It is unclear why the agency enforced these actions while updates to the Rule were nearly finalized. The amended Rule clarifies existing definitions and updates the Rule in response to modern realities, such as the time it takes to investigate a breach of privacy by an unauthorized third party, like a cybersecurity hack, but the updated Rule does not expand the scope of enforcement beyond vendors of personal health records.[209] Even though the Rule does not expand the scope of vendors handling personal health records and attempts to clarify its scope by providing entities with advance fair notice, the FTC's decision to continue enforcing the Rule while promulgating its updates raises a credible due process concern, especially for the businesses that settled with the FTC before it published its clearer, more explanatory version of the HBNR. Now that the FTC has finalized a clearer version of the old Rule, it should enforce the HBNR as consistently and transparently as possible to avoid future due process concerns. This caution is especially warranted considering recent Supreme Court decisions that chip away at the agency's enforcement capabilities and increasing public skepticism about the role and legitimacy of federal agencies.[210]

To address these concerns, when the FTC enforces the HBNR or any other privacy rule, the Commission should consider a notice-and-cure approach, which provides opportunities to comply with the HBNR before an enforcement action. The FTC should also consider adjudicative agency hearings in cases where the applicability of the HBNR is not clear from a plain reading of the Rule or any of the FTC's public statements. These cases may arise when the FTC targets entities whose business activities include both covered and non-covered functions. The HBNR makes no mention of hybrid entities, but the Department of Health and Human Services recognizes hybrid entities in its enforcement of the HIPAA Privacy Rule.[211] Under the HIPAA Privacy Rule, such an entity may elect to be designated as a hybrid entity and

208. Concurring Statement of Commissioner Christine S. Wilson Regarding BetterHelp, Fed. Trade Comm'n File No. 2023169. (Mar. 2, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/commissioner_wilson_concur_betterhelp_3.2.23.pdf.

209. Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 300jj; ARRA, *supra* note 20, at § 13405.

210. *See generally, e.g.*, *Loper Bright*, 603 U.S.; AMG Cap. Mgmt., LLC v. Fed. Trade Comm'n, 593 U.S. 67 (2021), Sec. & Exch. Comm'n v. Jarkesy, 603 U.S. 109 (2024).

211. *When Does a Covered Entity Have Discretion to Determine Whether a Research Component of the Entity is Part of Their Covered Functions, and Therefore, Subject to the HIPAA Privacy Rule?*, U.S. DEPT. OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/315/when-does-a-covered-entity-have-discretion-to-determine-covered-functions/index.html (last visited May 3, 2025).

must define and designate its health care component(s).[212] This distinction allows for clearer compliance expectations for the regulated entity and the agency by indicating which parts of the entity should reasonably be expected to comply with the HIPAA Privacy Rule before a breach ever occurs. Because the HBNR covers a more ambiguous category of vendors of consumer health data that falls outside HIPAA, many D2C businesses likely have hybrid or potentially hybrid models.

Notice-and-cure remedies typically apply to contracts, including contracts with the government. They alert businesses of the government's intent to end a contractual relationship due to the business's failure to comply with the conditions of the contract.[213] Government contracts are not the only place this strategy is employed. When the California Consumer Privacy Act (CCPA) was initially passed into law, the statute provided consumers with a right of action to sue businesses that failed to comply with the CCPA.[214] Prior to bringing suit, consumers were required to provide "a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated."[215] Unlike the CCPA, the FTC's HBNR is focused only on breach notification requirements, but an informal notice-and-cure approach may still be helpful to inform businesses as to whether they are a covered health care provider under the HBNR and may be subject to an HBNR enforcement action. Rather than burden the consumer with the responsibility of providing notice to businesses that may be out of compliance with the FTC HBNR, the FTC should issue notices to businesses to allow them to comply before facing civil penalties and permanent injunctions.[216] In particular, the FTC could send notices to potential hybrid entities that might arguably be identified as a "health care provider" for purposes of the statute. These notices would provide clearer compliance expectations for all parties, reduce pushback on the agency's enforcement power without diluting the consistency and enforcement power of the HBNR, and maintain the FTC's legitimacy as a federal institution. Additionally, the FTC should always welcome guidance and compliance questions from businesses making a good faith effort to comply with the statute.

212. *Id.*

213. *See, e.g.*, Delinquency Notices, 48 C.F.R. § 49.607.

214. Cal. Civ. Code § 1798.150.

215. *Id.*

216. Note that this proposed "notice-and-cure" method of compliance is a different compliance measure than a notice of penalty offense, which is "a document listing certain types of conduct that the Commission has determined, in one or more administrative orders (other than a consent order), to be unfair or deceptive in violation of the FTC Act." *Notices of Penalty Offenses*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/penalty-offenses.

In addition to an informal notice-and-cure approach, the FTC can also make use of administrative agency hearings. Rather than immediately file complaints seeking penalties and injunctions in federal district court, as the FTC did in GoodRx, Easy Healthcare, BetterHelp, Monument, and Cerebral, the agency should file complaints with an administrative law judge (ALJ).[217] This method would allow for a more detailed fact-finding process and remedy due process concerns by having a full examination before imposing a penalty.[218] Even if the Commission finds that there was a violation of the HBNR, the harshest penalty that the Commission can impose in an administrative hearing is a cease-and-desist order; the agency cannot proscribe the harsher penalties often sought in federal district court.[219] The agency does, however, retain the ability to seek a civil suit in a district court if the entity fails to comply with the cease-and-desist order.[220] The records from these proceedings can also provide further clarity to other businesses that are hesitant on sure how to obtain affirmative express consent from consumers when attempting to share their sensitive information or whether the business is a covered healthcare provider under the HBNR.

The FTC should provide clarity on the HBNR and its privacy enforcement by using the notice-and-cure approach and expanding the use of administrative hearings. These solutions would address due process concerns, provide material contributions to the development of federal breach notification and privacy rules, and encourage more businesses' cooperation, balanced by the possibility of further punitive measures in federal district court. These solutions are also better than maintaining stricter parameters within the HBNR, which would eliminate the necessary flexibility to adapt to changes in the direct-to-consumer healthcare industry. As applied to the HBNR, the legal maxim that hard cases make bad law rings true; the FTC should not restrict its enforcement capabilities under the HBNR because it cannot anticipate every kind of D2C healthcare provider that may face enforcement under the law. When these cases do arise, the FTC should apply less force to encourage learning and compliance, not punitive measures.

V. CONCLUSION

The Federal Trade Commission's revival and enforcement of the Health Breach Notification Rule shows promise for the future of data privacy protection, especially as it relates to sensitive health information. The original

217. *See* Rules of Practice for Adjudication Proceedings, *supra* note 191.
218. *Id.*
219. 15 U.S.C. § 45(b).
220. *Id.*

2009 Rule was created to complement the American public's increased reliance on digital services and personal records, which peaked during the 2019 COVID-19 pandemic. The updates to the HBNR acknowledge that reality. The FTC's updates to the HBNR reflect its purpose: to put covered entities on notice of their compliance requirements and confirm that they cannot enter the direct-to-consumer market without facing regulations that prioritize and protect consumer interests as it relates to their sensitive health information.

The HBNR's updates were within the FTC's statutory authority to make and were completed through a robust and democratic campaign of business guidance, congressional oversight, and more. While past Commissions have been reluctant to pursue consumer privacy regulations, the 2024 Commission demonstrated a commitment to producing meaningful and lasting change in consumer data privacy.