Harvard Journal of Law & Technology
Volume 39, Number 1 Fall 2025

M&A EXCEPTIONALISM IN PRIVACY LAW

*Erika M. Douglas**

ABSTRACT

This Article examines an important yet overlooked area of U.S. privacy law: the treatment of mergers and acquisitions ("M&A"). More than ever before, companies are buying and selling our personal data en masse through such corporate transactions. This Article offers the first descriptive and normative analysis of how U.S. privacy law applies to mergers and acquisitions. It argues that this law is underappreciating the significance of these transactions to our privacy in the digital era, and proposes action to fix this.

The Article begins by examining the privacy laws that might be expected to apply to such M&A. Instead, it finds widespread "M&A exceptionalism": the ordinary rules of privacy law often do not apply to personal data processing that occurs in mergers and acquisitions. Many federal sectoral and state privacy laws expressly exclude M&A from their rules that otherwise limit the sale and transfer of personal data. Where more general privacy law could apply to M&A, it is not being enforced against transactional privacy harms.

The Article then identifies and interrogates the drivers of this M&A exceptionalism, including: individualistic conceptions of privacy rights, the edification of corporate property interests in personal data, operational efficiency, and presumed consistency with reasonable expectations of privacy. It argues that while these reasons are not entirely misplaced, they tend to rely on a continuity fallacy that pervades privacy law, and are often outdated, or too general to support the current scope of privacy permissiveness toward M&A. Such M&A thinking is also difficult to reconcile with modern privacy concerns over opaque, bulk personal data sales in other contexts, like bankruptcy and data brokering.

Next, the Article adds factual support to the argument that privacy law underestimates M&A. It evaluates the privacy impact of fifteen personal data acquisitions by the world's largest technology companies,

---

* Associate Professor of Law, Temple University, Beasley School of Law. I would like to thank the participants of the 2025 Privacy Law Scholars Conference, particularly William McGeveran and Peter Swire, the participants of the 2025 Santa Clara Internet Law Works in Progress Conference, and the 2024 BYU Future of Antitrust Interdisciplinary Conference for their input on drafts of this Article, Tom Lin, Daniel Solove and Ryan Calo for their thoughtful suggestions on related literature and ideas, Jessie Hemmons for her outstanding research assistance and dedication throughout this project, as well as Valerie Wilson and Taylor Weilnau for their early research contributions. Any errors or omissions are my own.

using a comparison of the targets' privacy policies before and after each deal. This analysis finds that the effects of these deals on privacy are more variable and more harmful than privacy law assumes. Several of the acquisitions likely harmed privacy, because the target failed to obtain adequate consent to the deal, or the acquiror changed the policy post-acquisition to use personal data in unexpected ways. Others, though, appeared positive for privacy, resulting in clearer policy disclosures.

Finally, the Article offers answers on how to address M&A exceptionalism in privacy law. It proposes the first set of criteria for enforcers to screen mergers and acquisitions for privacy risk, outlines future research to understand the effects of M&A on privacy, and explains why such understanding is important to privacy law as a whole.

TABLE OF CONTENTS

I. INTRODUCTION

Consumer privacy advocates objected immediately when the social media company Facebook, now Meta, announced its acquisition of the online messaging company WhatsApp.[1] For years, WhatsApp had attracted users with its promises of better privacy protection than rival message services, and commitments not to allow data-driven advertising.[2] Facebook, a company notorious for privacy law violations and reliant on ads for its business model, seemed poised to break these promises after the acquisition.[3] The Federal Trade Commission ("FTC"), which is the primary enforcer of U.S. federal privacy law,

1. Complaint at 1–2, Elec. Priv. Info. Ctr. (EPIC) & Ctr. for Digit. Democracy (CDD), In the Matter of WhatsApp, Inc., Request for Investigation, Injunction and Other Relief (Mar. 6, 2014), https://epic.org/wp-content/uploads/privacy/ftc/whatsapp/WhatsApp-Complaint.pdf [https://perma.cc/3KBZ-B2MB] [hereinafter EPIC WhatsApp Complaint (2014)].

2. *Id.*; FTC Letter Re Facebook/WhatsApp from Jessica L. Rich, Dir. of the FTC Bureau of Consumer Prot., to Erin Egan, Chief Priv. Officer, Facebook, and to Anne Hoge, Gen. Couns., WhatsApp Inc. (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf [https://perma.cc/Y4M4-PZHN] [hereinafter FTC Facebook/WhatsApp Letter] ("WhatsApp has made a number of promises about the limited nature of the data it collects, maintains, and shares with third parties — promises that exceed the protections currently promised to Facebook users . . . . WhatsApp's privacy policy clearly states, among other things, that users' information will not be used for advertising purposes or sold to a third party for commercial or marketing use without the users' consent.").

3. Press Release, FTC, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises [https://perma.cc/E7L5-PJ3U].

took the milquetoast action of issuing a warning letter that informed the parties their failure to honor WhatsApp's privacy promises "could" violate federal privacy law.[4]

This non-binding agency action did little to protect user privacy. When the deal closed, it gave Facebook newfound access to the personal data of more than 450 million WhatsApp users.[5] Less than two years after the acquisition, the predicted privacy harms began to appear. Facebook announced changes to WhatsApp's privacy policy that would allow user identities to be linked across the services of WhatsApp and Facebook, enabling cross-service content feeds, targeted advertising, and the identification of personal contacts.[6] Still, the FTC did not bring enforcement action. It took until seven years after the acquisition for the agency to act, and even then its claims were framed in antitrust, not privacy law.[7]

The Facebook/WhatsApp saga offers a high-profile example of a widespread practice: the buying and selling of our personal data en masse through corporate transactions with little privacy oversight. These personal data-driven acquisitions abound in the modern economy.[8] Another notable example is Google's purchase of Fitbit, a fitness tracking company, through which Google obtained an estimated "181 billion hours of heart rate data, 9 billion nights of sleep, 457 billion minutes of exercise tracking, and 10 million [data points on] menstrual cycles and fertility windows."[9] Similarly, Amazon's purchase of Whole Foods gave the e-commerce acquiror sudden access to the

---

4. FTC Letter Re Facebook/WhatsApp, *supra* note 2 (stating "any use of WhatsApp's subscriber information that violates these privacy promises, by either WhatsApp or Facebook, could constitute a deceptive or unfair practice under the FTC Act").

5. Parmy Olson, *Facebook Closes $19 Billion WhatsApp Deal*, FORBES (Oct. 6, 2014), https://www.forbes.com/sites/parmyolson/2014/10/06/facebook-closes-19-billion-whatsapp-deal/ [https://perma.cc/YWF8-CTTM]; Jared Newman, *Facebook's WhatsApp Acquisition Explained*, TIME (Feb. 20, 2014), https://time.com/8806/facebooks-whatsapp-acquisition-explained/ [https://perma.cc/BVA2-XDY5].

6. Press Release, Eur. Comm'n, European Commission Fines Facebook €110 Million for Providing Misleading Information About WhatsApp Takeover (May 17, 2017), https://ec.europa.eu/commission/presscorner/detail/en/ip_17_1369 [https://perma.cc/246T-5NCJ] (describing Facebook's announced policy changes and plans for cross-service data matching); *see also* Complaint at ¶¶ 14–16, Elec. Priv. Info. Ctr. (EPIC) & Ctr. for Digit. Democracy (CDD), In the Matter of WhatsApp, Inc., Request for Investigation, Injunction, and Other Relief (Aug. 29, 2016), https://epic.org/wp-content/uploads/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf [https://perma.cc/9RDL-BS5Y] [hereinafter EPIC WhatsApp Complaint (2016)] (detailing plans for cross-service tailored marketing).

7. *See* FTC v. Meta Platforms, Inc., No. 1:20-cv-03590, at 69, 73–74 (D.D.C. Sep. 8, 2021). This ongoing litigation alleges that Facebook's acquisition of WhatsApp, among other deals, gave the company market power that it used to erode privacy-based competition.

8. *See infra* Appendix A.

9. Lucas Griebeler da Motta, Why We Should Be Careful About Google's Promises in the Fitbit Deal, PROMARKET (Aug. 21, 2020), https://www.promarket.org/2020/08/21/why-we-should-be-careful-about-googles-promises-in-the-fitbit-deal/ [https://perma.cc/B9MG-UB5W].

weekly grocery buying histories of millions of customers across the United States.[10] The FTC did not take privacy action against any of these transactions, though privacy and competition enforcers intervened in other jurisdictions.[11]

These billion-dollar deals reflect a new economic reality. Personal data is treated as a commercial asset, drawing analogies to oil or intellectual property in its immense value to corporations.[12] In the digital economy, a flood of data is produced on every aspect of our lives: our locations, online browsing, advertising views, driving, and even thermostat settings.[13] The largest technology companies in the world use this barrage of information to fuel online search, social media, advertising, and other digital services.[14] This new value of personal data is, in turn, driving the sorts of corporate transactions described above in which the crown jewels are personal data, and the consumer relationships necessary to collect more of it.

---

10. Whole Foods, Current Report (Form 10-K) (Nov. 18, 2016), https://www.sec.gov/Archives/edgar/data/865436/000086543616000366/wfm10k2016.htm [https://perma.cc/2F28-6S3U] (reporting Whole Foods is "the largest natural and organic foods supermarket in the U.S." with over eight million customer visits each week); *How Whole Foods Got Its Data Intelligence Strategy Right*, MERIT, https://web.archive.org/web/20230426065750/https://www.meritdata-tech.com/resources/blog/retail-data/whole-foods-data-intelligence/ [https://perma.cc/NP2W-VZL4] (archived Apr. 26, 2023).

11. Press Release, Eur. Comm'n, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions (Dec. 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484 [https://perma.cc/M7K4-9DWX] (imposing remedy of data segregation from Google for Fitbit user data); Autorità Garante della Concorrenza e del Mercato (It. Competition Auth.), WhatsApp Fined 3 Million Euro for Tricking Users Into Sharing Their Data with Facebook (May 12, 2017) https://en.agcm.it/en/media/press-releases/2017/5/alias-2380 [https://perma.cc/SBX4-GCYL].

12. *The World's Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/XS7D-CXJT]; Naren Gupta, *Data Is the New IP,* MEDIUM (Feb. 24, 2017), https://medium.com/nexus-collection/data-is-the-new-ip-d4764a1cf2f5 [https://perma.cc/HP2R-KJFM]; World Econ. F., *Personal Data: The Emergence of a New Asset Class* (2011) (recognizing data as a new asset class); Neelie Kroes, (Eur. Comm'n on Info. and Commc'n Tech. (ICT) Conf.), *Big Data for Europe* (Nov. 7, 2013), https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_13_893 [https://perma.cc/G9Q7-3AW4] ("[B]ig data is not just a new sector, but a new asset class. One that sits as a pillar of our economy, like human resources or financial capital.").

13. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 98–114 (2014) (cataloguing data-collecting smart devices); Gabriel Weinberg, *What Are the Biggest Tracker Networks and What Can I Do About Them?*, DUCKDUCKGO, https://spreadprivacy.com/biggest-tracker-networks/ [https://perma.cc/97YC-EZTR].

14. Jonathan Ponciano, *The World's Largest Technology Companies In 2023: A New Leader Emerges,* FORBES, (June 8, 2023) (including Alphabet Inc. (Google), Apple Inc., Microsoft Inc., Meta Platforms (Facebook) among the largest companies by revenue, profits, assets and stock market value); Swish Goswami, *What Does Big Tech Actually Do With Your Data?,* FORBES (Feb. 16, 2022), https://www.forbes.com/councils/forbestechcouncil/2022/02/16/what-does-big-tech-actually-do-with-your-data/ [https://perma.cc/9HBH-PR99].

Despite the rise of mass transfers of personal data through mergers and acquisitions ("M&A"),[15] these deals see almost no scrutiny in privacy law enforcement or scholarship.[16] The FTC's approach has changed little over the last decade — the agency recently issued another warning letter in Amazon's acquisition of One Medical, a membership-based medical care company with more than 800,000 patients, and mountains of personal health information.[17] These non-binding FTC

15. The term "acquisition" is primarily used throughout this Article to describe the types of corporate transaction examined, but the same logic will often apply to mergers, a term that is also used here from time to time. The distinction in corporate transactional forms, while important to corporate law, may be less so in evaluating privacy effects. *See infra* text accompanying notes 54–56 (finding that the form of corporate transaction does not necessarily dictate whether personal data processing occurs). The discussion here may also be applicable to other types of corporate transactions, such as joint ventures that expanded personal data access.

16. Most of the scholarship on corporate transactions and privacy focuses on more specific types of transactions, such as bankruptcy sales or secured transactions. *See* Christopher G. Bradley, *Privacy for Sale: The Law of Transaction in Consumer's Privacy Data*, 40 YALE J. ON REGUL. 127, 194–95 (2023) (examining privacy protections in bankruptcy transactions); Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 424 (2018) (examining the applicability of privacy law to the creation of security interests in personal data, and including analysis of bankruptcy protections); Lucy L. Thomson, *Personal Data for Sale in Bankruptcy: A Retrospective on the Consumer Privacy Ombudsman*, 34 AM. BANKR. INST. J. 58, 58 (2015); Luis Salazar, *Privacy and Bankruptcy Law*: *Part II: Specific Code Provisions*, 25 AM. BANKR. INST. J. 58, 58 (2007); Susan Jensen, *A Legislative History of the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005*, 79 AM. BANKR. L.J. 485, 485 (2005) (examining the history of the legislative amendments that introduced privacy protections into bankruptcy law). *But see* Reuben Binns & Elettra Bietti, *Dissolving Privacy, One Merger at a Time: Competition, Data and Third Party Tracking*, 36 COMPUT. L & SEC. REV. 1, 2 (2020) (applying competition law to select large technology transactions, focusing on firms active in the third-party tracking industry); Thomas Haley, *Illusory Privacy*, 98 IND. L.J. 75, 75 (2022) (analyzing contract law and privacy analysis of terms and conditions on popular websites and briefly addressing consent to acquisitions in the terms).

17. Press Release, FTC, Joint Statement of Chair Khan et al. Regarding Amazon.com, Inc's Acquisitions of 1Life Healthcare, Inc. (Feb. 27, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2210191amazononemedicalkhanslaughterwilsonbedoya.pdf [https://perma.cc/64XV-YHVG] ("Companies that fail to abide by the commitments and representations they have made to consumers can violate Section 5 of the FTC Act."). Although the Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies to some of One Medical's data, the FTC's letter implies that not all personal data is protected from use, stating that "Amazon and One Medical should make clear not only how they will use protected health information as defined by HIPAA *but also how the integrated entity will use any One Medical patient data for purposes beyond the provision of health care*." (emphasis added). *See also* Press Release, FTC, Statement of Commissioner Alvaro M. Bedoya Joined by Commissioner Rebecca Kelly Slaughter Regarding Amazon.com, Inc.'s Acquisition of 1Life Healthcare, Inc. (Feb. 27, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2210191amazononemedicalkhanslaughterwilsonbedoya.pdf [https://perma.cc/4UXS-QDJW] (expressing concern that de-identified health data is not subject to protection under the HIPAA Rule).

letters, rare public interest advocacy, and occasional scholarship on sectoral laws form the extent of privacy attention to these deals.[18]

Mergers and acquisitions are an odd blind spot in privacy law. Such law has long paid attention to other forms of opaque, mass transfers and sales of personal data, intervening in privacy-harming contracts,[19] data brokering,[20] and bankruptcy.[21] Mergers and acquisitions also bring about the bulk transfer of personal data to new corporate owners, are common across the economy, and, at times, raise the same potential problems of opacity and questionable consent. Yet these deals escape most privacy legislation and enforcement, and are oddly missing from the scholarship, beyond discrete areas like bankruptcy and health privacy.

This Article shines a spotlight on this missing transactional privacy law. It contributes the first theoretical and factual examination of the assumptions that drive this privacy inattention to M&A, and uses it to argue for closer scrutiny of deals that sell our personal data. The goal of this Article is to frame and provoke normative debate over the assumptions that privacy law makes about harm from M&A, or a lack thereof. It questions whether those assumptions remain appropriate given the immense changes underway in privacy law, and rising concern over commercialization of personal data.[22]

After this introduction in Part I, Part II traces the rise of personal data deals in the modern economy, and describes the major U.S. privacy laws relevant to these mergers and acquisitions. The Article

---

18. *See, e.g.*, EPIC WhatsApp Complaint (2014), *supra* note 1; EPIC WhatsApp Complaint (2016), *supra* note 6; Letter from Public Citizen to Lina Khan, Comm'r, FTC, Merrick Garland, Att'y Gen., U.S. Dep't of Just., Chiquita Brooks-LaSure, Adm'r, U.S. Ctr. for Medicare & Medicaid Serv., Sen. Chuck Schumer, Sen. Mitch McConnell, Rep. Nancy Pelosi et al. (Aug. 4, 2022), https://www.citizen.org/wp-content/uploads/public-citizen-amazon-onemedical-merger-letter.pdf [https://perma.cc/U3FF-6YF5] (expressing concern over the privacy and other harms likely to arise from Amazon's acquisition of One Medical); Dissenting Statement of Comm'r Pamela Jones Harbour, Google/DoubleClick, FTC File No. 071-0170 (Dec. 20, 2007) [hereinafter FTC Statement on Google/DoubleClick].

19. *See, e.g.*, Complaint ¶ 57, BetterHelp, Inc., FTC Docket No. C-4796 (July 7, 2023) (alleging a failure to "contractually limit how third parties could use and disclose" sensitive user data beyond the third parties' general terms of service, as part of an unfairness violation under FTC Act Section 5).

20. *See infra* Section III.D for a discussion of the FTC's longstanding enforcement against data brokers.

21. *See, e.g.*, Letter from Andrew N. Ferguson, Chairman, FTC, to Off. of U.S. Tr. (Mar. 31, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/23andme-letter-ferguson.pdf [https://perma.cc/A593-M7D8] (expressing "interests and concerns" of the agency over the sale of genetic, personal data of "millions of American consumers" by 23andMe as an asset in pending bankruptcy proceedings); Complaint ¶ 10, Toysmart.com, FTC File No. 00-11341 (July 10, 2000); *see also infra* Section III.D for a discussion of the Bankruptcy Code protections of privacy in data sales.

22. *See, e.g.*, SHOSHANA ZUBOFF, AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 521 (2019); ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 156–72 (2011); Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 Geo. Wash. Rev. 1, 29 (2021).

identifies widespread "M&A exceptionalism" in this legal landscape: the ordinary rules of privacy law are often not applied to the data processing that occurs in M&A, save the rare sectoral law. This is a function of three major factors. First, M&A are often expressly excluded from the limits that federal sectoral and state privacy laws otherwise impose on "sales" and "transfers" of data. Second, many deals fall beyond the limits of sector-specific U.S. privacy legislation. Third, the FTC has not enforced more general privacy law against transactional privacy harms. Where privacy law does apply to M&A, it relies on mechanisms that tend to offer weak protection against privacy harms, like notice and consent, and privacy policies that the merging companies themselves write — and change — unilaterally.[23]

Part III identifies and interrogates the theoretical foundations that drive this M&A exceptionalism, including: a history of individualistic privacy rights vs. collectivist exceptions, the edification of corporate property interests in personal data, operational efficiency of the target, and the presumed consistency of M&A with reasonable expectations of privacy.

It argues that these theoretical bases are often too general or too outdated to support the current scope of privacy permissiveness toward M&A. They also rely on a continuity fallacy that this Article identifies in privacy law, and which other areas of law often reject: the assumption that a corporate transaction causes no privacy harm if the law applies both before and after it. Lastly, these reasons for M&A exceptionalism are difficult to reconcile with privacy concerns over similar personal data transfers in other contexts, and with the growing worry over the commercial exploitation of personal data.

Part IV adds factual support to this re-evaluation of M&A exceptionalism. It scrutinizes the likely privacy effects of fifteen personal data acquisitions by the world's largest technology companies, using a comparison of the targets' privacy policies before and after each deal. Like the theoretical examination in Part III, this analysis finds that these deals impact our privacy in ways that are more variable and more harmful than assumed by privacy law. Several of the acquisitions appear to harm privacy, either through a lack of adequate consent for the transaction itself, or through privacy-reducing changes to the policies after the deal closes. Others, though, appear privacy-beneficial, leading to better disclosure or greater commitments to honor user preferences. The effects on privacy often depend on transaction-specific context, which is missing from current law and enforcement.

---

23. *See infra* Section II.B.3 for a discussion on the notice and consent privacy protection; *see also infra* Section IV.B.1 for a description of the unilateral changes permissions in privacy policies examined in this Article.

Part V offers specific solutions to ameliorate this M&A exceptionalism in privacy law. It proposes the first set of criteria to help enforcers screen for privacy risk in data-driven mergers and acquisitions, and calls for Congress to confirm their power to do so. It also charts a path for future research to build this understanding of transactional privacy effects, and canvasses the legal interventions that may become appropriate as this understanding develops. Finally, it argues that this development of transactional privacy law is crucial to privacy law as a whole, because of its great potential to address incipient harms, which can become difficult for privacy law to remedy ex post.

This examination of transactional privacy effects is timely given the broader, global reckoning underway in privacy law.[24] After years of growing dissatisfaction with privacy harms in the digital world, governments are passing stronger privacy laws at a frenetic pace.[25] Scholars are advancing new paradigms of privacy protection that reach beyond notice and consent to ex ante privacy controls with brighter lines around permitted practices.[26] These new laws and paradigms will govern the collection, use, and sale of our personal data for decades to come.[27]

As this Article explains, transactional privacy law belongs squarely within this reform effort, yet this revolution has left M&A almost entirely untouched. Both the descriptive contribution in Part II on the (non)application of privacy law to M&A, and the Part III interrogation of the foundations of that abstention are new to the literature. They build a foundation to fix this omission, and to better understand the impact of M&A on our privacy.

II. THE CURRENT LANDSCAPE: PERSONAL DATA M&A PROLIFERATE, YET PRIVACY LAW IS RARELY APPLIED

Our personal data has become a valuable asset that drives companies to enter into mergers and acquisitions. This Part describes this rise

---

24. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1690 (2020) ("The modern data industrial complex is facing a tidal wave of public support for a privacy law revolution."); David Doty, *The Privacy Revolution in Digital Is Unstoppable*, FORBES (May 20, 2019, 1:58 AM), https://www.forbes.com/sites/daviddoty/2019/05/20/the-privacy-revolution-in-digital-is-unstoppable/ [https://perma.cc/5QQW-P5US].

25. *See infra* note 63; Aly Apacible-Bernardo & Luke Fischer, *Identifying Global Privacy Laws, Relevant DPAs*, IAPP (Mar. 19, 2024), https://iapp.org/news/a/identifying-global-privacy-laws-relevant-dpas [https://perma.cc/2ZUB-BMAR] (describing the proliferation of data protection and privacy laws around the world).

26. Erika M. Douglas, *What is Privacy — to Antitrust Law*, 14 U.C. IRVINE L. REV. 817, 849–56 (2024) (examining the partial shift underway in privacy law toward protections beyond notice and consent).

27. Hartzog & Richards, *supra* note 24, at 1693 ("[W]e are on the cusp of a set of legal changes that will structure our emergent digital society for decades to come.").

in value and assetization. Then, it examines the related law, describing the current landscape and limits of privacy law as it applies, or, more often, does not apply, to personal data-driven M&A. As this Part explains, this nonapplication of privacy law to mergers and acquisitions is a function of legislative exceptions that remove M&A from the scope of many privacy statutes, and of the FTC's non-enforcement against transactional privacy harms.

A. The Rise of Personal Data in Mergers and Acquisitions

To understand the relevance of mergers and acquisitions to data privacy, it is first important to understand that our personal data has become a new and valuable asset class. Personal data is being treated like other intangible, corporate assets, like intellectual property, goodwill, or know-how, which drive the value of deals and are transferred as part of it. This value of personal data to businesses means that, more than ever before, our information is being bought and sold in corporate transactions, which this Article refers to here as "personal data" M&A.

In some sense, personal data has always been valuable to companies. White pages compilations and corporate loyalty programs have long enabled corporations to predict consumer behavior better, and to earn profits from that knowledge.[28] But in the digital economy, the commercial uses of personal data have exploded to unprecedented scale and value.[29] The new ubiquity of internet-connected technology like phones, computers, and smart devices, enables companies to collect, process, and sell our personal data in colossal amounts. The largest companies in the world, including Google, Meta, Amazon, Apple, and Microsoft, now depend on our personal information to fuel services in search and social media, to sell us goods, and to profit from behavioral advertising.[30]

The value of personal data is most apparent in the technology sector, where a target's primary or significant value may lie in the company's stash of extensive personal information and in its strong potential to collect more of the same. Take, for example, Amazon's acquisition of the high-end grocery chain, Whole Foods, in 2017. At first

---

28. *See, e.g.*, Sandy Skrogan, *Kroger's Analytics and Personalized Pricing Keep It a Step Ahead of Its Competitors*, GROCERY DIVE (July 10, 2017), https://www.grocerydive.com/news/grocery--krogers-analytics-and-personalized-pricing-keep-it-a-step-ahead-of-its-comp/534926/ [https://perma.cc/T8BX-8EN2] (emphasizing the role of consumer data in Kroger's grocery retail success).

29. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022) (to be codified at 16 C.F.R. Ch. 1) [hereinafter FTC ANPR on Com. Surveillance] (seeking comment to consider regulating companies' use and monetization of personal digital data).

30. *See* Jeannie Marie Paterson et al., *The Hidden Harms of Targeted Advertising by Algorithms and Interventions from the Consumer Protection Toolkit*, 9 INT'L J. OF CONSUMER L. AND PRACTICE, 1 (2021).

glance, the purchase of this brick-and-mortar retail grocer by Amazon, an online retailer and cloud computing giant, might seem an awkward strategic fit. But the grocery industry has particular talent in tracking its customers, and analyzing their purchases in an in-depth manner,[31] in part because grocery purchases are highly habitual and frequent. As a premium, organic grocery store, Whole Foods held troves of granular data about affluent consumers and their weekly grocery buying habits, with the relationships necessary to collect such data on an ongoing basis.[32] Post-acquisition, Amazon now knows not only what durable goods consumers purchase through its own e-commerce portal, Amazon Marketplace, but also the buying behavior of consumers at the grocery store. This acquisition enabled the combined company to cross-sell Whole Foods customers on its delivery services and more, to target advertising, to know what customers are likely to buy and when, and to use personal data to bring Amazon that much closer to its goal of becoming "the everything store."[33]

As mentioned above, Google's acquisition of Fitbit is another high-profile personal data transaction.[34] Fitbit's main product is a wearable fitness tracker by the same name.[35] Technology giant Google could easily have built similar hardware to compete in wearable fitness tech, as a company with a history of developing tablets and other devices.[36] Instead, Google chose to enter through acquisition of Fitbit. A major reason for this choice was personal data.[37] At the time of the acquisition there were nearly 30 million Fitbit users, and the company had amassed extensive and granular data troves on each user through its trackers.[38] Tracked data included individuals' sleep patterns, heartbeats, steps,

---

31. Skrogan, *supra* note 28 and accompanying text (emphasizing the role of consumer data in Kroger's grocery retail success).

32. Greg Petro, *Amazon's Acquisition of Whole Foods Is About Two Things: Data and Product*, FORBES (Aug. 2, 2017, 12:13), https://www.forbes.com/sites/gregpetro/2017/08/02/amazons-acquisition-of-whole-foods-is-about-two-things-data-and-product/ [https://perma.cc/S5QC-546Z].

33. BRAD STONE, THE EVERYTHING STORE: JEFF BEZOS AND THE AGE OF AMAZON (2013).

34. Fitbit, Inc., Current Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934 (Form 8-K) (Jan. 14, 2021), https://www.sec.gov/Archives/edgar/data/1447599/000119312521008670/d95819d8k.htm [https://perma.cc/M2X6-G443] (Fitbit became a wholly-owned subsidiary of Google LLC on January 14, 2021).

35. *See* FITBIT, https://web.archive.org/web/20240926160246/https://www.fitbit.com/global/us/home [https://perma.cc/K5HZ-ZBJP]. This is Fitbit's prior website, which now redirects to the Google Store.

36. Robert Scammell, *20 Years of Google: 20 Products That Shaped the Company*, VERDICT (Sep. 4, 2018), https://www.verdict.co.uk/20-years-of-google-20-products-that-shaped-the-company/ [https://perma.cc/XVS5-EPSF] (listing Google's hardware and software inventions such as its Chrome search engine, the Chromebook laptop, Chromecast telecast devices, and Google Maps).

37. *See* Griebeler da Motta, *supra* note 9.

38. *Id.*

water and food intake, weight, and menstrual health.[39] The transaction gave Google access to Fitbit's masses of data and an installed user base to collect even more personal data in the future. While Google insisted the transaction was about hardware, European antitrust enforcers saw it differently. The European Commission imposed commitments on the company to segregate Fitbit data to prevent it from being used for ad targeting.[40] This remedy was based on competition concerns in antitrust law, but it also benefited European users' privacy by limiting post-acquisition ad targeting based on Fitbit data.[41] In the United States, neither privacy nor antitrust enforcers intervened.

These are high-profile examples of a vast array of corporate deals in which personal data plays an important role. There is no tracking of how many mergers and acquisitions involve large amounts of personal data, much less the type or volume of data being transferred, but proxies suggest such transactions are happening regularly across the economy. In the most recently reported year of 2022, the FTC and the Department of Justice Antitrust Division received merger filings for 3,152 transactions, the second highest levels in a decade.[42] Of those transactions, more than half, over 1,500 transactions in just one year, were in industries that use personal data heavily: health, banking, information technology, and consumer goods and services transactions.[43] A decade earlier, the same industries comprised fewer than 600 deals a year, and only 42% of all filed transactions.[44] These numbers suggest rising, widespread acquisitiveness in sectors that rely on personal data, though they are a rough proxy that reflects only the largest of corporate transactions for which merger filings are required.[45]

---

39. *Id.*

40. Press Release, European Commission, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions (Dec. 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484 [https://perma.cc/QN5L-2VST].

41. *Id.*

42. FED. TRADE COMM'N, HART-SCOTT-RODINO ANN. REP. 2 (Fiscal Year 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/fy2022hsrreportcorrected.pdf [https://perma.cc/9D5W-K3P3].

43. *Id.* at 7 (sum of FTC categorization of business of acquired entity for health 4.2%, banking 10.4%, IT 8.7%, consumer goods & services 31.3%). A similar list of industries has been identified as those with bankruptcy oversight of the sale of consumer data, which also suggests these industries are the most likely to involve consumer information. *See* Bradley, *supra* note 16, at 155 (identifying retail, health services, media/technology, hospitality, financial, and education).

44. FED. TRADE COMM'N, HART-SCOTT-RODINO ANN. REP. 2, at 7 (Fiscal Year 2012), https://www.ftc.gov/sites/default/files/documents/reports_annual/35th-report-fy2012/130430hsrreport_0.pdf [https://perma.cc/L6XJ-QGUS] (sum of FTC categorization of business of acquired entity for health 3.9%, banking 19.1%, IT 7.1%, consumer goods and services 11.7%). This totals 41.8% of the 1,429 reported transactions in fiscal year 2012, amounting to approximately 597 deals.

45. *Id.* These figures reflect only the transactions for which a filing was required under the Hart-Scott-Rodino Act (HSR Act). HSR Act filings are required only if the acquisition meets

Further, the FTC and scholarly work demonstrate that the five largest technology firms are highly acquisitive in industries that rely on personal data. The FTC found that in the decade leading up to 2019, these firms alone had completed more than 800 acquisitions too small to be reportable to the agency under antitrust law.[46] These deals were concentrated in industries likely to involve consumer data, such as mobile devices and device-based software and content, applications software, and internet content and commerce services.[47] Scholarly work confirms that the five largest technology companies (Alphabet/Google, Amazon, Apple, Facebook/Meta, and Microsoft) have among the highest percentage of data-intensive targets among the companies they acquire.[48] These five companies are the subject of the empirical analysis in this Article, which examines the effects of acquisitions on privacy policies.[49]

This immense value of personal data, and its corresponding importance in certain mergers and acquisitions, is a new phenomenon driven by the digital economic revolution. Given this rising centrality and prevalence of personal data in corporate transactions, it is high time to evaluate the effects of these deals on our data privacy and their related treatment by privacy law.

B. Privacy Law is Rarely Applied to M&A — When It Is, Protection Relies on Notice and Consent

There are three primary sources of U.S. privacy law relevant to mergers and acquisitions: (1) a variety of "sectoral" privacy laws that apply only to certain entities and types of personal data, and which focus on more sensitive data as financial, credit, health, genetic, and

---

a minimum value, and in certain acquisitions, a minimum party size by sales and assets, and no special exemption applies. Section 201 of the HSR Act amended the Clayton Act, adding a new Section 7A, 15 U.S.C. § 18a (2023), to require reporting to these agencies certain proposed acquisitions of voting securities, non-corporate interests, or assets prior to consummation.

46. FED. TRADE COMM'N, NON-HSR REPORTED ACQUISITIONS BY SELECT TECHNOLOGY PLATFORMS, 2010–2019: AN FTC STUDY, at 10 (2021), https://www.ftc.gov/system/files/documents/reports/non-hsr-reported-acquisitions-select-technology-platforms-2010-2019-ftc-study/p201201technologyplatformstudy2021.pdf [https://perma.cc/K6QW-M9XY] [hereinafter FTC, Non-HSR Reported Acquisitions]. The FTC sought information and documents from Alphabet Inc., Amazon.com, Inc., Apple Inc., Facebook, Inc., and Microsoft Corp. on the terms, scope, structure, and purpose of transactions that each company consummated between January 1, 2010, and December 31, 2019, for which the company did not file a HSR Act merger notification form. Of these, 65% were of the type of an acquisition of control in shares or assets.

47. *Id.* at 27.

48. Ginger Zhe Jin et al., *How Do Top Acquirors Compare in Technology Mergers? New Evidence from an S&P Taxonomy*, 89 INT'L J. INDUS. ORG. 102891, 1 (2023) (finding private equity firms and the top twenty-five S&P500 companies as a whole also displayed high levels of targets with data-intensive products).

49. *See infra* Part IV.

children's information; (2) a growing number of comprehensive, state-level privacy laws; and (3) the FTC's common law of data privacy, which is not restricted to particular sectors or entities.[50] Together, these laws impose certain controls on the collection, use, disclosure, and protection of personal data.[51]

As this Section explains, these major U.S. privacy laws often are not applied to personal data M&A. This nonapplication pervades the law even though such deals often involve the types of personal data sales and transfers that are ordinarily subject to data privacy protection. Sectoral and state privacy legislation frequently excepts mergers and acquisitions, such that those ordinary protections do not apply. The statutes that do apply to M&A are limited, and capture only deals that involve specific entities and data within the purview of sectoral laws. For most transactions, that leaves the FTC's common law of data privacy as the main source of potential protection against M&A privacy harms. While this law applies in theory to M&A, in practice, the FTC has not engaged in enforcement against transactional privacy harms.

This landscape of transactional privacy law leaves the impression of "M&A exceptionalism": despite the increasing centrality of personal data to corporate transactions, these deals are not subject to the same rules that privacy law applies to other, similar data processing. This Article coins this term of M&A exceptionalism to capture the idea that

---

50. This list includes the primary categories of privacy law that would affect mergers and acquisitions. It leaves aside the laws that limit government uses of information, as well as some more specific state laws that may apply to particular types of data. What precisely constitutes federal privacy legislation is itself defined in varying ways. This Article considers those laws commonly identified as the major federal privacy statutes. *See, e.g.*, Sedona Conference, *Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice*, 20 SEDONA CONF. J. 233, 316 (2019) (defining "information security and data privacy laws" as those "related to the collection, use, disclosure, and protection of personal data," and including, Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681–1681x; Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §§ 7701–7713 (2018); Privacy Act of 1974, 5 U.S.C. § 552(a) (2018); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(g) (2018); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3423 (2018), as amended Privacy Protection Act of 1980, 42 U.S.C. §§ 2000aa–2000aa-12; Cable Communications Policy Act of 1984, 47 U.S.C. ch. 5, subch. V–A; Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523 (2018); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2018); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2018); Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725 (2018); Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. §§ 1001–1010 (2018); Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.) [hereinafter HIPAA]; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2018) [hereinafter COPPA]; Financial Services Modernization Act (Gramm-Leach-Bliley Act) of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.) [hereinafter GLBA]; and state laws governing the use of electronic communications and the use of information collected online, among other state laws such as data-breach notification laws, and Federal Trade Commission privacy guidelines).

51. *Id.*

data processing in a merger or acquisition often includes activities that would ordinarily be regulated as a sale, disclosure, or transfer of personal data, but when carried out under the cover of M&A, those activities are excluded from the scope of various privacy laws as written and as enforced.[52]

1. Privacy Legislation Often Excludes M&A, and Covers Only Certain Entities and Data Types

Federal and state privacy legislation often contains express exceptions that remove mergers and acquisitions from its scope.[53] The protections in these laws center around limits on data activities, such as the "transfer," "disclosure," "sharing," or "selling" of personal data without adequate consent.[54] These are activities likely to occur during most mergers and acquisitions.[55] Such corporate transactions typically involve an asset sale or a share sale. An asset sale would transfer personal data held by the target to the acquiror along with other assets. Such sale or transfer will give the acquiror access to that personal data, absent any privacy law limits on doing so. While perhaps less obvious, a share sale could also result in a transfer or disclosure of personal data, assuming the deal gives the acquiror control of the target.[56] In practical terms, that change in control means that post-acquisition, the acquiror gains the power to move and change access to the personal data held by the target that it now controls, including changes to the target's privacy policy and settings. Finally, a transfer or disclosure could also occur as part of due diligence conducted by the acquiror before the deal closes, whether a share or asset sale. The deals examined in the empirical

52. The "exceptions to this exception" narrative are the few sectoral laws that do still apply to mergers and acquisitions, such as COPPA. *See infra* note 81.

53. *See, e.g.*, GLBA, *infra* text accompanying note 59; HIPAA, *infra* text accompanying note 59; state law exceptions, *infra* text accompanying note 64.

54. *See, e.g.*, 45 C.F.R. § 164.502(a) (2024) (the HIPAA rule) (limiting the "sale" and/or "disclosure" of protected health information); 15 U.S.C. § 6802(a) (2018) (the GLBA rule) (limiting the "disclos[ure]" of "any nonpublic personal information"); 16 C.F.R. § 313.3(k) (2021) (Privacy of Consumer Financial Information Rule) (implementing 15 U.S.C. § 6801(b) (2023)); CAL. CIV. CODE § 1798.140(ad) (West 2025) ("selling"); CAL. CIV. CODE § 1798.140(ah) (West 2025) ("sharing").

55. There are a handful of other federal data privacy laws that are not discussed here because they are likely inapplicable to M&A. They regulate activities that do not occur as a result of such transactions or that would be merely incidental to the deal. This includes laws that impose limits on telemarketing (Telephone Consumer Protection Act, 47 U.S.C. § 227 (2018)), laws that limit the transmission of commercial email messages (Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) of 2003, 15 U.S.C. §§ 7701–13 (2023)) and wiretapping (Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. §§ 2510–11 (2023)), and laws that apply to other contexts, such as the Genetic Information Non-Discrimination Act of 2008, Pub. L. 110–233, 122 Stat 881 (2008), which limits the use of genetic information in the course of health insurance and employment.

56. This leaves aside minority or non-controlling acquisitions for another discussion.

section of this Article happen to be share acquisitions, but the point here is that the form of the corporate transaction does not dictate the personal data processing.

Despite personal data M&A often involving transfers, disclosures, and sales of personal data — the types of activities ordinarily scrutinized by privacy legislation — such legislation often expressly excludes mergers and acquisitions. For example, the Gramm-Leach-Bliley Act ("GLBA") and its rules ordinarily limit the disclosure and sharing of consumer financial data by financial institutions to non-affiliated third parties.[57] But these rules carve out any transfers "[i]n connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit."[58] The Health Insurance Portability and Accountability Act ("HIPAA") rules similarly exclude a "transfer, merger, or consolidation of all or part" between covered entities from the scope of privacy protections.[59] HIPAA's limits on the use, disclosure, and sale of protected health information by certain entities do not apply to such deals.[60] Transactions are also exempted from HIPAA if, following the merger or consolidation, the entity will "become" a covered entity as a result of the deal,[61] as is data processing for the purposes of due diligence related to such transactions.[62]

---

57. The GLBA rules limit the disclosure and sharing of consumer financial data by financial institutions to non-affiliated third parties, requiring notice to consumers of their opt-out rights prior to such disclosure. 16 C.F.R. § 313.3(a), (k) (2025) (Privacy of Consumer Financial Information Rule) (implementing 15 U.S.C. § 6801(b) (2023)).

58. 16 C.F.R. § 313.15(a)(6) (2025). While the FTC's guidance conditions this exception on the acquiror stepping into the shoes of the seller's privacy policy, the regulations themselves do not require such ongoing compliance. 65 Fed. Reg. 33660–61 (expressing this opinion for mergers between financial institutions).

59. The HIPAA rules achieve this by permitting data processing for "health care operations," which is defined to include such corporate transactions. 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(iv) (2024) (permitting a sale, transfer, merger or consolidation for "health care operations"); 45 C.F.R. § 164.501(6)(iv) (2024) (defining "health care operations" as activities by a covered entity that include "the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity"). For further certainty, the definition of a "sale" of protected health information also expressly excludes these activities, referring back to the health care operations definition. 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(iv) (2024). Neither HIPAA statute, rules, nor guidance address transactions involving *non*-covered entities. This suggests the usual protections of the Act would apply to require patient authorization (or adequate safeguards) for data transfers to a non-covered acquiror.

60. 45 C.F.R. § 164.502(3)–(4) (2024). "Business associates" of these entities are also included in these limits.

61. 45 C.F.R. § 164.501(6)(iv) (2024).

62. *Id.* Other federal privacy legislation like the Cable Communications Policy Act of 1984 is less express but contains oblique exemptions for "legitimate business activity" that could also be interpreted to exclude mergers and acquisitions from the scope of its protections. 47 U.S.C. § 551(c)(2)(A) (2023). This Act otherwise prohibits cable operators from disclosing personally identifiable information without prior written or electronic consent of the subscriber.

The new crop of state comprehensive privacy legislation all contain similar exceptions for M&A.[63] These state laws bar certain "sale," "sharing," or "transfer" of personal information without adequate consent, but not when these activities occur as part of a merger or acquisition.[64] All expressly exclude M&A from their definitions of these

63. Since California took the lead in 2018, twenty states have now passed their first-ever broad, data privacy protection statutes, establishing many new data privacy rights and protections (as of May 2025). California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–199 (2024); Colorado Privacy Act of 2021, COL. REV. STAT. §§ 6-1-1301–1313 (2023); The Connecticut Act Concerning Personal Data Privacy and Online Monitoring, CONN. GEN. STAT. §§ 42-515–529 (2023); Delaware Online Privacy and Protection Act, DEL. CODE 6 §§ 12D-101–111 (2024); Florida Digital Bill of Rights, FLA. STAT. §§ 501.701–722 (2024); Indiana Consumer Data Protection Act, IND. CODE §§ 24-15-2–6 (2023); Iowa Consumer Data Protection Act, IOWA CODE §§ 715D.1–9 (2023); Kentucky Consumer Data Protection Act, KY. REV. STAT. ANN. §§ 367.3611–3629 (2024); The Maryland Online Data Privacy Act, MD. CODE ANN., COMMERCIAL LAW §§ 14-4701–4714 (2024); Minnesota Consumer Data Privacy Act, MINN. STAT. §§ 325O.01–11 (2024); Montana Consumer Data Privacy Act, MONT. CODE ANN §§ 30-14-2801-2817 (2023); Data Privacy Act, NEB. REV. STAT. §§ 87-1101–1130 (2024); New Hampshire Data Privacy Act, N.H. REV. STATE. ANN. §§ 507-H:1–12 (2024); New Jersey Data Protection Act, N.J. REV. STAT. §§ C.56:8-166.4–19 (2024); Oregon Consumer Privacy Act, OR. REV. STAT. §§ 646A.570–893 (2023); Rhode Island Data Transparency and Privacy Protection Act, R. I. GEN. LAWS §§ 6-48.1–10 (2024); Texas Data Privacy and Security Act, TEX. BUS. & COM. CODE ANN. §§ 541.001–205 (2023); The Utah Consumer Privacy Act, UTAH CODE ANN. §§ 13-61-101–103 (LexisNexis 2022); Tennessee Information Protection Act, TENN. CODE ANN. § 47-18-3201–3214 (2023); Virginia Consumer Data Protection Action, VA. CODE §§ 59.1-575–584 (2024); *see also* Biometric Information Privacy Act, 740 Ill. COMP. STAT. ANN. §§ 14/1–14/99 (West 2018) (establishing privacy protection of biometric information).

64. CAL. CIV. CODE § 1798.140(ad)(2)(C) (West 2020) ("[A] business does not sell personal information when [t]he business transfers to a third party the personal information of a consumer as . . . part of a merger, acquisition . . . ."); § 1798.140 (ah)(2)(C) ("[A] business does not share personal information when . . . [t]he business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition . . . ."); COLO. REV. STAT. § 6-1-1303(23)(b)(iv) (2024) ("'Sale', 'sell', or 'sold' does not include; . . . the disclosure or transfer to a third party of personal data as an asset that is part of a proposed or actual merger, acquisition . . . ."); CONN. PUB. ACT NO. 22-15, § 1 (26)(F) (2023) ("'Sale of personal data' does not include . . . the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition . . . or a proposed merger, acquisition . . . ."); DEL. CODE 6 § 12D-102(29)(f) (2024) ("'Sale of personal data' does not include . . . [t]he disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition . . . or a proposed merger, acquisition . . . ."); IND. CODE § 24-15-2-27(b)(5) (2024) ("'Sale of personal data' . . . does not include . . . the disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition . . . ."); IOWA CODE § 715D.1(25)(f) (2023) ("'Sale of personal data' does not include . . . [t]he disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition . . . ."); KY. REV. STAT. ANN. § 367.3611(27(e) (West 2024) ("Sale of personal data does not include . . . [t]he disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition . . . ."); MD. CODE ANN., COMMERCIAL LAW § 14-4701(ff)(2)(vi) (West 2024) ("'Sale of personal data' does not include . . . [t]he disclosure or transfer of personal data to a third party as an asset that is part of an actual or proposed merger, acquisition . . . ."); MINN. STAT. § 325M.11(u)(5) (2024) ("Sale does not include . . . the disclosure or transfer of personal data to a third party as an asset that is part of a completed or proposed merger, acquisition . . . ."); MONT. CODE ANN. § 30-14-2802(23)(b)(vi) (2023) ("'Sale of personal data' . . . does not include . . . the disclosure or transfer of personal data to a third party as an asset that is part of a merger,

regulated activities.[65] For example, California's legislation, which was the model for many other states, grants rights for individuals to limit the "sharing" and "selling" of personal information,[66] but carves out of both definitions the transfer of an "asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business."[67] These exceptions remove the processing of health, financial, and other personal data from the scope of legislative protections when it is transferred, shared, or sold under cover of a merger or acquisition.

The existence of these exceptions, in and of themselves, suggests that such legislation *would* otherwise apply to corporate transactions. The reasons for these M&A exceptions have not been explained in the literature or legislative history in much, if any, depth.[68]

Finally, it is important to note that not every federal sectoral privacy law includes this type of M&A exception. Key federal statutes on children's data,[69] educational institutions,[70] and state-level biometric[71]

---

acquisition . . . ."); NEB. REV. STAT. §§ 87-1102(29)(b)(v)(A), (B) (2024) ("'Sale of personal data' does not include . . . [t]he disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual . . . [m]erger; [a]quisition . . . ."); N.H. REV. STATE. ANN. § 507-H:1(XXVII)(f) (2024) ("'Sale of personal data' does not include . . . [t]he disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition . . . ."); N.J. REV. STAT. § C.56:8-166.4(1) (2024) ("'Sale' shall not include . . . [t]he disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition . . . ."); OR. REV. STAT. § 646A.570(17)(b)(C) (2023) ("'Sale' or 'sell' does not include . . . [a] disclosure or transfer of personal data from a controller to a third party as part of a proposed or completed merger, acquisition . . . ."); R.I. GEN. LAWS § 6-48.1-2(25)(ii) (2024) ("'Sale of personal data' does not include . . . the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition . . . or a proposed merger, acquisition . . . ."); TENN. CODE ANN. § 47-18-3301(25)(B)(v) (2023) ("'Sale of personal information' . . . does not include . . . [t]he disclosure or transfer of personal information to a third party as an asset that is part of a merger, acquisition . . . ."); TEX. BUS. & COM. CODE ANN. § 541.001(28)(E) (2023) ("'Sale of personal data' . . . does not include . . . the disclosure or transfer of personal data to a third party as an asset that is part of a merger or acquisition."); UTAH CODE ANN. § 13-61-101(31)(b)(vii) (2022) ("'Sale,' 'sell,' or 'sold' does not include . . . a controller's transfer of personal data to a third party as an asset that is part of a proposed or actual merger, an acquisition . . . ."); VA. CODE ANN. § 59.1-575 (2024) ("'Sale of personal data' does not include . . . [t]he disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition . . . .").

65. *See supra* note 64.

66. *See* CAL. CIV. CODE § 1798.140(ad) (2024); CAL. CIV. CODE § 1798.140(ah) (2024).

67. CAL. CIV. CODE § 1798.140(ad)(2)(C) (2024) (excluding mergers and acquisitions from the definition of "selling," provided that information is used or shared consistently with this title); § 1798.140(ah)(2)(C) (2024) (excluding from "sharing," provided that information is used or shared consistently with this title).

68. *See infra* Part III (canvassing the probable rationales behind exceptions for mergers and acquisitions in privacy law).

69. *See infra* note 81 for a discussion on COPPA.

70. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2013).

71. Illinois, Texas, and Washington have laws that limit the processing of biometric data that contain no exceptions for mergers or acquisitions. 740 ILL. COMP. STAT. 14/15 (2008); TEX. BUS. & COM. CODE ANN. § 503.001 (2009); WASH. REV. CODE § 19.375.010 (2017).

data do *not* except M&A. These laws capture data processing in deals to the extent it constitutes regulated activity, such as selling or disclosing. Still, these sectoral laws are inherently limited in ways that leave many mergers and acquisitions uncovered. First, there is no sectoral legislation applicable in many personal data-heavy sectors, such as high tech, grocery and other retail, real estate, or travel.[72] Second, even in the areas governed by sectoral legislation, these laws only apply to certain entities and types of data, as discussed below. While these are more general features (or flaws) of the sectoral scheme, they also deeply affect the law's application to M&A.

Mergers and acquisitions that do not involve covered entities are not subject to sectoral legislative protections. For example, HIPAA and its rules apply only to "covered entities" — defined to mean only health care providers, health plans, health clearinghouses, and certain business associates of such entities.[73] HIPAA's limits leave unprotected any mergers or acquisitions between entities that collect health information but are not on this covered list, such as fitness apps or trackers like Fitbit.[74] While not a merger or acquisition, the FTC's recent action against BetterHelp, Inc. ("BetterHelp"), an online therapy service, highlights these striking limits of HIPAA.[75] Many of the therapists who worked with BetterHelp were not HIPAA-covered entities, which left their patient health information and the fact of their relationship with

---

For example, private entities cannot "sell, lease, trade, or otherwise profit from" biometric data under the leading Illinois biometric privacy law. 740 ILL. COMP. STAT. 14/15 (2008); The "disclosure" of such data is also prohibited, unless certain conditions of authorization or exceptions are met. *Id.*

72. *See, e.g.*, Skrogan, *supra* note 28; Kashmir Hill, *Could Target Sell Its 'Pregnancy Prediction Score'?*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/could-target-sell-its-pregnancyprediction-score/ [https://perma.cc/95M2-GGC5]; Wendy Fry, *Landlords Are Using AI to Raise Rents — and Cities Are Starting to Push Back*, THE MARKUP (Dec. 2, 2024), https://themarkup.org/locked-out/2024/12/02/landlords-are-using-ai-to-raise-rents-and-cities-are-starting-to-push-back [https://perma.cc/LKY6-UKJX].

73. 45 C.F.R. § 160.103 (2024) ("covered entities"); *id.* ("business associate"); Helen Nissenbaum & Heather Patterson, *Biosensing in Context: Health Privacy in a Connected World*, *in* QUANTIFIED: BIOSENSING TECHNOLOGIES IN EVERYDAY LIFE 79, 92 (Dawn Nafus ed., 2016) ("[H]ealth-self tracking information does not usually fall under the purview of HIPAA because the law is limited to discrete healthcare relationships, rather than health information.").

74. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 52 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/2A27-CURR] (observing that often "health apps are collecting [personally identifiable patient information] through consumer-facing products, to which HIPAA protections do not apply"); Elvy, *supra* note 16, at 497–98 (noting that HIPAA is unlikely to apply to fitness tracking devices since the companies do not provide "medical or health services").

75. *See* Complaint, BetterHelp, Inc., *supra* note 19.

patients unprotected by any sectoral laws.[76] This highly personal health information is free to be transferred in a corporate transaction.

Further, sectoral laws can only protect certain sub-types of personally identifiable data in deals, such as children's,[77] health,[78] educational,[79] or biometric[80] data. For example, the Children's Online Privacy Protection Act ("COPPA") does not have exceptions for M&A[81] — its rules apply to corporate transactions — but those rules serve only to protect the data of children under thirteen, when it is processed by the operators of websites and online services.[82] Deals that involve non-covered entities and data of children over age thirteen are both outside of the legislative scope. A merger or acquisition could, for example, involve a mixture of protected data that relates to children under thirteen and unprotected data that relates to children over thirteen.

This bounded relevance of sectoral privacy laws leaves many deals, or data within them, beyond their reach. Sectoral laws applied to only two of the fifteen technology transactions examined in Part IV of this Article.[83] No sectoral legislation applied to acquisitions that raised the most acute privacy concerns, like Facebook's acquisition of WhatsApp. This spottiness of the sectoral approach of U.S. legislation significantly limits transactional privacy law and leaves many data-driven mergers and acquisitions unexamined.[84]

---

76. *Id.* ¶ 68.

77. *See* discussion on Children's Online Privacy Protection Act (COPPA), *infra* note 81 and accompanying text.

78. *See* discussion on HIPAA Rule, *supra* note 59 and accompanying text.

79. FERPA, *supra* note 70.

80. *See* 740 ILL. COMP. STAT. ANN. § 14/15 (2008); TEX. BUS. & COM. CODE ANN. § 503.001 (2009); WASH. REV. CODE § 19.375.020 (2017).

81. COPPA rules require notice and "verifiable parental consent prior to collecting, using, or disclosing personal information from children." 16 C.F.R. § 312.4(a) (2025). The transfer of information in a merger or acquisition, or related due diligence, may constitute a "disclosure," which is broadly defined in the COPPA rules, or "use," which is not defined, meaning the law could apply to corporate deals. The COPPA rules define "disclosure" to include the "release of personal information" of the child "for any purpose" with narrow exceptions, none of which relate to mergers and acquisitions. 16 C.F.R. § 312.2 (2025) (defining "[d]isclose or disclosure"). "Release of personal information" is also broadly defined as "the sharing, selling, renting, or transfer of personal information to any third party." *Id.* (defining "[r]elease of personal information").

82. 15 U.S.C. § 6501(1) (1998) (defining a "child" as anyone under age 13); 15 U.S.C. § 6502(a)(1) (1998) (prohibiting operators or online services aimed at children).

83. *See infra* Part IV. Based on deal documents, it appears FERPA applied to data at issue in Brightbytes and HIPAA applied to data at issue in One Medical.

84. *See, e.g.*, 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)(iv) (2024) (holding "sale" does not include private health information disclosed as part of a "sale, transfer, merger, or consolidation of all or part of the covered entity"); 16 C.F.R. § 313.15(a)(6) (2021) (holding consumer notice and opt-out requirements do not apply when non-public information is disclosed as part of "a proposed or actual sale[or] merger").

2. No FTC Section 5 Privacy Complaints Against M&A

The other major component of U.S. federal privacy law is Section 5 of the FTC Act, which declares unlawful any unfair or deceptive acts or practices that affect commerce.[85] Unlike the federal sectoral legislation discussed above, Section 5 is a general law that applies across the economy. In theory, that means Section 5 could be invoked against privacy harms arising from any merger or acquisition. In practice, the FTC has never brought any claims of privacy harm from a merger or acquisition.[86]

Though privacy is not mentioned in the text of Section 5,[87] the FTC has been using this consumer protection authority to enforce against unfair and deceptive privacy practices since the 1990s, building up a "common law" of data privacy in the form of FTC complaints, settlements, and a few litigated cases.[88] The FTC has often brought these privacy cases under the deception branch of Section 5, which bars misrepresentations, omissions, or other practices that are likely to materially mislead a consumer acting reasonably in the circumstances, to the consumer's detriment.[89] These FTC complaints hold companies to their stated privacy policies[90] and privacy settings[91] when they seek to violate those promises, require companies to disclose adequately how

85. 15 U.S.C. § 45(a)(1) (2012).

86. This statement relates to the ordinary-course M&A that are the subject of this Article. The FTC has intervened in bankruptcy proceedings involving the sale of personal data. *See* First Amended Complaint for Permanent Injunction and Other Equitable Relief ¶ 11, Toysmart.com, Inc., FTC File No. 00-11341 (July 21, 2000) https://www.ftc.gov/sites/default/files/documents/cases/toysmartcomplaint.htm [https://perma.cc/L9N3-JCNM].

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

88. *Id.* (describing and labelling the emergence of the FTC's new common law of privacy, consisting of the common-law-like body of settlement agreements reached between the FTC and companies accused of unfair and deceptive trade practices).

89. *Id.* at 638 (noting the FTC has primarily used its deception authority but confirming a "trend of judicious yet increasing pleading of unfairness" by the agency). To be actionable, the deception must be "material," which is defined as "likely to affect a consumer's choice of or conduct regarding a product." Fed. Trade Comm'n, FTC Policy Statement on Deception (Oct. 14, 1984), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/GP7Y-7HT6] (appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984)) [hereinafter FTC Policy Statement on Deception].

90. *See, e.g.*, Complaint ¶¶ 5–6, Eli Lilly & Co., 133 F.T.C. 763 (May 8, 2002), https://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillydo.htm [https://perma.cc/RN79-S462] (alleging Eli Lilly company disclosed customers' personal information in violation of privacy policy).

91. Complaint ¶ 14, Google Inc., FTC File No. 102-3136, Dkt. No. C-4336 (Oct. 13, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf [https://perma.cc/E6D6-LNS9] (alleging Google failed to observe privacy settings of users as part of the deceptive acts).

personal data is used,[92] prevent data collection using spyware,[93] and require sufficient data security practices to protect privacy.[94]

At times, the FTC has also used the Section 5 prohibition on "unfair" acts or practices, which it defines as those that (1) cause or are likely to cause substantial injury to consumers,[95] (2) are not reasonably avoidable by consumers themselves,[96] and (3) are not outweighed by countervailing benefits to consumers or to competition.[97] These FTC complaints have challenged misconduct such as: retroactive changes to privacy policies,[98] deceitful data collection,[99] the improper use of data,[100] and unfair default privacy settings or other design factors[101] that prevent consumers from exercising choice.[102] Recent complaints have also alleged that the sale or other transfer of sensitive data could, in itself, be unfair.[103]

---

92. *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief ¶ 13, Frostwire, LLC, FTC File No. 11-cv-23643 (S.D. Fla. Oct. 7, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf [https://perma.cc/4RYJ-PTGG] (alleging deception based on a failure of Frostwire to adequately disclose default public sharing of user files by its software).

93. Complaint ¶ 12, Aspen Way Enter., Inc., FTC File No. 112-3151, Dkt. No. C-4392 (Apr. 11, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415aspenwaycmpt.pdf [https://perma.cc/EQ4P-Y8NY].

94. For an assortment of other practices that have been challenged under Section 5, see the summary in Solove & Hartzog, *supra* note 87, at 627–43.

95. 15 U.S.C. § 45(n) (2012).

96. *Id.* The FTC has used its unfairness authority to intervene when misconduct "prevent[s] consumers from effectively making their own decisions . . . ." *See* FED. TRADE COMM'N, FTC POLICY STATEMENT ON UNFAIRNESS (Dec. 17, 1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness [https://perma.cc/94C9-2ZE4] (appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984)) [hereinafter FTC Policy Statement on Unfairness].

97. 15 U.S.C. § 45(n) (2012); *see* FTC Policy Statement on Unfairness, *supra* note 96.

98. *See, e.g.*, Complaint, Gateway Learning Corp., 138 F.T.C. 443, 475–76 (2004) (alleging Gateway retroactively changed its privacy policy to permit personal data to be rented to third parties); Decision and Order, 1Health.io Inc., FTC File No. 192-3170, Dkt. No. C- 4798 (Sep. 6, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/1Health-Complaint.pdf [https://perma.cc/Y76V-LEN7].

99. *See, e.g.*, Aspen Way Enter., Inc., *supra* note 93 ¶ 5 (alleging Aspen installed spyware software on its rental computers).

100. *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief ¶ 8, ReverseAuction.com, Inc., FTC File No. 00-CV-00032 (D.D.C. Jan. 6, 2000) https://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.govreversecmp.htm [https://perma.cc/9WRH-7MAD] (alleging collection of data in violation of eBay's terms of use and later use of that data to send spam emails).

101. Frostwire, LLC., *supra* note 92 ¶ 17 (alleging Frostwire failed to notify users that, by default, previously downloaded files on users' computers were shared publicly even from "unshared" folders).

102. FTC Policy Statement on Unfairness, *supra* note 96 ("[The FTC makes clear that its purpose is] not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision-making.").

103. *See, e.g.*, Complaint, X-Mode Social, Inc., FTC File No. 212-3038, Dkt. No. C-4802 (Apr. 11, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialComplaint.pdf

Throughout this history of hundreds of FTC actions, the agency has never brought a privacy case alleging harm from a merger or acquisition.[104] None of the privacy complaints from the 1990s to the present advance a theory that an acquiror violated Section 5 after a corporate transaction gave it access to personal data, abused its new power over the target's privacy policy, or caused any other transactional privacy harm.[105]

Despite this lack of M&A-related enforcement, the FTC's position — at least in theory — is that Section 5 applies to protect against privacy harm from mergers and acquisitions. Once privacy promises are made, the FTC has declared that "regardless of the [proposed] acquisition," individuals have the right to rely on those promises remaining in effect.[106] This view was clearly articulated in the agency's nonbinding letter to Facebook and WhatsApp in 2014.[107] The FTC warned that a failure of the merging parties to honor the promises made in WhatsApp's privacy policy, or in other public statements, about the collection and use of personal data "could" constitute an unfair or deceptive act in violation of Section 5 of the FTC Act.[108] It explained that companies who acquire personal data in a merger "cannot use [that] data in a manner that is *materially inconsistent* with promises made at the time the data was collected" unless the company obtains "affirmative express consent" from the data subject for the new use.[109] Further, if the company changes its data processing practices for "newly-collected" data after the merger, it should also give users the opportunity to opt out of such changes or at least make it clear they can stop using the services.[110]

Essentially, this would apply Section 5 through a bifurcated rule for old and new data, both of which rely heavily on consent. For preexisting data, the acquiror is limited: it can continue to use personal data as the target did, or in ways that are not materially inconsistent with promises about that use. For other uses, it must seek affirmative, express consent. For newly-collected data, the best practice is to allow individuals to opt out of those other uses, though this statement on future data collection was framed as a recommendation in

---

[https://perma.cc/KVQ8-Z9QZ] (alleging in Count I unfairness violation based on the sale, licensing or other transfer of precise location data associated with persistent, unique identifiers revealing visits to sensitive locations such as places of worship, reproductive health or addiction recovery).

104. *See* Solove & Hartzog, *supra* note 87 (counting 170 FTC cases from 1997 to the article writing in 2014). The FTC has since continued to pursue many privacy law cases.

105. *Id.*

106. FTC Letter Re Facebook/WhatsApp, *supra* note 2, at 1.

107. *Id.*

108. *Id.*

109. *Id*. at 3 (emphasis added).

110. *Id.*

Facebook/WhatsApp rather than as a potential Section 5 violation.[111] This enforcement position has remained theoretical, given the lack of FTC cases on M&A privacy harm.

While the FTC has not brought any M&A *privacy* claims, it has — somewhat counterintuitively — brought an *antitrust* claim to address the privacy effects of Meta's acquisitions.[112] In FTC v. Meta Platforms Inc., the agency and several states allege that Meta (previously Facebook) used its market power over social media markets to erode privacy quality to lower levels than would have been offered in a competitive market.[113] It argues that Meta obtained this power through its pattern of acquisition or exclusion of nascent competitors like WhatsApp and Instagram — termed a "buy or bury" strategy in the litigation.[114]

Although the harm is privacy-related, the claims are pressed into the shape of an antitrust case. The violation is alleged under the unfair methods of competition provisions of Section 5(a) of the FTC Act,[115] a distinct branch of Section 5 from that which the FTC uses to protect data privacy.[116] Specifically, the agency claims that Meta's conduct caused a decline in "consumer choice," including fewer data privacy protection options "regarding the amount and nature of advertising . . . the availability, quality, and variety of data protection privacy options for users [and] options regarding data gathering and data usage practices."[117] In other words, the company's acquisitions enabled it to illegally limit privacy competition, and as a result, reduce privacy protections available in the market. The FTC has gained early-stage judicial support for its theory of privacy harms in the litigation, but it has yet to be tested in a trial on the merits.[118] In recent litigation against

---

111. *Id.*

112. Substitute Amended Complaint for Injunctive and Other Equitable Relief, Facebook, Inc., FTC File No. 1:20-cv-03590-JEB (D.D.C. Sep. 8, 2021) https://www.ftc.gov/system/files/documents/cases/2021-09-08_redacted_substitute_amended_complaint_ecf_no._82.pdf [https://perma.cc/NY9W-4Z8M].

113. *Id.* ¶ 222. The FTC's initial complaint against Facebook was dismissed, and this discussion refers to the FTC's second, amended complaint.

114. *Id.* ¶ 77.

115. *Id.* ¶¶ 235, 242.

116. *See supra* Section II.B.2 for a discussion on the common law of data privacy.

117. Substitute Amended Complaint for Injunctive and Other Equitable Relief ¶ 221, *supra* note 112.

118. In a partial denial of Facebook's motion to dismiss, Judge James Boasberg of the District of Columbia found it plausible that consumers would prefer social networking services with more privacy-protective ad delivery mechanisms. F.T.C. v. Facebook, Inc., 581 F. Supp. 3d 34, 55 (D.D.C. 2022) (finding support for this conclusion in federal legislation that addresses "various privacy and advertising concerns related to consumer technology" and referencing as examples of such federal legislation 15 U.S.C. §§ 6101–6608 (2010) (Telemarketing and Consumer Fraud and Abuse Prevention Act); 15 U.S.C. §§ 7701–7713 (2003) (Controlling the Assault of Non-Solicited Pornography and Marketing Act); and 47 U.S.C. § 227 (2019) (Telephone Consumer Protection Act)). In the parallel state claims, Judge Boasberg ruled that the states had standing based on privacy harm to their citizens, who

other technology giants, courts have been skeptical toward similar claims of monopoly harms to privacy competition.[119]

These FTC arguments are somewhat awkward and ultimately offer incomplete protection against transactional privacy harms. The awkwardness stems from Meta's acquisition history. Back when Meta acquired WhatsApp and Instagram in 2012 and 2014, respectively, consumer protection advocates raised these very same privacy harms to the FTC.[120] The agency did not take binding action under either its privacy or competition authorities to guard against those harms, which the agency itself is now claiming did occur. This suggests the FTC was not able to accurately predict the privacy effects of the deals at the time they occurred. If the FTC's position in the *Meta* case is correct, it also means that privacy harm was occurring and left unaddressed in the decade that passed between these acquisitions and the filing of the current antitrust case.[121]

Even if the FTC succeeds with these novel antitrust claims, antitrust law offers an incomplete tool for addressing transactional privacy harms. The function of antitrust law is to protect competition.[122] Competition and privacy are not necessarily correlated with each other; in markets that commercialize personal data, increasing competition may reduce privacy.[123] The competition mandate of antitrust also acts as a limit on the power of antitrust — authorities do not have a roving mandate to fix privacy harms that are untethered to an antitrust law violation.[124] Antitrust claims are limited to addressing privacy effects *that*

---

experienced "reductions in the quality and variety of privacy options and content available to them in that [social media] market." New York v. Facebook, Inc., 549 F. Supp. 3d 6, 23 (D.D.C. 2021) (quoting the States' Redacted Complaint, ¶¶ 8, 247–50, and finding it plausible if "a shade vague"). The states' claims were, however, dismissed on other grounds of laches. *Id.* at 13.

119. United States v. Google LLC, 747 F. Supp. 3d 1, 119 (D.D.C. 2024) (expressing skepticism that declining privacy quality in Google's online search was a result of its monopoly power); hiQ Labs, Inc. v. LinkedIn, Corp., 31 F.4th 1180, 1189–90 (9th Cir. 2022), *order dissolved* on unrelated grounds No. 17-CV-03301, 2022 WL 18399964 (N.D. Cal. Aug. 1, 2022) (finding, in response to LinkedIn claims of data privacy protection as a justification in response to allegations of state antitrust law violations; "little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy" in such information); hiQ Labs, Inc. v. LinkedIn, Corp., 273 F. Supp. 3d 1099, 1119 (claiming user privacy interests are "at best uncertain").

120. *See, e.g.*, EPIC WhatsApp Complaint (2014), *supra* note 1.

121. *See infra* Appendix A (noting Facebook's acquisition of Instagram in 2012, and WhatsApp in 2014).

122. Brown Shoe Co. v. United States, 370 U.S. 1502, 1521 (1962) (holding antitrust law protects "*competition*, not *competitors*") (emphasis in original).

123. Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J. F. 647, 661–69 (2021); James C. Cooper & John M. Yun, *Antitrust & Privacy: It's Complicated*, 2022 U. ILL. J.L. TECH. & POL'Y 343, 365 (2022).

124. Herbert Hovenkamp, *Antitrust Interoperability Remedies*, 123 COLUM. L. REV. F. 1, 11 (2023).

arise from substantial harms to competition.[125] This limit leaves any standalone privacy impacts from a deal — those not caused by changes in competition, but that still harm privacy interests — beyond the liability ambit of antitrust law.[126] The FTC has recognized this view on the limits of its antitrust jurisdiction over privacy since at least the Google/DoubleClick acquisition in 2007,[127] and it is shared by other competition authorities internationally.[128] It means this new breed of antitrust-*cum*-privacy claims can offer at best partial protection of data privacy interests, acting as an incomplete stopgap for competition-related privacy harms while transactional privacy law itself is failing.

3. When the Law Applies, Transactional Privacy Protection Depends on Notice, Consent, and Purpose Continuity

M&A exceptionalism has its limits. When privacy law *does* apply to M&A, the touchstone for legal processing of personal data is almost always the same: notice and consent.[129] Corporations give notice to individuals of how their personal data will be collected, used, and sold, then seek consent for that processing.

Consent is the basis for legitimizing data collection, use, and other processing across much of U.S. privacy law. As Heidi Hurd eloquently describes, consent works a "moral magic" across many legal contexts to render actions permissible: it "turns a trespass into a dinner party; a battery into a handshake; a theft into a gift; an invasion of privacy into an intimate moment."[130] In privacy law, a failure to obtain adequate consent to data processing has become a primary identifier of privacy harms.[131] With adequate consent, that data processing becomes lawful;

---

125. *See, e.g.*, Noah J. Phillips, Comm'r, FTC, Remarks at the Center for Internet and Society at Stanford Law School: Should We Block This Merger? Some Thoughts on Converging Antitrust and Privacy 3 (Jan. 30, 2020) (stating that "competition law is not designed to protect privacy").

126. *But see* Erika Douglas, *U.S. Antitrust Remedies and Data Privacy*, *in* RESEARCH HANDBOOK ON COMPETITION LAW AND DATA PRIVACY 355, 360–79 (Maria Ioannidou & Despoina Mantzari eds., 2025) (discussing the role and limits of privacy considerations in antitrust behavioral remedies, rather than liability claims).

127. *See* FTC Statement on Google/DoubleClick, *supra* note 18.

128. For example, European competition authorities found that the privacy concerns raised by Google's acquisition of fitness tracking company Fitbit were "not within the remit of merger control," but could be addressed by data protection law post-merger. European Commission, *supra* note 40; ERIKA DOUGLAS, DIGITAL CROSSROADS: THE INTERSECTION OF COMPETITION LAW AND DATA PRIVACY 90 (2021) (discussing other jurisdictions).

129. Daniel J. Solove*, Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 596 (2024) ("Consent plays a profound role in nearly all privacy laws.") [hereinafter *Murky Consent*].

130. Heidi M. Hurd, *The Moral Magic of Consent*, 2 LEG 121, 123 (1996).

131. This centrality of consent is often traced to the FIPPs. *See infra* note 191 and accompanying text for a discussion of FIPPs. These foundational principles for U.S. privacy law emphasize each individual's interest in receiving notice of data gathered about themselves and the right to consent to the collection and use of their personal data. *Id.*

without it, the legislation is violated. While notice and consent models of privacy protection are fiercely and extensively criticized, consent remains central to much of existing privacy law. Where that law applies to M&A, be it sectoral, state, or FTC Act Section 5, consent is required to legitimize transactional processing of data.

Corporations regularly invoke this magic of notice and consent by including a "merger" or "business continuity" clause in their privacy policies. While the specifics vary by policy, these clauses tend to give notice of potential personal data processing in connection with a merger, acquisition, or other corporate change in control or asset sale, then grant express consent to the processing, transfer, or sale of data for such purposes. In the fifteen acquisitions studied in this Article, all but three of the targets' pre-acquisition privacy policies contain business continuity clauses that grant permission for collected data to be transferred in a merger or acquisition.[132]

This reflects the ubiquity of these business continuity clauses in modern commerce. One study found that "nearly half" of the terms on the 145 most-visited English language websites "provide that consumer information may be transferred in the event of a sale of a business with no requirement that consumers even be notified of the sale."[133] This widespread use is, in itself, a reflection of the expected and rising value of personal data to companies, including in M&A. Corporations want to ensure permission to transfer power over the personal data they collect.

But merely including a business continuity clause in a policy may not be enough to render lawful the data processing in a merger or acquisition. Of central importance to modern privacy law is not just whether consent was technically obtained, but whether that consent was legally adequate. There are various legal framings of what constitutes "adequate" consent, as Daniel Solove aptly describes:

> Common in the United States, the notice-and-choice approach involves a dubious form of implied consent. Organizations provide a notice of privacy practices, and consent is implied if people fail to opt out of certain forms of data collection and use, or if people continue to do business with the organization. Consent is thus presumed from inaction.
>
> In contrast, the EU's GDPR takes an express consent approach, which requires affirmative and unambiguous consent and rejects implied consent through

132. *See infra* Section IV.B.2 (discussing target policies relying on weak consent to the transaction).

133. *See* Haley, *supra* note 16, at 114.

> inaction. An express consent approach requires that people opt in to the collection and processing of their data by taking an affirmative action to indicate consent, such as checking a box or clicking an accept button.[134]

The first approach, implied notice and consent, is common in U.S. privacy statutes.[135] However, the second approach of express consent more closely resembles the FTC's view on what is required for post-M&A policy changes: "affirmative and express" consent to a material change in data use.[136] More recently, though outside of the merger context, the FTC has continued to require affirmative and express consent, elaborating that this means consent is a "freely given, specific, informed, and unambiguous indication of an individual consumer's wishes demonstrating agreement by the individual, such as by an affirmative action, following a [c]lear and [c]onspicuous [d]isclosure to the individual . . . ."[137] Since, more often than not, Section 5 is the only law applicable to a merger or acquisition, this Article adopts the express consent approach for its analysis in Part IV.

Where privacy law applies to M&A, an important determinant of the scope of such consent is purpose specification. "Purpose specification" is a fundamental concept in privacy law, requiring that the reason(s) why data is being collected be specified at the time of collection and consent so that individuals can understand how their data will be used.[138] The Fair Information Practice Principles ("FIPPs", or sometimes "FIPs", a set of influential principles of privacy protection that formed the basis for much of U.S. privacy law) explain, "There must be a way for an individual to prevent information about [them that was] obtained for one purpose from being used or made available for other purposes without [their] consent."[139] The FIPPs are highlighting here that consent can only be understood in relation to the purposes or uses to which consent is being given. The purposes specified at collection act as a limit on the scope of consent to prevent processing for incompatible uses, which would require further consent to use for those other purposes.

---

134. *See Murky Consent*, *supra* note 129, at 599.

135. *Id.*

136. *See* FTC Letter Re Facebook/WhatsApp, *supra* note 2, at 3.

137. Decision and Order at 2, X-Mode Social, Inc., FTC File No. 212-3038, No. C-4802 (Apr. 11, 2024) https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf [https://perma.cc/6NHC-3FJ3] (defining "affirmative express consent").

138. *See* FIPPs, *infra* note 191, at 41 and accompanying text; Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 520 (2006) (observing that the purpose specification principle is embodied in various privacy laws).

139. *See* FIPPs, *infra* note 191, at 41 and accompanying text.

The concept of purpose specification permeates U.S. privacy law, restricting secondary uses of collected information. For example, the Privacy Act of 1974 requires government agencies to inform individuals of "the principal purpose or purposes for which the information is intended to be used."[140] The GLBA places limits on the "reuse" of personal financial data when provided by one company to another, though as discussed above, mergers are excepted from the scope of this law.[141] And almost all comprehensive state laws require specification of the purpose for which data is collected and processed at the time of collection, and that processing be limited to what is reasonably necessary or compatible with that disclosed purpose, unless further consent is obtained.[142]

The FTC reflects this role of purpose specification in the applicability of Section 5 of the FTC Act to mergers and acquisitions. The agency emphasizes that privacy promises around that use of personal data continue in effect after a deal, and prohibits uses post-transaction that are "materially inconsistent" with promises made when the data was collected, unless further consent is obtained.[143] Florida's and California's comprehensive privacy statutes are similar, and expressly require notice to consumers when the acquiror alters its use or sharing of the personal information in a manner "materially inconsistent" with promises made at the time of collection.[144]

---

140. 5 U.S.C. § 552a(e)(3)(B) (2024).

141. 15 U.S.C. § 6802(c) (2010). The GDPR also offers a succinct illustration of purpose specification. It requires that personal data be collected for "specified, explicit and legitimate purposes" and cannot "further processed in a manner that is incompatible with those purposes." European Parliament and Council Regulation (EU) 2016/679 of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 35, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng [https://perma.cc/7WYD-2UH5].

142. As of August 2025: *see* Cal. Civ. Code § 1798.100(a)(1), (c) (2020); Col. Rev. Stat. § 6-1-1308(2), (4) (2023); Conn. Gen. Stat. § 42-520(a)(1), (2) (2024); Del. Code Ann. 6 § 12D-106(a)(1), (2) (2023); Fla. Stat. § 501.71(1)(a), (2)(a) (2024); Ind. Code § 24-15-4-1(1), (2) (2024); Iowa Code § 715D.7(6) (2025); Ky. Rev. Stat. Ann. §§ 367.3617(1)(a), (b) (2024); Md. Code Ann., Com. Law § 14–4707 (a)(8), (b)(1)(i) (2024); Minn. Stat. § 325M.16(2)(a), (b) (2024); Mont. Code Ann § 30-14-2812(1)(a), (2)(a) (2023); Neb. Rev. Stat. § 87-1129(1)(a), (b) (2024); N.H. Rev. State. Ann. § 507-H:6(I)(a), (b) (2024); N.J. Rev. Stat. § 56:8-166.12(9)(a)(1), (2) (2024); Or. Rev. Stat. §§ 646A.578(1)(a), (2)(a) (2024); 6 R.I. Gen. Laws § 6-48.1-7(s) (2024); Tex. Bus. & Com. Code Ann. § 541.101(a)(1), (b)(1) (2023); Va. Code Ann. § 59.1-578(a)(1), (2) (2024). Utah was the sole exception, requiring that the purpose be stated but not explicitly limiting subsequent use in keeping with that purpose. Utah Code Ann. § 13-61-101(31)(b)(iii).

143. FTC Letter Re Facebook/WhatsApp, *supra* note 2, at 3.

144. CAL. CIV. CODE § 1798.140 (ad)(2)(C) (2024) (adding the caveat that this exemption does not authorize a business to make "material, retroactive" changes to their privacy policies, or other changes that would violate the Unfair and Deceptive Practices Act); *see also id.* § 1798.100(a)(1), (2) (2020); FLA. STAT. § 501.716(1)(k) (2023) (requiring an acquiror to provide sufficient notice to consumers if it intends to materially alter the use or data-sharing practices). Other state comprehensive privacy laws did not contain equivalent provisions at the time of writing.

Purpose specification thus acts as a constraint on the acquiror's consent-based use of personal data post-deal, protecting individuals' data privacy through continuity of use from the target. After the merger, personal data must be used for purposes consistent with the stated pre-merger policy or uses not inconsistent with those purposes. This does not bar the acquiror from using data differently than the target — there is some flexibility — but the uses must not be too far afield from those for which consent was given. If the acquiror uses the data in a new way after a merger or acquisition, the relevant legal question then becomes whether the new use by the acquiror is materially inconsistent. If it is, then the analysis returns to the adequacy of notice and consent for that new use. If it is not, then the original consent is considered adequate. In this way, the concepts of purpose specification and materially consistent use work to achieve an important balance, promoting transparency, predictability, and the formation of reasonable expectations on the scope of data processing, for individuals, while still permitting businesses to use data in related and expected ways.[145]

Finally, while not specific to M&A, any discussion of this notice and consent-based law requires an important acknowledgment: this approach to privacy law protection has faced intense criticism for decades.[146] The well-established scholarly critiques of notice and consent could fill their own volume, and these often center on notice and consent's inadequacy to protect privacy in digital life. The argument is that consent cannot scale in a meaningful way to address the widespread use, collection, and connection of data in the modern economy.[147] This means individuals are inundated with an overwhelming number of privacy choices, making it impractical to read privacy policies or notice, much less seek to understand the legalese in which the policies are written.[148] Scholars argue that this has rendered consent a legal fiction or formalism in some contexts, bearing little relationship to the actual protection of privacy.[149] The broader debates suggest that the FTC's stated legal standard for post-acquisition policy changes — affirmative and express consent for materially inconsistent use[150] — may have limited real ability to protect individuals' privacy interests in deals.

---

145. ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 03/2013 ON PURPOSE LIMITATION 11 (2013), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [https://perma.cc/25LH-7JXW] (explaining the role of purpose specification in data protection law).

146. *See, e.g., Murky Consent*, *supra* note 129, at 596; ARI EZRA WALDMAN, INDUSTRY UNBOUND THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 52 (2021); Hartzog & Richards, *supra* note 24; Haley, *supra* note 16.

147. *See, e.g.*, Hartzog & Richards, *supra* note 24, at 1735.

148. Solove, *supra* note 22, at 5; Waldman, *supra* note 146, at 52.

149. *See Murky Consent*, *supra* note 129.

150. *See* FTC Letter Re Facebook/WhatsApp, *supra* note 2, at 3.

These problems leave notice and consent in a paradoxical position. Despite decades of intense and often merited criticism for its inadequacy in protecting privacy, notice and consent continues to be the main approach of much of U.S. privacy law. Given its continued prominence in the law, this Article evaluates whether there are harms arising from M&A that could be recognized and addressed under those existing paradigms of law based on notice and consent. There has been scant evaluation of whether these "ordinary" notice and consent-based privacy laws are being properly applied to mergers and acquisitions, and it makes sense to, stepwise, examine this application first.

At the same time, the Article takes a skeptical view of the notice and consent protection of existing law. The critiques of notice and consent often have even greater purchase when applied to the types of data transfers that occur in mergers and acquisitions. It can be particularly challenging for individuals to protect themselves against unwanted data transfers and aggregations that take place through M&A. In the complex digital data ecosystem, it is difficult for individuals to know or understand the likely impacts of placing their data, once held by the target, into a new and broader data universe of the acquiror, much less give informed consent to that occurrence. Transactions necessarily place personal data into a new context and create the potential for harms from data aggregation.[151] It is not clear that individuals could understand or predict the impacts, inferences, or the extent of harm to their privacy that can arise from an acquisition-driven combination of data. Without that understanding, it is not clear that individuals are providing meaningful consent to the data processing in mergers and acquisitions.[152]

* * * * *

In sum, this analysis finds transactional privacy law to be a patchy and unintuitive morass. Much of the state and federal legislation that might be expected to apply to M&A does not. This is a function of express exceptions that take M&A out of the definitions of acts like selling or transferring personal data, and of the sectoral nature of these laws, which cover only certain data and entities in a way that places many deals out of scope.

That leaves the more generally applicable Section 5 of the FTC Act to protect transactional privacy. In theory, the FTC could use this law to prevent privacy harms from M&A. In practice, it has not done so. The agency has never brought any privacy cases alleging transactional harms (though it has brought one antitrust case).

---

151. *See infra* Section III.E for a discussion of aggregation harm theory.

152. *See infra* Part V for future research questions that look beyond notice and consent.

Finally, when privacy law does apply, its protection takes the form of notice and consent, with an emphasis on purpose continuity. These consent-based approaches present challenges for transactional privacy protection, and these challenges have yet to be well-examined in privacy debates. This legal labyrinth amounts to M&A exceptionalism, and it leaves behind a lack of effective privacy oversight for much of the selling and transferring of personal data that takes place through mergers and acquisitions.

III. THE THEORY: M&A EXCEPTIONALISM IN PRIVACY LAW IS NOT WELL-JUSTIFIED — OR EVEN WELL-EXPLAINED

As this examination of existing privacy law reveals, mergers and acquisitions that move our personal data often seem to be treated differently. It could be that this M&A exceptionalism is justified. If the judgment is that any harm from M&A to privacy is de minimis, or is outweighed by higher-priority, conflicting policy interests, then privacy law should continue its current approach. After all, privacy law contains many other exceptions where other interests prevail over absolute privacy. Privacy statutes or related rules almost universally contain exceptions to assist law enforcement,[153] and many have exceptions in the name of public health and safety.[154] There are also privacy exceptions to enable data access for research,[155] for reasons of practical efficiency,[156] and to limit perceived compliance burdens on small companies.[157] The law has limits to its willingness to protect privacy interests

153. Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 487, 504 (2013) [hereinafter Murphy] (observing that "every . . . federal statute has, from its inception, provided controlled access [to personal data] for an assortment of entities" such as public health officials, researchers, emergency responders, educators, therapists, medical professionals, and regulators and identifying twenty federal statutes that contain an exception for law enforcement from general protections otherwise applied); *see also, e.g.*, 45 C.F.R. § 164.512(f) (2024) (including HIPAA rule and exception for law enforcement); Gramm-Leach-Bliley Act, 15 U.S.C. § 6802(e)(5) (2023) (including law enforcement exception); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(b)(1)(J)(ii) (2023) (including law enforcement exception).

154. *See, e.g.*, The Privacy Act, 5 U.S.C. § 552a(b)(1)–(13) (2024) (containing exceptions permitting federal agency disclosure of personal data for purposes such as criminal or civil law enforcement by another agency, pursuant to a court order, or where there is a showing of "compelling circumstances affecting the health or safety of an individual," among other exceptions); 45 C.F.R. § 164.512(b) (2024) (including HIPAA rule, public health exceptions); Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(c)(5) (2025) (including exception in the interests of the safety of the child); FERPA, 20 U.S.C. § 1232g(b)(1)(I) (2013) (including health and safety exception).

155. *See, e.g.*, 45 C.F.R. § 164.512(i) (2024) (including HIPAA rule and research exceptions); FERPA, 20 U.S.C. § 1232g(b)(1)(F) (2013) (including research exception).

156. *See* discussion *infra* Section III.C.

157. *See* discussion *infra* note 202.

where other uses of personal data are presumed to be socially advantageous and allowed to prevail over privacy-driven data control.

But these exceptions stand in stark contrast to M&A exceptionalism in that they are well-known and well-debated. These exceptions provoke intense debate over their appropriate scope, particularly those related to law enforcement[158] and public health,[159] which can have constitutional dimensions. While views vary on the appropriate scope of each exception, these debates are valuable in themselves, serving to crystallize the tradeoffs at stake between privacy and these other interests.

There is no equivalent dialogue on M&A exceptionalism in privacy law. Neither privacy law nor scholarship have earnestly turned their mind to, or even sought to identify, the rationales for this light touch toward M&A. The congressional record is largely silent on the reasons for the federal sectoral exclusions of M&A.[160] For HIPAA, the merger exception is not even in the text of the statute that Congress passed — it was created after the passage of the legislation through agency-issued rules.[161] Nor is there clarity around why, at times, mergers and acquisitions are being re-included in the scope of certain privacy legislation at the state level.[162] This quiet is particularly striking in comparison to the rich debates over the legitimacy and scope of many other legislative exceptions to privacy protection in areas like law enforcement or public health.[163] It also seems counterintuitive in light of those debates; the other legislative exceptions mentioned here often present compelling and clear countervailing public interests. The M&A exceptions protect interests of a nature more private, financial, and ill-articulated, yet seem to exist under the privacy radar. This lack of scrutiny has left it unclear why privacy law overlooks M&A, much less whether that approach is justified. The nature of any countervailing interests, their appropriate weight, and the implications for the scope of such M&A exceptions are all unexamined.

---

158. *See generally* Murphy, *supra* note 153; Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,* 102 MICH. L. REV. 801, 857–87 (2004).

159. *See, e.g.*, David O. Argente, Chang-Tai Hsieh & Munseob Lee, *The Cost of Privacy: Welfare Effects of the Disclosure of COVID-19 Cases*, 104 REV. ECON. & STAT. 176 (2022); Lisa M. Lee, Charles M. Heilig & Angela White, *Ethical Justification for Conducting Public Health Surveillance Without Patient Consent*, 102 AM. J. PUB. HEALTH 38 (2012); Julie Myers, Thomas R. Frieden, Kamal M. Bherwani & Kelly J. Henning, *Privacy and Public Health at Risk: Public Health Confidentiality in the Digital Age*, 98 AM. J. PUB. HEALTH 793 (2008).

160. The exception is some congressional reference to the reason for the GLBA exception for M&A, which focuses on continuity of financial services. *See also infra* Section III.C.

161. 45 C.F.R. § 164.502(a) (2024).

162. *See, e.g.*, CAL. CIV. CODE § 1798.120(a)(2) (2024) (requiring acquirors to honor user pre-acquisition opt-out requests after 2024 amendment).

163. *See* Murphy, *supra* note 153; Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254 (2011); Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011).

It is time to scrutinize this M&A exceptionalism in privacy law. The immense commercial value of personal data, its growing role in corporate deals, and the broader re-examination and revitalization of privacy law all point to the need to consider the treatment of M&A. The topic is particularly timely, as leading states like California rethink and narrow their merger exceptions, an approach that other states are likely to follow.[164]

This Part identifies and critiques the likely rationales behind this M&A exceptionalism in privacy law. The probable reasons include the historical framing of privacy rights as individualistic versus collectivist exceptions, the edification of corporate property interests, operational efficiency, presumed consistency with reasonable expectations of privacy, and the continuity fallacy of privacy law. To construct these explanations, the discussion draws on the history of U.S. privacy law, comparisons to other common legislative exceptions whose rationale has been more extensively explained, and the legal treatment of other types of mass personal data sales.

The goal of this Part is to spark normative debate over the appropriate theory or theories to shape how privacy law treats (or excepts) M&A. It also argues that these presumptive rationales are often weak relative to the scale and scope of M&A exceptionalism. It further observes that privacy debates are challenging the same precepts that drive this M&A exceptionalism, such as the assumption that privacy interests are individualistic rather than collective, and the permissiveness around commercial uses of personal data in the digital economy. This privacy rethink should extend to corporate transactions.

A. Individualistic Privacy Versus Collective Public Interests in M&A

M&A exceptionalism can be explained in part by the historical tendency of privacy debates to conceptualize privacy rights as individualistic, and exceptions as collective. This history exists as a backdrop for many of the more specific explanations discussed below.

Information privacy protection and related law have often been framed as a matter of individual control over personal data. From the earliest views of privacy as a "right to be let alone,"[165] to influential views on personal data control,[166] privacy has long been conceived of as an individualized interest in limiting access to self and information about oneself. The philosophical and political underpinnings of privacy emphasized that its value inured to individuals "primarily for self-

164. CAL. CIV. CODE § 1798.120(a)(2) (2024) (requiring acquirors to honor user pre-acquisition opt-out requests).

165. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

166. *See* Alan Westin, *Privacy and Freedom*, 25 WASH. & LEE L. REV. 166 (1968).

development or for the establishment of intimate or human relationships."[167]

But such control has never been absolute. In the 1960s, Alan Westin influentially conceived of information privacy as "the right of the individual to decide . . . when and on what terms [their] acts should be revealed to the general public," but with "extraordinary exceptions in the interests of society."[168] Privacy legislation features many of these exceptions, where privacy protection cedes to other public interests in collecting and processing data.[169] This is reflected in the legislative exceptions canvassed above: law enforcement, public health, research, and efficiency, and many more.[170]

These exceptions have been shaped by views of their collective public benefit, framed in opposition to privacy protection as an individualistic interest.[171] Priscilla M. Regan, in her thoughtful history of privacy legislation from the 1970s onward, explains how the bounds of privacy protection were deeply influenced by this "emphasis on an atomistic individual and the legal protection of his or her rights."[172] The striking of privacy as an individualistic interest set the stage for privacy protection to be balanced or weighed against collective rights or values, and the latter by nature of their collectivism were more compelling. Regan describes the political forces shaping American privacy law as two threads: one promoting self- or individual interest and the other, the public interest.[173] Arguments for privacy have "relied primarily [on] self-interest."[174] In contrast, forces seeking to weaken or limit privacy legislation have relied on both threads, invoking "commitment to the public good" as well as self-interest accommodation.[175] Those

---

167. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 24 (1995).

168. ALAN WESTIN, PRIVACY AND FREEDOM 46 (1967); *see also* FIPPs, *infra* note 191 (emphasizing data control through notice and consent); *see, e.g.*, Jane R. Bambauer, *How to Get the Property Out of Privacy Law*, 133 YALE L.J. F. 1087, 1096 (2024) (noting the recognition that individual control over privacy is not absolute across leading privacy scholars, from the era of Alan Westin in the 1960s to present in the work of Daniel J. Solove, Helen Nissenbaum and Neil Richards). While this paradigm of control is regularly and fairly challenged in debates over privacy policy, much of U.S. federal and state data privacy law continues to rely on it.

169. *See* Murphy, *supra* note 153, at 503 (finding that "no [federal] privacy statutes erect absolute bars to access" to the controlled information).

170. *See* discussion *supra* notes 153–55.

171. REGAN, *supra* note 167, at 24; Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906 (2013) (tracing privacy's roots to "the tradition of liberal individualism, which supplies both the conventional understanding of the self that privacy is thought to protect and the criteria that an intellectually defensible theory of the right to privacy must satisfy").

172. REGAN, *supra* note 167, at 24.

173. *Id.* at 182 (applying Jane Mansbridge's more general framing of political forces specifically to privacy).

174. *Id.*

175. *Id.*

opposing privacy protection have thus benefited from two sources of support, while those concerned about privacy have relied on only one.[176] Framing privacy as each person's right to be "let alone," elicited only self-interest, not broader values, which made it easier to justify legislative exceptions to privacy in the name of countervailing societal interests. The exceptions to privacy rights offered up loftier, shared values, invoking institutional and public values of a higher order than individualism to drive exceptionality from privacy rights.[177] As Regan explains:

> Once this [individualistic framing] occurred, policy formulation focused not on the idea or value of privacy but on how to balance competing interests. Opponents of privacy legislation did not attack privacy as an idea or value but instead emphasized the importance of a competing idea. In each of these cases, the competing idea had broad appeal — efficiency of government operations, law enforcement and national security[178]

M&A exceptionalism reflects this vein of grand compromises that characterize much of data privacy legislation — the judgment that some other, public interest prevails over privacy — and requires the use of personal data to achieve it. Privacy scholarship since the late 1990s has correctly sought to emphasize the many public, social benefits and parameters of data privacy, including its constitutive importance to society, democracy and freedom.[179] But most U.S. federal privacy legislation was born under the narrative of individualism that prevailed before this effort.

Even now, this individualistic view seems to have staying power. In privacy claims, courts continue to have trouble recognizing harms

---

176. *Id.* at 183.

177. *Id.* at 3 ("In the case of information privacy, in which privacy advocates had no other allies, the balancing involved in establishing fair information principles was framed in terms of the individual interest in privacy versus organizational and public interests.").

178. *Id.* at 210.

179. *See, e.g.*, Cohen, *supra* note 171, at 1906 ("In short, privacy incursions harm individuals, but not only individuals. Privacy incursions in the name of progress, innovation, and ordered liberty jeopardize the continuing vitality of the political and intellectual culture that we say we value."); Danielle K. Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 818 (2022) ("Privacy harms often involve injury not just to individuals but to society."); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 882–84 (2003); Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 724 (1999) (discussing how decisional privacy allows "individuals, families, and other nongovernmental entities" to make important choices).

beyond those at the individual level.[180] Comprehensive state legislation, despite originating thirty years after the era Regan describes, still contains similar exceptions for M&A.[181] To the extent that paradigms of individualist protection versus collectivist exceptions shaped the treatment of M&A in privacy law, that shape persists today.

This still leaves an important question: what exactly are the countervailing public interests animating the M&A exceptions in privacy law? Perhaps the most obvious one rests on corporate law conceptions of shareholder interests in value realization. The standard justification for allowing mergers and acquisitions is that such transactions can advance the financial interests of those with a stake in the corporation.[182] The M&A exceptions allow shareholders of the target corporation to realize the value of the corporation's investments in the collection, use, and other processing of personal data.

Relatedly, the M&A exceptions may resonate in innovation policy and the incentives created by startup exit opportunities. More than ever before, venture exit is occurring via acquisition rather than through initial public offerings.[183] The lure of value realization from startup companies that process personal data may rely in part on the ability to sell to a corporate buyer.

But the realization of shareholder value, including through corporate transactions, may be more about the advancement of private than public interests. Corporate law is quick to defend the importance of shareholder value creation, but that value accrues primarily to a narrow and privileged slice of the public that holds stock. For example, the M&A legislative exceptions apply equally to acquisitions of public and private companies. The acquisition of a private or even closely held corporation benefits from the same exemption, even though it benefits the few who own the target. Of the fifteen deals analyzed in this Article, all but four were acquisitions of privately held targets.[184] The deals benefited the pool of owners, which often comprises founders, investors, and employees for these types of technology companies.

---

180. Citron & Solove, *supra* note 179, at 818–19 (observing that courts "often still fail to consider the societal impact of privacy harms" even when lawsuits seek to edify those interests).

181. *See supra* Section II.B.1 (discussing state exceptions for M&A).

182. *See, e.g.*, Ian B. Lee, *The Role of the Public Interest in Corporate Law*, *in* RESEARCH HANDBOOK ON THE ECONOMICS OF CORPORATE LAW 106, 106 (Claire A. Hill & Brett H. McDonnell eds., 2012) (explaining that the standard account of how corporate law advances the public interests is by "facilitating transactions in which individuals pursue their private interest" but noting a more progressive school of corporate thought that seeks to expand the role of corporate law in achieving public interests by using it to constrain corporate actors' pursuit of their own interests).

183. Florian Ederer & Bruno Pellegrino, *The Great Startup Sellout and the Rise of Oligopoly,* 113 AM. ECON. ASS'N. PAPERS & PROC. 274, 276 (2023) (documenting the decline of IPOs as a mechanism of startup exit).

184. The publicly traded target companies included in this analysis are Fitbit, LinkedIn, One Medical, and Whole Foods.

Other identifiable interests of the public, or at least a set of users, may include continuity to receive the target's services, and efficiency. M&A exceptions ensure that data is accessible post-acquisition, enabling service continuity. Another possible public interest is that of practical convenience or efficiency, that users are not required to spend their time and attention to consent to data processing within their reasonable expectations of privacy. The assumption of reasonable expectations may beg the question of whether these deals are in the public interest. These rationales are interrogated in more depth below.

On the whole, these public benefits have not been well-articulated and seem to pale in comparison to the interests that compel the other common statutory exceptions in privacy law. Privacy statutes or related rules almost universally contain exceptions to enable law enforcement[185] and often contain exceptions in the name of public health and safety[186] and to enable data access for research.[187] This list reflects an array of more apparent and compelling public interests, with each exception rooted in collective benefits that weigh heavily against the control of private information.[188] Yet still these exceptions draw much more scholarly debate than those for M&A. At the very least, the assumed public interests in M&A should be expressly identified to enable an equivalent debate.

Finally, to the extent that M&A exceptionality relies on the assumption that all mergers are in these (or some other) public interest, that rationale is far too general to withstand scrutiny. Other areas of law that apply a public interest standard to mergers ask whether *particular* deals, or types of deals, are in that interest. These other laws also identify criteria against which to measure the implicit or express public interest of a deal. These are often specific to the area of law. For example, telecommunications law considers how a deal could impact fair access to services and competition, antitrust law considers how deals may harm competition, and national security law considers the risks of foreign ownership, control or influence. The benefits and risks depend on the specific deal characteristics. In 2024, Congress required the divestiture of Chinese ownership in TikTok, a social media company, based on a national security concern that the company would act as a conduit for foreign access to U.S. user data.[189] In antitrust law, the public

185. *See* discussion *supra* note 153.

186. *See, e.g.*, 5 U.S.C. § 552a(b)(8) (2024); 20 U.S.C. § 1232g(a)(4)(B) (2013).

187. *See, e.g.*,45 C.F.R. § 164.512(i) (2024).

188. *See* Murphy, *supra* note 153, at 515 (arguing the scope of these exceptions varies widely and does not follow an "intuitive scaling of protections" relative to the privacy or countervailing public interest at stake — for example, cable records are arguably more protected than health records).

189. Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024). TikTok itself is a U.S. company, but its ultimate

benefits of a merger also depend on the characteristics of the deal, in particular, whether the target and acquiror are competitors. The legislative exceptions in privacy law consider none of these factors. Instead, they bluntly exclude all M&A, with no attention to the criteria that determine the public interest, which can be deeply affected by the parties to the deal. This generality of the M&A exceptions makes it difficult to discern their basis, and whether such treatment in law is defensible.

B. Edification of Corporate Property Interests in Personal Data

Another likely driver of M&A exceptionalism in privacy law is the edification of corporate property interests in personal data. The laws of property convey limited power over how or when property is used.[190] The M&A exceptions in privacy law are, in effect, conveying such power over how and when personal data held by the target is used. By excluding M&A from its scope, privacy legislation in effect gives the target the power to pass along those interests in collecting and processing our personal data to the entity that acquires it in a transaction. The data being sold is "ours" in the sense it is personal in nature. But this M&A exceptionalism also edifies the property interests of the corporation that collected, processed, and stored that data, as an asset and value driver of the company and its services.

The historical roots of privacy law are consistent with this rationale behind M&A exceptionalism. Most U.S. federal data privacy law is modeled on the FIPPs, a series of influential, basic principles of privacy protection.[191] The FIPPs tend to be cast in the model of the discussion above, in which privacy protection emphasizes control, but with recognized limits in the public interest. Some scholars, though, identify in the FIPPs a recognition of mutuality of interests in personal data.[192] As

---

parent, ByteDance Ltd. is based in China. For a more detailed discussion of the Congressional and presidential actions against TikTok, see Peter Swire & Samm Sacks, *The New Intersection of Privacy and National Security: Personal Data as a Dual Use Technology* (May 25, 2025) (on file with author).

190. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972).

191. U.S. Dep't of Health, Educ. & Welfare, Records Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems 41–42 (1973), https://epic.org/wp-content/uploads/2021/11/1973-hew-report.pdf [https://perma.cc/AQ4E-QADC] [hereinafter FIPPs]. Originally articulated in the 1970s by the U.S. Department of Health, Education, and Welfare, the FIPs or FIPPs have reached far beyond their health-specific origins to shape the core of privacy law. The FIPPs state that "[t]here must be a way for an individual to prevent information about [themselves] that was obtained for one purpose from being used or made available for other purposes without [their] consent." *Id.* For more on the development of the FIPPs, see Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 Md. L. Rev. 952 (2017).

192. Jane R. Bambauer, *How to Get the Property Out of Privacy Law*, 133 YALE L.J. F. 1087, 1096 (2024).

the Department of Health, Education, and Welfare explained in the FIPPs:

> records of personal data usually reflect and mediate relationships in which both individuals and institutions have an interest, and are usually made for purposes that are shared by institutions and individuals. In fact, it would be inconsistent with this essential characteristic of mutuality to assign the individual record subject a unilateral role in making decisions about the nature and use of [their] record.[193]

Such a mutuality of interest is reflected in privacy legislation's M&A exceptions, though it is not articulated expressly in these terms. By allowing personal data to be transferred in corporate transactions, a bounded corporate interest is being recognized and edified by privacy law in the personal data corporations cultivate from individuals. That interest includes the power to transfer the data via a corporate transaction, within the bounds of the consent of those individuals.

While this may be the rationale behind such exceptions, it does not necessarily justify the current legal treatment. M&A exceptions in privacy law serve to legitimize commercial ownership interests in our data. In doing so, these exceptions reflect the judgment that corporate interests take precedence over the public or other countervailing interests in transactional data privacy. But across privacy law, debates are raging around this very issue of the legitimacy and appropriate bounds of such commercial interests in our personal data.

Scholars are framing privacy in terms of dignity, sovereignty, and ethics as a means of contesting the assumed benefits of monetizing our personal information in the digital world. Perhaps most famously, Shoshana Zuboff has challenged the very idea of this "surveillance capitalism," casting it as an invasion of dignitary interests that intertwine privacy with self.[194] Anita Allen objects to the bargaining away or waiving away of privacy rights, at least in some core areas, on grounds that privacy is a fundamental right that belongs to the core of human dignity.[195] Daniel Solove, Woodrow Hartzog, and Neil Richards have all pushed recently for U.S. data privacy law to reevaluate the desirability of pro-market assumption around personal data transactions.[196]

---

193. FIPPs, *supra* note 191, at 40.

194. Zuboff, *supra* note 22.

195. ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 171 (2011).

196. *See, e.g.*, Solove & Hartzog, *supra* note 87; Hartzog & Richards, *supra* note 24; Solove, *supra* note 22, at 35–36 ("The fact that people trade their privacy for products or services does not mean that these transactions are desirable in their current form . . . . [T]he mere fact that people make a tradeoff does not mean that the tradeoff is fair, legitimate, or justifiable.").

This reevaluation speaks to the core goals of data protection regimes, which "seek to permit more ethical surveillance and data processing at the expense of foundational questions about whether that surveillance and processing should be allowed in the first place."[197]

The FTC has, at times, also begun to reexamine the status quo of corporate monetization of personal data in the digital world. Under the Biden Administration, the FTC provocatively self-described one of its rulemaking forays as a "crack down on harmful commercial surveillance and lax data security."[198] The term "commercial surveillance" is defined simply as "the business of collecting, analyzing, and profiting from information about people."[199] This encompasses much of the now-lawful commercial activity in the digital economy, and in doing so, views the selling of personal data, and its use for targeted advertising, with unprecedented suspicion. It demonstrates a new willingness to query the appropriateness of commercial use of personal data *in itself*, rather than any particular practices or harms that occur when data is processed for profit in certain ways, such as without consent.[200]

M&A exceptions belong squarely within those normative debates around corporate interests in personal data, but so far have been overlooked. It is worth asking whether privacy law should continue to empower corporations to transfer our personal data in mergers and acquisitions and considering any limits the law should impose on that power. This has only been addressed in certain narrow contexts where privacy legislation does apply to M&A, such as deals that trigger COPPA protection. Many other deals have no statutory protections. There is no debate, much less an answer, on the appropriate legal bounds of corporate interests in personal data bought, sold, or transferred through mergers and acquisitions.

C. Efficiency or Operational Convenience

Another reason for M&A exceptionalism is likely operational convenience or efficiency. As scholar Jane Bambauer frames it, privacy statutes were modeled on the FIPPs, which emphasized control "while leaving enough leeway and loopholes for the regulated industries to achieve some minimum level of innovation and operational

197. Hartzog & Richards, *supra* note 24, at 1693–94.

198. Press Release, FTC, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices [https://perma.cc/G8GV-BBJU]; *see also* Fed. Trade Comm'n ANPR on Com. Surveillance, *supra* note 29.

199. Fed. Trade Comm'n ANPR on Com. Surveillance, *supra* note 29.

200. *Id.* ("The FTC is concerned that companies monetize surveillance in a wide variety of ways. Companies may use some of the information they collect to provide products and services, but they can also use it to make money.").

efficiency."[201] Applied here, the logic is that corporate transactions will routinely occur, and consumer or business interests in the continuity of those business operations compel M&A exceptions from privacy law. This countervailing interest in commercial efficiency may explain M&A exceptionalism, and it coexists with the rationale of protecting corporate property interests in data.

The related assumption is that the administrative costs of seeking consent to routine corporate transactions outweigh the likely benefits to privacy protection of doing so. In simple terms, consent costs time and money. Including M&A in the scope of privacy law would impose real administrative costs, both on companies seeking to comply with notice and consent requirements as they execute mergers, and on individuals in the time it would take to consent to such transactions.

Privacy legislation is riddled with other "practical" exceptions that seem to be driven by similar rationales of efficiency or convenience.[202] The Privacy Act allows governmental uses that are "routine" without requiring consent.[203] Sometimes exceptions are necessary for the operation of the legislative scheme, as under COPPA, which permits the use of children's information to know from whom to obtain the consent that the law itself requires.[204] Still other exceptions have a duality of character that suggests efficiency is a driver alongside reasonable expectations of privacy. For example, the GLBA limits disclosure of certain financial information to unaffiliated third parties, but contains an exception to permit such disclosure where it is necessary to provide services the consumers themselves requested.[205] Similarly, HIPAA contains exceptions to its usual protections to permit covered entities to use and disclose protected health information for the purposes of medical treatment and collecting payment.[206] It is reasonable to assume that we, as data subjects, want our banks to use our financial information to

201. Bambauer, *supra* note 168, at 1095.

202. Other bounds of privacy laws also seem to have an efficiency character. For example, many U.S. state laws do not apply to businesses below a certain size, or to nonprofits. *See, e.g.*, VA. CODE § 59.1-576(A)–(B) (2024) (applying only to businesses that meet certain thresholds for the number of consumers whose personal data is processed, and excluding "any . . . nonprofit organization . . . ."); CAL. CIV. CODE § 1798.140(d) (2024) (defining "business" based on minimum revenue or user numbers). This is not because such businesses are so unlikely to violate privacy law that they ought to be excluded. From the perspective purely of privacy protection, such business should be included and may even pose a greater likelihood of violations due to fewer privacy compliance resources. Their exclusion echoes in a regulatory efficiency compromise — the compliance costs and burdens of privacy law are thought to be too onerous for the smallest entities relative the scale of likely data processing harms.

203. 5 U.S.C. § 552a(b)(3) (2024).

204. 15 U.S.C. § 6502(b)(2)(B) (1998).

205. 15 U.S.C. § 6802(e)(1)(A) (2010) (permitting disclosure of personal information to nonaffiliated third parties "as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer" in connection with certain specified financial activities and services).

206. 45 C.F.R. § 164.506(c) (2013).

give us services we have requested, and want our medical providers to access and use our medical history to give us medical treatment. While the costs of notice and consent are justified to protect privacy in certain situations, in these instances, the legislative judgment seems to be that the administrative burden outweighs the likely privacy benefits and expectations.

This rationale is interrelated with the presumed value of service continuity after a corporate transaction. It impliedly assumes that individual users benefit from M&A exceptions, because these exceptions enable the target's data-driven services to continue to be offered after the deal.[207] It is fair to infer some interest on the part of individual users in continuing to use the target's services. Imagine the target company operates an email service; post-acquisition, consumers would benefit from the continued access to their email accounts, and their past email messages. If instead the personal data was barred or limited from being transferred as part of a corporate transaction, the merger or acquisition could threaten the delivery of services from the target's business. The deal might lead to individuals losing access to their old information, the deletion of that information, and limits or even termination of services previously offered by the target. The M&A exceptions seem to assume the value of this service continuity is so great that the prudent course is to save the data subject and the controller of resources that would be expended on obtaining consent.[208]

This efficiency rationale is expressly reflected in the history of the HIPAA exception for M&A between covered entities. In its 2002 final notice on a revised HIPAA privacy rule, the U.S. Department of Health and Human Services seemed to agree with comments on this exception that intertwined the benefits of service continuity with avoidance of unnecessary consent burdens, observing that:

> health care would be delayed and consumers would be inconvenienced if covered entities were required to obtain individual consent or authorization before they could access health records that are newly acquired assets resulting from the sale, transfer, merger, or consolidation of all or part of a covered entity. Commenters further claimed that the administrative burden of acquiring individual permission and culling records of consumers who do not give consent would be too great, and would cause some entities to simply store

207. *See supra* Section III.C.
208. *See* discussion *infra* Section III.D.

> or destroy the records instead. Consequently, health information would be inaccessible.[209]

Similar rationale appears in the history of the GLBA exception for mergers and acquisitions. A report from the Committee on Banking and Financial Services on the (then) proposed GLBA explains the purpose of the M&A exception (and others under Section 501(d)) as follows:

> The scope of these exceptions is designed to ensure that the disclosure, access, and opt-out rules promulgated by the FTC pursuant to the subtitle do not impede the ordinary business activities of financial institutions or their ability to provide a multitude of services in an efficient manner to their customers.[210]

It is worth re-examining these related efficiency assumptions on service continuity relative to the burden of consent. On one hand, the costs of obtaining consent may have been practically different in the 1990s and early 2000s when these exceptions were crafted. At the time, obtaining consent likely required more paper and cost to complete by mail than the online consent that would be typical today. On the other hand, the benefit of service continuity from a corporate transaction depends heavily on the counterfactual of what would occur without the deal. If, in the absence of the acquisition, the target would have continued to provide access to the same services or goods on similar privacy terms, then the deal is not necessary to achieve the benefit of service continuity. If the target would have ceased offering services in the absence of the transaction, then individuals do benefit from service continuity from the deal — without it, they would lose access to the services, and perhaps to their data itself. Such a failing firm scenario for targets may be rare, though. None of the firms examined for this Article were on the verge of going out of business before the acquisition.[211]

By this logic, service continuity offers a fairly weak justification for M&A exceptionalism, because individuals are likely to continue receiving the target's services even without the deal. Privacy law

---

209. Final Rule, Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182, 53190 (Aug. 14, 2002) (to be codified at 45 C.F.R. 164).

210. H.R. Rep. No. 106-74, pt. 3, at 202 (1999).

211. Another potential scenario is that the personal data, or access to it, is omitted from the deal, but services continue. This seems unlikely for the data-driven acquisitions examined here. The personal data is a value driver for the corporate transaction. Without it, the target loses much of its value, and the transaction is unlikely to go ahead. The services often cannot function without data access. That leaves the first scenario as the most likely — that the target continues operating without the acquisition — except in unusual situations of bankruptcy, which is already subject to legal oversight of the privacy impacts.

accounts for none of this potential variation in its treatment of corporate deals, exempting M&A regardless of alternatives to the deal or actual service impacts. Nor does it recognize that a merger or acquisition offers no promise of continuity. It is also possible that the acquiror buys the target and terminates certain of its services.

More fundamentally, this rationale of efficiency or operational convenience assumes that individuals are agnostic towards which entity processes their data, Company A (target) or Company B (acquiror). The outcry over transactions like Facebook's acquisition of WhatsApp, and Google's acquisition of Fitbit suggests that is not the case for certain acquisitions.[212] Whether or not the deal is within users' reasonable expectations of privacy can depend on acquiror identity, an issue examined separately below.

The scope of the M&A exceptions is also distinguishable in an important way from the other types of efficiency or operational exceptions mentioned above. These other exceptions in the GLBA, HIPAA, and COPPA tend to limit the *purpose* for which the data can be used: to advance fairly assumed interests of the consumer, such as providing requested financial services or health services, or to solicit a required consent to data processing. The legislative exceptions for M&A are much less fettered by a particular purpose for the data use. They permit the deal itself, and after it, impose no equivalent limits on the purpose for which the data is used by the acquiror. That later use may not be consistent with the reasonably inferred desires or requests of the data subject like it is for these other exceptions. Although that later use may be limited by applicable sectoral laws, and by Section 5 of the FTC Act, which require affirmative, express consent to material changes,[213] Section 5 is not being enforced in the context of M&A. This leaves any post-acquisition uses less constrained by law than other efficiency-driven exceptions in privacy law.[214]

Finally, to the extent that M&A exceptions in sectoral laws rely on a perceived choice between service continuity and the application of privacy law, that is a false dichotomy. The assumed benefits of service continuity could often be achieved even if privacy law was applied to M&A. If companies had to seek adequate consent to data-driven transactions, individual users could still benefit from continued services if they consent. A consent requirement would simply transfer the decision about the costs and benefits of service continuity to individual data

212. *See* EPIC WhatsApp Complaint (2014), *supra* note 1, at 6–8.

213. *See*, *e.g.*, FTC Letter Re Facebook/WhatsApp, *supra* note 2; Decision and Order, X-Mode Social, Inc., *supra* note 137; Final Decisions and Order, BetterHelp, Inc., FTC File No. 202 3169, No. C-4796 (July 7, 2023) (requiring affirmative, express consent for Section 5 FTC Act compliance).

214. The legislative exceptions impose no purpose limitations (other than use for the merger or acquisition), but the privacy policy of the target may limit the purposes for which personal data is used. This is discussed below. *See infra* Section IV.C.2.a.

subjects, instead of assuming such benefits for every deal and every individual. By the same logic, the target's services could continue to be offered after the deal even if the acquiror made express commitments around the continuity of privacy protection. To the extent that M&A exceptionalism is premised on public benefits from service continuity and the costs of consent, that offers weak justification for its breadth.

D. Presumed Consistency with Reasonable Expectations of Privacy

M&A exceptionalism could also be premised on reasonable expectations of privacy. The underlying assumption may be that individuals' reasonable expectations of privacy do not extend to the data processing that occurs in corporate transactions. There has been little examination of what the expectations of privacy may be for corporate transactions, other than the FTC's unenforced view that material changes in use without express, affirmative consent are beyond those expectations.

The assumption that all M&A-related data processing falls within reasonable expectations of privacy is too general to withstand scrutiny. It overlooks all context specific to a corporate transaction. The substance of such an expectation, or perhaps more accurately whether deal-related data processing lies within it, is likely to depend on transaction-specific facts. These may include industries of the buyer and seller, privacy promises made by the target, the privacy reputation of the buyer, and whether the standards of privacy protection will be maintained after the transaction. The public outcry over certain mergers, such as Facebook's acquisition of WhatsApp, seemed to depend on several of these variables.[215]

The M&A exceptions, in other words, make blunt assumptions about reasonable expectations of privacy. Legislative exceptions for mergers and acquisitions do not account for any of the above variables that can influence expectations, except when both target and acquiror are covered by a sectoral statute, such as HIPAA (which relies on the continuity fallacy, discussed below). The FTC seems to account for some of these factors in its views of when enforcement should occur, yet its action to protect privacy in response to them has been almost nonexistent.

Further, the assumption that all M&A are within reasonable expectations of privacy is difficult to reconcile with privacy law's treatment of other mass sales of personal data. The law intervenes to protect privacy interests when data is auctioned off unfairly by data brokers, transferred to third parties under contracts without adequate consent, or sold

215. *See, e.g.*, EPIC WhatsApp Complaint (2014), *supra* note 1. This Article explores how several of these deal-specific variables impact data privacy, particularly acquiror identity, by examining real transactions in Part IV.

in bankruptcy as an asset.[216] Privacy law views mass, opaque sales of personal data as often harmful when they occur through these other transactions; it is not clear why all M&A, which can do the same thing, should be treated differently. These other contexts are not identical to M&A, but can raise similar concerns over the effects on privacy of mass personal data selling and transfers.

As a starting point, commercial uses of data have long drawn closer scrutiny from privacy law than non-commercial uses. In particular, the act of "selling" personal data has often been of concern, although its lawfulness tends to be tied to consent. The adamant corporate promise that we "do not sell or rent user personal information to anyone" was one of the first to appear on websites[217] and continues to be ubiquitous today. In comprehensive state privacy law, one of the earliest rights to emerge was the right to opt-out of the sale of personal data.[218] Conversely, the same state laws often exclude nonprofit entities from their scope, meaning that non-commercial data use is permitted.[219]

Privacy concerns are often heightened when large amounts of personal data are being sold. This is reflected in the privacy treatment of bankruptcy, and of data brokers, but not in the treatment afforded to mergers and acquisitions.

At the federal level, the selling of personal data in bankruptcy proceedings is one of the few areas of law that affords express privacy protections in a transaction.[220] The assets of a bankrupt company can include valuable personal information. Before amendments to the Bankruptcy Code in 2005, trustees in bankruptcy proceedings were selling such personal data to the highest bidder, regardless of the bidder's privacy bona fides, and despite such sales violating the bankrupt

---

216. *See* Complaint ¶¶ 52–53, X-Mode Social, Inc., *supra* note 103; Bradley, *supra* note 16. While these contexts are not identical to M&A, they offer parallels to understand harm that may arise in deals, and demand reconciliation with the current permissiveness toward mergers and acquisitions.

217. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE A REPORT TO CONGRESS 25 (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf [https://perma.cc/NM2G-EH9X] (finding that website privacy policies often used general privacy protective language, including the example that the company "does not sell" user information).

218. CAL. CIV. CODE § 1798.120(a)(1) (West 2024) (requiring businesses to provide customers the opportunity to opt-out of the sale of their data).

219. *See supra* note 202 (discussing exceptions for nonprofit entities in state comprehensive privacy laws).

220. *See, e.g.*, Sara Gerke, Melissa B. Jacoby & I. Glenn Cohen, *Bankruptcy, Genetic Information, and Privacy — Selling Personal Information*, 392 NEW ENG. J. MED. 937 (2025) (recent, high-profile example of the genetic data sold in the 23andMe bankruptcy).

company's privacy policy.[221] These trustees and creditors were unconcerned with privacy; their goal was to maximize the value recovered from selling that personal data as an asset. In 2005, Congress made the choice to impose certain privacy protections on these data sales. It amended the Bankruptcy Code to require the sale of personal data in bankruptcy to comply with the debtor's privacy policy, or with privacy law.[222] Privacy ombudspersons are now appointed to assess the legality of the sale of consumer data in such proceedings, particularly when the sale is not permitted by the bankrupt company's privacy policy.[223] This provides at least some privacy protection for individuals whose personal information is auctioned off in bankruptcy proceedings, in exchange for a potential decrease in the value that creditors recover from such data sales.[224]

It is theoretically inconsistent to protect privacy interests when personal data is being sold in bankruptcy, yet not in the much more common situation of personal data transferred or sold in M&A. It is tempting to point to the very fact of legal oversight of bankruptcy data sales as the key difference between the two, but that begs the question of whether the law ought to intervene in M&A as well. Many ordinary-course acquisitions are subject to legal intervention and oversight from other areas of law: antitrust, securities, corporate law, national security, industry regulation and beyond. When adequately important public interests are at stake, Congress regularly creates law that conditions or oversees mergers and acquisitions. It could choose to do so for data privacy in certain mergers and acquisitions, just as it does for bankruptcy, if that is necessary to prevent harm.

---

221. First Amended Complaint for Permanent Injunction and Other Equitable Relief ¶ 11, Toysmart.com, Inc., FTC File No. 00-11341 (D. Mass. July 21, 2000); *see also* Press Release, FTC, FTC Requests Bankruptcy Court Take Steps to Protect RadioShack Consumers' Personal Information (2015), https://www.ftc.gov/news-events/news/press-releases/2015/05/ftc-requests-bankruptcy-court-take-steps-protect-radioshack-consumers-personal-information [https://perma.cc/2WKL-KP7S].

222. Bankruptcy Abuse Prevention and Consumer Protection Act of 2005, Pub. L. No. 109-8, § 231, 119 Stat. 23, 72–73 (2005) (codified as amended at 11 U.S.C. § 363(b)(1) (2023)) (amending section 363(b)(1) of title 11 of the United States Code to include restrictions on a debtor's ability to transfer personally identifiable information when a privacy policy restricts its transfer). When the debtor has a privacy policy that prohibits the transfer of personally identifiable information that is being sold or leased as an asset, such a transfer is allowed in bankruptcy only if the transfer is (1) consistent with that debtor's privacy policy or (2) after appointment of a privacy ombudsperson, the transfer is approved by a court that finds it would not violate privacy law (or other "non-bankruptcy" law). 11 U.S.C. § 363(b)(1) (2023).

223. 11 U.S.C. §§ 332, 363(b)(1)(B) (2023) (providing for the appointing of a privacy ombuds where the sale of consumer data would be contrary to an existing privacy policy); Bradley, *supra* note 16, at 161 (observing that although the provisions of the Act may not require it, ombuds have still been appointed in "a number of cases" where the transfer likely complies with the privacy policy).

224. *But see* Bradley, *supra* note 16, at 194–95 (observing that these protections afforded in bankruptcy are limited by the frailties of data privacy law itself).

Data brokering is another area of privacy law concern over mass personal data buying and selling that is hard to reconcile with M&A exceptionalism. Since the late 1990s, the FTC has scrutinized data brokers, whose business is to collect personal information from an array of sources for the purpose of reselling or sharing that data with other businesses.[225] The FTC has conducted industry studies, published awareness-raising reports, and taken enforcement action, all in a sustained effort to limit the data broker industry and its effects on privacy.[226] The agency's effort continues today.[227]

The agency's concerns over data brokers echo in certain mergers and acquisitions, though perhaps less acutely. The FTC has framed the data broker problem as primarily one of transparency, or a lack thereof, for the data subjects whose information is being bought and sold by these brokers.[228] Because data brokers are not consumer-facing — meaning these companies do not provide products or services directly to the consumers about whom they collect information — consumers are often unaware of the existence of data brokers. The identity of the broker selling consumer information is opaque because the broker has no direct relationship with the consumer.[229] The information collection itself also lacks transparency; the data is gleaned from a variety of sources the consumer did not intend for use by a data broker, such as "bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' everyday interactions."[230] Consumers may be unaware that information is being collected by data brokers from these sources. The FTC concern seems to be exacerbated by the sheer scale of data broker operations. It observes that of nine brokers examined in the study, one held "over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new records each month to its

225. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014) (noting that "since the late 1990s" the FTC has been active in examining the practices of data brokers; defining "data brokers") [hereinafter FTC REPORT, DATA BROKERS].

226. *See id.* (emphasizing throughout concerns related to a lack of transparency and accountability for data brokers); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 69 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/EDM6-XBXZ] (observing opacity in data broker practices not covered by the Fair Credit Reporting Act and recommending legislation to improve the transparency of industry practices).

227. *See, e.g.*, Decision and Order, X-Mode Social, Inc., *supra* note 137.

228. FTC REPORT, DATA BROKERS, *supra* note 225, at i.

229. *See, e.g.*, Complaint ¶¶ 46–47, X-Mode Social, Inc., *supra* note 103 (observing that "consumers never directly interact with" the impugned data broker, and that "[t]he market for mobile location data is complex and typically opaque to consumers").

230. FTC REPORT, DATA BROKERS, *supra* note 225, at 46.

databases."[231] The scope of information held by these companies raised concern, given the brokers' or buyers' potential ability to infer other information from these data points, including sensitive information.[232]

Personal data M&A can raise similar concerns around transparency, aggregation and scale. While there are distinctions between data brokering and M&A — both acquiror and target may be known to the consumer, and M&A tends to involve a single sale or transfer, not the repeated sale of personal data of data brokering — there are also striking parallels. Like the business of data brokers, mergers and acquisitions can increase data access for the acquiror, and by doing so, create the potential for harm from aggregation and cross-referencing, which can reveal otherwise undisclosed information about individual data subjects.[233] Like data brokering, these corporate acquisitions also effect mass buying and selling of consumers' personal data. Targets may have millions of users and masses of their personally identified or identifiable information, which is part of their commercial value to the acquiror. Consider for example, that when Google acquired Fitbit, the company held health tracking data from twenty-eight million users.[234] This included trillions of measurements on heart rate, sleep hours, steps and menstrual cycle tracking.[235] Publicly available estimates of the scale of data transferred in the fifteen deals examined here are included in Appendix A. All involve massive amounts of user information.

Finally, as with data brokers, a personal data merger or acquisition can raise transparency concerns. The sale of a target makes personal data available to a buyer with whom the individual user may have no prior relationship. Individuals whose data is at stake may or may not have interacted with the acquiror. An acquisition, like a data brokerage, is a business-to-business transaction, not consumer-facing. Consumers whose data is transferred or accessed may not even be aware that a deal is occurring in a merger or acquisition, much like in data brokerage. Corporate transactions may often be higher profile than data broker activities, and thus perhaps more likely to come to the attention of consumers, but that depends on the level of deal publicity. If anything, the consumer may become aware that their data has been acquired after the transaction occurs, perhaps by virtue of a new privacy policy being announced. This timing makes it challenging for individuals to protect their privacy rights in an effective manner, as data has already flowed

231. *Id.* at 46–47.

232. *Id.* at 47–49.

233. *See infra* Section III.E for a discussion of the risk of aggregation harms from mergers.

234. Fitbit Team, *Fitbit to Be Acquired by Google*, GOOGLE BLOG (Oct. 17, 2019), https://blog.google/products/fitbit/fitbit-be-acquired-google/ [https://perma.cc/8ADM-SX7X].

235. Griebeler da Motta, *supra* note 9.

to a new entity and the privacy consequence of that change may be difficult to undo.

For all of these reasons, it can be difficult for consumers to protect themselves against unwanted data transfers that occur through mergers and acquisitions. This inability of consumers to protect themselves from harm is an element of a Section 5 unfairness claim, which requires harm that individuals cannot "reasonably" avoid by themselves.[236]

On a broader scale, these comparisons to bankruptcy and data brokering highlight that M&A has somehow escaped the scholarly and agency reckoning around commercial uses of personal data. As discussed above, scholars have mounted increasing criticism of the commercial exploitation of personal data, and have been joined at times by federal agencies like the FTC.[237] This reflects a new skepticism toward the starting assumption in U.S. law that personal data should, by default, be available for commercial use. Yet mergers and acquisitions that give glaring, sudden, and widespread access to our personal information are strangely missing from this debate. Both this new skepticism over commercial uses of personal data, and the classic, longstanding privacy concern over selling of personal data in bankruptcy and data brokering seem at odds with the limited attention paid to personal data mergers and acquisitions. These corporate transactions that sell personal data are a natural point at which to consider the propriety of recognizing corporate interest in that data and to exert control to achieve privacy protection on behalf of many individuals. It seems conceptually inconsistent for privacy law to fret over ordinary course, everyday data-selling, or bankruptcy and data brokers, while treating personal data M&A with such leniency.

E. The Continuity Fallacy in Privacy Law Misses the Potential for Deal-Driven Harms Like Aggregation and Muddying

The unstated logic of M&A exceptionalism seems to be as follows: if privacy law applies before the transaction (to the target), and privacy law applies after the transaction (to the acquiror), then the transaction will not give rise to privacy harm. An example is the HIPAA rules, which allow HIPAA-covered entities to engage in transactions with each other without violating their statutory obligations.[238] This covered-entity exception envisions a seamless transaction in which privacy

236. FTC Policy Statement on Unfairness, *supra* note 96.

237. *See supra* text accompanying notes 194–99.

238. The first version of the HIPAA privacy rules hinted at this logic, as the language in this exception referred to a "successor in interest" upon a sale or transfer of its assets, implying the buyer steps into the obligations of the target. 65 Fed. Reg. 82607, 82609 (Dec. 28, 2000); *see also* Standards for Privacy of Individually Identifiable Health Information 67 Fed. Reg. 53182 (Aug. 14, 2002) (to be codified at 45 C.F.R 164).

is not affected, because HIPAA applies both before and after the deal to the entities involved.

This continuity fallacy is worth revisiting. Other areas of law reject this equivalency, finding that a need remains for merger control to limit harms. For example, the same (incorrect) argument could be made in antitrust law. Before an acquisition, antitrust law bars a target from engaging in anticompetitive conduct, such as monopolization and collusion.[239] After an acquisition, it also bars the acquiror from engaging in such conduct.[240] Yet still Congress saw fit to implement merger review and control for certain large deals, and antitrust enforcers regularly challenge transactions that are likely to cause substantial harm to competition in the future.[241] Many other areas of law recognize that scrutiny of transactions is justified, regardless of the application of the law to the parties both before and after the deal, including securities law, corporate law, national security law, and industry-specific merger regulation in areas such as telecommunications and transportation, to name but a few.[242]

The transactional interventions across these areas of law reflect a positive form of legal opportunism. Corporate transactions create an opportunity for the law to intervene ex ante to stop harms that may be difficult to undo later, like harms to national security or competition. Privacy harms from transactions belong on this list. Once inflicted, privacy harms can be difficult or impossible to undo. There may be no erasing the effects once an identity is disclosed, an invasive ad is served, or data is aggregated in ways that reveal sensitive information to a new company after a deal. Further, courts have struggled to recognize privacy harms, which often arrive in the form of future risk of injury, and may lack the direct financial or physical impacts that are firmly established forms of harm in law.[243] Much of privacy law is applied after harms occur, despite these difficulties of remediation and proof. Corporate transactions offer a significant lever for privacy law

239. *See, e.g.*, Sherman Antitrust Act 15 U.S.C. §§ 1–2 (1890).

240. *Id.*

241. 15 U.S.C. § 18 (1996) (prohibiting the acquisition of "the whole or any part of the assets of another person engaged also in commerce or in any activity affecting commerce, where in any line of commerce or in any activity affecting commerce in any section of the country, the effect of such acquisition may be substantially to lessen competition, or to tend to create a monopoly").

242. *See* Sedona Conference, *supra* note 50 and accompanying text.

243. Citron & Solove, *supra* note 180, at 796 (observing that courts "refuse to recognize privacy harms that do not involve tangible financial or physical injury"); *id.* at 814 (observing the FTC's emphasis on financial and physical harms); *id.* at 816–19 (observing the features of privacy harms that often make them difficult for the law to recognize); *see also* Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361 (2014) (discussing the challenges of privacy harm recognition); Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 504–07 (2010).

to stop harms before they occur,[244] but that requires revisiting the assumptions in current law that continuity of application is adequate.

These interventions also recognize that continuity of application of the law is not enough if harms arise *from the transaction itself*. The application of the law before and after may not be adequate to protect against these types of transaction-caused impacts.

The nature and potential for such deal-driven harms seems particularly under-examined in privacy law, perhaps due to M&A exceptionalism in privacy law. Such harms might arise either from a lack of, or inadequate, consent to the deal, both of which are identified for several transactions in Part IV of this Article. Deal harms might also come in more novel forms, such as muddying the application of privacy rules, or harms from unexpected data aggregation.

California's recent amendments to its opt-out provisions in state privacy legislation offer a simple example of how mergers and acquisitions can muddy privacy rules and create the potential for deal-driven harms. California privacy law permits consumers to opt-out from sale or sharing of personal data.[245] As a result of a deal, the target and acquiror must reconcile their lists of individuals who have opted out from personal data sale or sharing. Some consumers may have opted out from the target but not the acquiror (perhaps because they have no prior relationship with the acquiror). Others may have filed an opt-out only with the acquiror but allowed the target to sell and share their data. Or, they may have opted out from both entities.[246] The law in California was unclear about which preference prevails, that of the target or the acquiror, demonstrating how transactions can muddy the application of privacy law rules. This also highlights the continuity fallacy at work: the application of the law pre-amendment both before and after the transaction was not enough to resolve this ambiguity. The deal might be used by the target to argue the opt-out choice was made with the target and does not apply to the acquiror, resulting in a decline in privacy protection.

In 2024, California updated its Consumer Privacy Act as applicable to the first situation, where a consumer opts out from the target but not the acquiror. The changes make clear that a business that obtains personal data through the acquisition of another business, whether through a merger, acquisition, bankruptcy, or other transaction, must honor any prior customer opt-out from sale or sharing of personal data.[247] In other words, the consumer's direction to the target business not to sell or

244. *See infra* Section IV.C (discussing the potential of transactional privacy law to ameliorate challenges in existing privacy law).

245. Cal. Civ. Code § 1798.120(a)(1) (West 2024).

246. Where no opt-out was filed with the target, this amendment would not apply; it requires honoring of opt-outs filed with the target.

247. Cal. Civ. Code § 1798.120(a)(2) (West 2024).

share such data survives the corporate transaction. The bill is cast as "rectifying an ambiguity" in the prior law about whether such opt-outs continue in force after an acquisition.[248] It prevents that acquiror from claiming the consumer opted-out only of the sale and sharing by the target, not by the combined entity.

The transaction itself could also create data aggregation harms not addressed by the continuous application of the law. By nature, data-driven M&A will often result in combinations of personal data that would not otherwise occur. This creates the potential for a type of privacy harm that has been described outside of the merger context as an "aggregation" harm.[249] Daniel Solove identifies the potential for the aggregation of data to cause dignitary harms, arising from the combination of the data in ways that unsettle individuals' expectations.[250] While one or two pieces of information may not, standing alone, be very informative about a person, the more data that is combined, the more detailed the picture can be drawn of that person. The combination of scattered bits of information can often be more than the sum of its parts, revealing new information about that individual which they did not expect would be known when they provided the discrete data sources.

This definition of aggregation harms did not expressly contemplate corporate transactions, but it applies well to the aggregation harm risks that can be created by personal data M&A.[251] The risk of aggregation harm arises because a corporate transaction changes the context in which personal data exists. The target company joins the acquiror's corporate family and brings the personal data it holds along with it, placing that personal data within a new ecosystem of other data already held by the acquiror. In fact, such data combinations drive the value and point of many of the deals examined here. Amazon wants to know what customers are buying from their marketplace, *and* what customers are buying from Whole Foods. Google wants to know what users are searching *and* users' health tracking information on Fitbit devices.

---

248. Cal. Assembly Comm. on Priv. and Consumer Prot., Hearing on AB 1824: California Consumer Privacy Act of 2018: opt-out right: mergers, Cal. State Assemb., 2023-2024 Reg. Sess., at 4. Ultimately, AB 1824 was passed.

249. Solove, *supra* note 138, at 506–07.

250. *Id.*

251. Aggregation harms are identified in the privacy scholarship, but not for mergers and acquisitions. Solove catalogues the recognition of aggregation harms in government data handling, and in the criminal context. Solove*, supra* note 138, at 505–06 (discussing government aggregation) and at 508–09 (discussing aggregation in criminal contexts). Notable cases about aggregation harms are criminal and Fourth Amendment related, far from the sorts of civil information privacy at issue in mergers and acquisitions. *See, e.g.*, Carpenter v. United States, 585 U.S. 296, 301 (2018) (taking into account the large quantity of data collected by cell phone tracking in evaluating the impact on privacy). The analysis in *Carpenter* implies recognition of aggregation harm and that the combination of data in large and detailed amounts over time, as in cell phone records, is distinct from more episodic collection in its effects on privacy.

This deal-driven change in corporate structure and control will often expand data access and use not only to the acquiror, but beyond that to the acquiror's corporate family. Most of the privacy policies examined for this Article include consent to the use and collection of data in various forms by "affiliates" of the target.[252] A merger or acquisition will often cause the companies included within the category of "affiliates" to expand.[253] As the corporate family grows larger, it increases the potential for wider access to personal data and aggregation, even without any change in the privacy policy terms. This can enable new connections and inferences to be drawn that were not possible pre-acquisition, with privacy impacts.

This data aggregation arising from M&A can have both costs and benefits for individuals' privacy. Aggregation may be positive. It could, for example, enable users to login once across multiple services for convenience, to combine their networks or data across services, or to benefit from cross-promotions among affiliates. After its purchase of Whole Foods, Amazon combined the companies' online purchasing functionality. There is now a single app that acts as a consumer portal for both goods purchases (via Amazon Marketplace) and grocery shopping (via Whole Foods).

Data aggregation also creates the risk of real privacy harm, by upsetting individuals' settled expectations about reasonable uses of their personal information.[254] Individuals dole out information in different contexts, with expected limits on what is known. They may give some data only to the acquiror, or only to the target, or some to both, and each with particular but distinct expectations around context and use. The merger or acquisition enables aggregation, upsetting these expectations by combining data "in new, potentially unanticipated ways to reveal facts about a person that are not readily known," and to a much greater extent than initially expected.[255]

In that sense, mergers and acquisitions can cause a "privacy lurch."[256] Scholar Paul Ohm coined this term to describe a sudden shift in privacy practices, in which a company departs from its usual practices and foists "new ground rules" on users.[257] He argues that such lurches upset long-settled expectations around data processing, causing

252. The only pre-acquisition policies that do not mention sharing with "affiliates" are those of WhatsApp and DoubleClick. *See, e.g.*, *infra* note 301.

253. Depending on the deal structure, the acquiror may become an affiliate of the target. The affiliates of the acquiror may also become affiliates of the target. This argument assumes, as is true for most of the deals examined in this Article, that there are no provisions in the privacy policy or law that otherwise limit data flow.

254. Solove, *supra* note 138, at 507.

255. *Id.*

256. Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 909 (2013).

257. *Id.*

privacy harms that are not well recognized in law.[258] In defining the concept of a lurch, Ohm emphasized privacy changes internal to a single company, such as the "pivots" often associated with new approaches or business models for existing companies infamous in Silicon Valley, including Google's collapse of its seventy different service privacy policies into one omnibus policy, or Facebook's slow march from a private to public network.[259]

But data-driven mergers and acquisitions fit well within the concept of a privacy lurch. These corporate deals can abruptly change data uses, context, and availability, unsettling individuals' expectations around data use that were formed when the companies existed separately. The Facebook/WhatsApp deal, where this Article began, is a paradigmatic example. Even if technically no privacy law violation occurred at the time of the deal, users objected to the corporate transaction because they had been sold a bill of goods on their data use that suddenly was no longer applicable.[260] Users had been promised and anticipated certain data practices in signing up for WhatsApp service, including the ability to send messages without monitoring or advertising. This lurched with the new Facebook ownership. Corporate ownership changes in data-driven services unsettle expectations in a way that users may find harmful.

Because this unsettling depends on expectations formed with the target, the risk of aggregation harms from a merger or acquisition can depend on factors specific to the transaction, such as the relationships of the individuals with the merging companies, and the data each company holds. Some individuals may have no prior relationship to the acquiror, meaning the deal expands access to their data to include the acquiror and its corporate family. The very fact of this broader disclosure that an individual has an account with a target could impact privacy. Consider disclosure of the existence of an account with BetterHelp for therapy, a subscription to an addiction treatment app, or an account with a religion-themed online dating service,[261] all of which may be sensitive information. When the acquiror finds out the account user information, this insight is disclosed.

Other individuals may have existing business relationships with both the target and the acquiror. This can reduce, but will not necessarily eliminate, the potential for aggregation harms. The data held by each company will almost always be different. Connecting the personal

---

258. *Id.* at 934–36 (discussing the challenges notice-and-choice models face in addressing privacy lurches).

259. *Id.* at 915–21.

260. *See* EPIC WhatsApp Complaint (2014), *supra* note 1.

261. *See, e.g.*, JDATE, https://www.jdate.com/ [https://perma.cc/9W69-AU44] ("[L]argest Jewish dating application"); SALT, https://www.be-salt.com/ [https://perma.cc/39QV-JSA3] ("Meeting . . . single Christians . . . who share your faith[.]"); MUZZ, https://muzz.com/us/en/ [https://perma.cc/FP2U-DDJW] ("Muslim dating and marriage app[.]").

data held by the target with that of the acquiror could enable much more granular information or inferences, and corresponding privacy harm.[262] Consider a user who buys a combination of strong immune support vitamins and minerals each week at Whole Foods. Standing alone that tells Whole Foods only that the customer is health conscious. Post-acquisition, Amazon could connect that grocery purchase to the purchase of a wig from Amazon's online marketplace. As Daniel Solove notes (outside the merger context), these buying patterns could, when put together, enable a strong inference that the individual is fighting cancer.[263] Or, perhaps an individual who once bought many sugary sweets has stopped doing so, swapping out low-sugar items in their weekly Whole Foods order. The same person has started making numerous footcare purchases on Amazon, and these data points are connected by virtue of the Amazon/Whole Foods acquisition. An inference might be drawn that the individual has diabetes. This new and sensitive health information might be susceptible to use for targeted drug advertising or even obtained by insurance companies.

These are simple examples of data aggregation. In the modern data economy, the potential for aggregation from a corporate deal expands exponentially, in ways that can be complex and difficult for individuals to predict. Powerful artificial intelligence can now be applied to those data troves in ways that make highly personal inferences more likely, and more extensive post-acquisition. Artificial intelligence-driven software tools are programmed to extract extraordinary amounts of data automatically, to sort and classify the data to look for patterns, to predict future behavior, and to make automated decisions, sometimes in real time.[264] Once a merger or acquisition allows access to personal data, these technological advancements can draw connections and

262. Depending on the data that the acquiror holds, this type of transaction could also lead to identification harms, in which digital profiles become connected to a particular human being in real life. Solove, *supra* note 138, at 511. While aggregation creates a more comprehensive digital identity, identification connects that identity to a real person offline. Imagine a transaction in which the target company holds only anonymized or pseudonymized user records, but the acquiror knows the true identities of users. Post-merger, the acquiror can combine the data to identify the real identities of the target users. This requires little imagination — it describes a risk in Facebook's acquisition of WhatsApp. WhatsApp identified its users only via phone numbers, with no requirement for true identities on user accounts. But Facebook requires the use of a real name for user profiles on its titular service, and often phone numbers for verification. After the deal, Facebook announced plans to link accounts that use the same phone number on WhatsApp, a move that sparked privacy objections. *See* EPIC WhatsApp Complaint (2014), *supra* note 1, at 8. All of the data related to those profiles then also becomes linked, from Facebook posts and messages to online tracking data.

263. This example is drawn from DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 28 (2011).

264. *See* NAT'L INSTIT. OF STANDARDS AND TECH. (NIST), ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) (Jan. 26, 2023), https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf [https://perma.cc/4ZGD-8VGB].

predictions,[265] enabling inferences about sensitive information like sexual orientation, religion, immigration status, substance use, and physical or mental illness.[266]

This discussion of muddying, aggregation harms, and a lack of consent to corporate transactions speaks to how mergers and acquisitions can place individuals in a different data position than they were in before the transaction. Because of the deal itself, their personal data is made more widely available to new corporate entities and may be connected with other data in ways that can reveal new and personal information. This may harm data privacy, even if privacy law applies both before and after the transaction. Privacy law seems to overlook this potential for deal-driven harm, instead assuming that the law's application both before and after a corporate transaction will provide adequate protection.

* * * * *

In sum, the reasons for excepting M&A from privacy legislation and enforcement are murky. The rationale has not been well-articulated, but is likely some combination of those above, relying on the presumed public benefits of mergers relative to individualistic privacy interests, the edification of corporate property interests, efficiency considerations, continuity fallacies, and assumptions of reasonable expectations of privacy.

None of these rationales should be immediately or entirely dismissed. But it is worth considering whether they stand up to scrutiny, and the weight any countervailing interests or benefits bear relative to privacy impacts at stake. As personal data acquisitions become more common, and as privacy interests grow weightier in the digital economy, these justifications may no longer support the near-wholesale exemptions of mergers and acquisitions from the ordinary scope of consent-based privacy protections. The exclusion of M&A from privacy law seems increasingly inconsistent with broader concerns that

---

265. Jennifer King & Caroline Meinhardt, *Rethinking Privacy in the AI Era*, STAN. INSTIT. FOR HUM.-CENTERED A.I., 1, 21 (Feb. 22, 2024).

266. Justin Sherman, *How Shady Companies Guess Your Religion, Sexual Orientation, and Mental Health*, SLATE (Apr. 26, 2023, at 12:55 ET), https://slate.com/technology/2023/04/data-broker-inference-privacy-legislation.html [https://perma.cc/MSY9-425R]; Sara Morrison, *This Outed Priest's Story is a Warning for Everyone About the Need for Data Privacy Laws*, VOX (July 21, 2021, at 19:20 ET), https://www.vox.com/recode/22587248/grindr-app-location-data-outed-priest-jeffrey-burrill-pillar-data-harvesting [https://perma.cc/6688-V26F]; Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy*, DUKE SANFORD SCH. OF PUB. POL'Y 1, 6 (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf [https://perma.cc/GRW6-QRQC] (describing the types of data collected and the risks to individuals).

animate modern privacy law and debates, and specific concerns over mass data selling in other contexts. It also seems to depend on assumptions that overlook the potential for deal-driven harms, and judgments about reasonable expectations of privacy that may no longer be defensible in modern privacy law.

IV. THE FACTS: THE PRIVACY IMPACTS OF HIGH-PROFILE PERSONAL DATA ACQUISITIONS

So far, this analysis demonstrates that M&A exceptionalism is not well-justified in legal theory. But that does not necessarily mean that privacy law ought to change. If harm from M&A to privacy is minimal or nonexistent, that is a compelling reason for the law to continue its M&A exceptionalism.

This Part begins to tackle this immense factual issue of whether and how personal data acquisitions are causing harm to data privacy. It does so by analyzing the likely privacy impacts of fifteen high-profile, personal data-driven acquisitions by massive technology firms. The targets each held or had access to a significant amount of individuals' personal data at the time of the acquisition.

This analysis uses the privacy policies of the target company, both before and after the deal, as a proxy for measuring changes in privacy protection. First, it evaluates whether there was adequate consent to the acquisition itself based on the terms of the target company's privacy policy in effect when the acquisition closed. Second, it considers the likely impact of the transaction on privacy protection by comparing the privacy policy in effect at closing to the first set of changes made to the policy terms after the acquisition.

The analysis indicates that transactional privacy harms are occurring, though it finds the privacy effects of the deals studied are likely mixed. The first part of the analysis concludes that several of the deals had missing or weak consent to the transaction itself, which likely resulted in privacy harms. The second part finds that in ten of the fifteen deals studied, the acquirors made changes to the target's privacy policy soon after the acquisition closed, often to the terms that govern the uses of personal data. Most of these changes were unilaterally imposed based on implied consent. Some of these post-acquisition changes were likely harmful to privacy, such as those that added new terms to permit the use of personal data for advertising. Others were likely beneficial to privacy, at least to some extent, because the changes increased the clarity of the disclosures on data processing, or expressed new intent to honor user settings that limit data processing. These mixed effects support a similar conclusion to the theoretical analysis above: that privacy law is overly blunt or general in assuming away harms from almost all mergers and acquisitions.

A. Study Methodology

The acquisitions examined in this Article are listed in Appendix A (the "Dataset").[267] The deals closed between 2006–2023. Each was selected because it involved an acquiror that was a large technology firm and a target that held a significant amount of, or access to, individuals' personal data. Further, several of these deals provoked objections from consumer privacy advocates, alleging likely future privacy harm, and others had characteristics similar to transactions that prompted such objections. These acquirors have drawn significant attention for both the rapid pace of their acquisitions[268] and their privacy misconduct.[269] These concerns have not previously been connected in the literature, but viewed together, make these companies a clear choice to assess the nexus of privacy effects and corporate transactions. It suggests that if privacy harm is occurring from acquisitions, it will be apparent in this set of deals.

The analysis is based on the privacy policies of the target company in each acquisition, which were used to evaluate the promised privacy protection both before and after the deal. These privacy policies are a logical starting place to investigate transactional privacy impacts, for several reasons. Due to M&A exceptionalism, these policies play an outsized role in transactional privacy protection as the main mechanisms used to obtain consent to M&A. The FTC's common law of privacy operates from the precept that companies must honor the privacy promises made in these policies, among other representations.[270] In that sense, a failure to adhere to privacy policy terms, or other unfair or deceptive acts related to such policies, are classic Section 5 FTC Act violations, and offer a key measurement of likely privacy harm. Such privacy quality can often be amorphous and difficult to measure, but

267. *See infra* Appendix A.

268. *See* FTC, Non-HSR Reported Acquisitions, *supra* note 46; *see also, e.g.*, Staff of Subcomm. on Antitrust, Com., and Admin L., 116th Cong., Investigation of Competition in Digital Markets: Majority Staff Rep. and Recommendations (2020); Ginger Zhe Jin et al., *supra* note 48 (finding that Alphabet/Google, Amazon, Apple, Facebook and Microsoft together completed a much higher number of tech acquisitions per firm than the other groups of top acquirors, though noting private equity firms are also highly acquisitive in data-heavy industries).

269. For example, both Facebook and Google have violated prior FTC orders related to their privacy practices. Press Release, FTC, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples [https://perma.cc/Z9SU-9WEZ]; Press Release, FTC, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook [https://perma.cc/WY5C-4Z46] (settling "charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information").

270. Solove & Hartzog, *supra* note 87.

these privacy policies, and changes to their terms, offer a concrete way to consider how acquisitions affect the quality of privacy protection. The terms in the privacy policy are also particularly susceptible to a speedy, detectable revision after a merger or acquisition.[271]

The analysis is carried out based on two privacy policies for each acquisition: the "pre-acquisition" policy, which is the policy in effect as close as possible in time to the transaction closing date,[272] and the "post-acquisition" policy, which is the first new policy version issued after the date the acquisition closed. In other words, the post-acquisition policy is the first policy change to occur under new ownership.

The privacy policies used in this analysis were collected from two sources. The first is the target company's online, archived privacy policies. These policies are often maintained separately from the acquiror's policy even post-acquisition. The second source, which was used when the policy was unavailable from the target itself, is the internet content archive the Wayback Machine. The Wayback Machine is a nonprofit internet archive that stores past internet sites in their digital form.[273] It preserves content that was once online but may no longer be available from the original website and so enabled the recovery of privacy policies that are no longer posted on the targets' websites.

To identify the "pre-acquisition" privacy policy, the study first determined the date on which the transaction closed. The analysis then worked backwards in time, using one or both of the sources above, to identify the target company's privacy policy that was in effect as close as possible in time, but prior to, the transaction closing date. Initially, the research assumption was that the acquiror would not have control over the target to modify such policy terms before the closing date. However, at least three policies were found to have changed just before the closing of a transaction, and the substance of the changes suggested the acquiror may have been involved in the change.[274] When a policy was changed within one month or less leading up to the transaction, this study attributed the change to the effect of the transaction, even if that change was technically prior to the deal closing. For deals with these near-in-time changes, the study went one version further back in time to identify the "pre-acquisition" policy, on the assumption that this prior policy would be more reflective of the terms that existed before the impacts of the acquisition.

Then, to identify the "post-acquisition" privacy policy, the study used one or both of the above sources to locate the next point in time

---

271. *See supra* Part III (identifying drivers of privacy policy change).

272. *But see infra* Section IV.C.2 (discussion of the small number of deals, notably Facebook/Instagram, in which a third policy was also considered based on an amendment made extremely near in time (less than a month) before the transaction closed).

273. The Wayback Machine is available at https://web.archive.org/.

274. *See infra* text accompanying notes 277–86 for a discussion of these policies.

after the acquisition closing when a new privacy policy was issued. In other words, the analysis determined the date of next change to the policy after the acquisition closed. This first-changed policy after closing is referred to as the "post-acquisition" policy in the analysis provided in this Article.

B. Missing and Weak Consent to the Acquisition Itself in Target Privacy Policies

Consent remains the touchstone of legality for much of U.S. privacy law.[275] When assessing the impact of a merger or acquisition on privacy, the clearest question in existing law is whether the individuals whose personal data was transferred or sold in that deal provided adequate consent to that data processing. When consent to the transaction was inadequate, the analysis here assumes the transaction likely resulted in privacy harm.

This Section evaluates this question of consent for the fifteen acquisitions in the Article's Dataset, based on the terms of the target's pre-acquisition privacy policy.[276] It finds that three of the transactions lacked any consent to the deal in the terms of the privacy policy. These transactions likely violated privacy law as it now exists, and in doing so, presumptively caused privacy harm. In the remaining twelve deals, the analysis finds there was a clause purporting to grant consent but argues that the form of that consent often failed to meet the FTC's legal standards.

1. Several Policies Lack Consent to the Acquisition

Three of the fifteen deals in the Dataset lacked basic consent to the acquisition itself in the target's privacy policy: Nest,[277] Onavo[278] and Instagram.[279] As explained above, it is common for companies to seek consent to future mergers and acquisitions by including a business continuity clause in their privacy policies, which often gives notice of potential future data processing in connection with a future merger or

---

275. *See supra* Section II.B (discussing the role of consent in privacy law when it applies to mergers and acquisitions).

276. Or near in time to closing as discussed in the next Section, when the acquiror seemed to have affected the terms pre-closing.

277. *10-08-2013 Privacy Statement — Archived*, NEST, https://nest.com/legal/privacy-statement/archive/?date=10-08-2013) [https://perma.cc/33FB-W8DH] [hereinafter Nest Pre-Acquisition Policy].

278. *Privacy Policy*, ONAVO (archived Aug. 12, 2013), https://web.archive.org/web/20130812125416/http:/www.onavo.com/privacy_policy [https://perma.cc/8Q2P-WPFV] [hereinafter Onavo Pre-Acquisition Policy].

279. *Privacy Policy*, INSTAGRAM (archived July 1, 2012), https://web.archive.org/web/20120701233809/http://instagram.com:80/about/legal/privacy/ [https://perma.cc/K5SD-QFDY] [hereinafter Instagram Pre-Acquisition Policy (July 2012)].

acquisition and obtains blanket consent to data processing, transfers and sales in those future deals.[280] The pre-acquisition policies for these three deals contained no such business continuity clauses at the time their acquisition was announced. Each of these targets was acquired in a significant transaction shortly after the date on which the pre-acquisition policies were examined for this Article: Nest was acquired by Google, and Onavo and Instagram were both acquired by Facebook.

These consent failures offer perhaps the clearest illustration of transactional privacy harms in this Article. This lack of any terms of consent means that the data processing in the acquisition would likely violate Section 5 of the FTC Act, unless some other consent to the transaction was obtained outside of the policy.

The deception branch of Section 5 bars misrepresentations, omissions, or other practices that are likely to materially mislead a consumer acting reasonably in the circumstances, to the consumer's detriment.[281] The lack of basic consent to these three transactions looks like a material omission from the privacy policy. The pre-acquisition policies from Nest and Instagram fail to advise of the potential for personal data to be transferred or sold in a corporate transaction, and all three policies failed to obtain consent to the collected personal data being transferred in such a deal.[282] Nor do these policies contain more general clauses that, while not specific to mergers or acquisitions, grant permission for data sales or transfers that could be stretched into consent to a corporate transaction.[283]

The circumstances of Instagram's acquisition and business continuity clause appear to be the most egregiously misleading, and unavoidable by consumers. At the time Facebook announced its acquisition of the company in April 2012, the Instagram privacy policy contained no business continuity clause at all.[284] As late as July 2012, there was still no such clause in the Instagram policy.[285] Then, a business continuity clause appeared in the privacy policy effective August 30, 2012,

---

280. *See supra* Section II.B.3 for a discussion of these clauses. When the law applies, transactional privacy protection depends on notice, consent and purpose continuity.

281. *See* FTC Policy Statement on Deception, *supra* note 89.

282. Oddly, the Onavo pre-acquisition policy expressly provides for *notice* of a potential merger or acquisition, but the terms fail to grant consent to any such sale, transfer, or use of data that might result from a corporate transaction. *See* Onavo Pre-Acquisition Policy, *supra* note 278.

283. *See* Onavo Pre-Acquisition Policy, *supra* note 278; Instagram Pre-Acquisition Policy, *supra* note 279; Nest Pre-Acquisition Policy, *supra* note 277.

284. *Privacy Policy*, INSTAGRAM (archived Apr. 30, 2012), https://web.archive.org/web/20120430092943/http://instagram.com/about/legal/privacy [perma.cc/C2RQ-MH9W].

285. Instagram Pre-Acquisition Policy (July 2012), *supra* note 279.

just a day before the transaction closed on August 31, 2012.[286] Given this abrupt timing, the Facebook/Instagram acquisition is categorized here as a transaction in which there was, in effect, no business continuity clause in the pre-acquisition policy. Although in very technical terms such a clause existed immediately before the deal occurred, the timing suggests it was added for the express purpose of enabling the deal. The personal data Instagram collected before the deal, up until immediately prior, was pursuant to a policy that did not seek consent to a merger or acquisition involving that information or even warn of that potential. These timing details for Instagram's policy modifications illustrate not only the omission of important information at the time of consent, but also the striking malleability of privacy protections that depend on company policies, which can be unilaterally and rapidly changed to grant permission to acquire personal data.[287]

These violations could also be framed as a misrepresentation, rather than an omission, under Section 5. All three policies adamantly promise that they will not sell the personal information collected to third parties without consent.[288] Instagram is particularly blunt and broad in its insistence that it "will not rent or sell potentially personally-identifying and personally-identifying information to anyone."[289] These express promises not to sell data are clear and simple. An individual reading such a clause in a privacy policy could reasonably expect that such terms mean what they say — that their personal data is not going to be sold, whether through M&A or other means. Where a policy says nothing further about M&A, as in these three acquisitions, it encourages a reasonable belief that these more general promises not to sell also apply to a corporate transaction. Had individuals instead been

---

286. Instagram, Inc. Privacy Policy "Snapshot", INSTAGRAM (archived Aug. 31, 2012), https://web.archive.org/web/20120831132207/http://instagram.com:80/about/legal/privacy/ [https://perma.cc/DB6L-ZB2M] [hereinafter Instagram Pre-Acquisition Policy (Aug. 2012)]. The parties announced on September 6, 2012, that the deal had closed, but Facebook's securities filing indicates the actual closing data as "August." Facebook, Inc., Quarterly Report (Form 10-Q) (Oct. 24, 2012). A media article similarly identifies the closing date as August 31. Jenna Wortham, *It's Official: Facebook Closes Its Acquisition of Instagram*, N. Y. TIMES (Sep. 6, 2012, at 11:50 ET), https://archive.nytimes.com/bits.blogs.nytimes.com/2012/09/06/its-official-facebook-closes-its-acquisition-of-instagram/ [https://perma.cc/5P3Y-ZC6C]. Either closing date reflects a change to the privacy policy immediately preceding the closing, either by one day or by one week.

287. *See infra* Section IV.C.1 (observing the prevalence of unilateral change clauses in the privacy policies examined by this Article).

288. Onavo Pre-Acquisition Policy, *supra* note 278 ("We do not share, sell, rent or lease your personal information or data to third parties, unless you provided us your explicit consent to do so or subject to this Policy."); Instagram Pre-Acquisition Policy (July 2012), *supra* note 279 ("Instagram will not rent or sell potentially personally-identifying and personally-identifying information to anyone."); Nest Pre-Acquisition Policy, *supra* note 277 ("Under no circumstance do we share Personally Identifiable Information for any commercial or marketing purpose unrelated to the delivery of Nest Products and services without asking you first. Period. We do not rent or sell our customer lists.").

289. Instagram Pre-Acquisition Policy (July 2012), *supra* note 279.

given the correct information that their data may be sold or transferred in a corporate deal, they may have chosen not to provide that data, or to provide less of it.

An acquiror in a corporate transaction might argue the transaction is not a sale or transfer of the "personal data" to a third party, but rather of the business itself. This is a distinction drawn in corporate and other areas of law, which identify the asset or share being sold with particularity, distinguishing between the sale of a corporate entity, or the data as an asset.[290]

A similar argument has provoked controversy in bankruptcy proceedings when personal data is being sold to a third party as an asset of the debtor corporation. There is significant disagreement over whether these general promises not to sell information to third parties should be read to prevent the sale of individuals' data in these bankruptcy transactions.[291] Some privacy ombuds, the individuals appointed during bankruptcy to oversee consumers' interests in the sale of personal data, contend that the purchaser of the business in bankruptcy is a successor-in-interest, who stands in the shoes of the debtor, and therefore is not a "third party" barred by the common terminology often used in these clauses.[292] Other ombuds view such language as ambiguous at best, and conclude that a bankruptcy sale violates a promise not to sell personal data to third parties.[293]

This bankruptcy distinction is less defensible from the perspective of transactional privacy effects. The difference between an asset sale, which gives ownership of the personal information, or a share sale that transfers corporate control over access to that personal information, does not seem determinative of the privacy effects of the transaction. The potential impact of the transaction on access to an individual's information may be the same, regardless of the specific form taken by the sale.[294] Further, when the specific promise is not to sell your data to "anyone," as in Instagram's pre-acquisition policy (rather than the more common promise not to sell to "third parties"), the bankruptcy logic of a successor-in-interest does not apply.

---

290. *See* Zolman Cavitch & David L. Hoehnen, *Buying or Selling a Corporate Business: Stocks or Assets*, 28 OHIO STATE L.J. 614, 623 (1967).

291. *See* Bradley, *supra* note 16, at 162–63 (noting such clauses as a "significant area of disagreement" and discussing the various perspectives).

292. *Id.* at 162. Privacy ombuds are appointed to oversee the sale of consumer data in bankruptcy proceedings. *See also id.* at 133–34 (explaining the role of privacy ombuds).

293. *Id.* at 163; *see also id.* at 161 (noting that provided the sale is to a "qualified buyer," transfers of personal data in a bankruptcy are often still permitted, even if the transfer violates the privacy policy).

294. *See supra* text accompanying notes 56–63 (arguing that the form of the corporate transaction is not necessarily determinative of its privacy effects). This leaves aside any privacy protections that might be adopted in a particular deal, such as data silos or other data segregation.

Finally, a Section 5 violation requires that the omission or misrepresentation be material. The FTC views a representation as material when it is "likely to affect a consumer's choice of or conduct regarding a product."[295] This is based on relevant Section 5 decisions, with further support from the *Restatement (Second) of Torts*, which defines materiality to include those omissions or representations which the reasonable person would view as important in deciding how to act.[296]

Based on this law, these representations on the sale of data were likely material for these deals. When an express claim is made that personal data will not be sold — as it was here — the FTC will often presume such claims to be material to consumer decision making.[297]

If framed instead as an omission of a business continuity clause, the FTC would also base the materiality assessment on whether the omission likely affected consumers' choices to use the products of Instagram, Onavo and Nest. This need not be true of every consumer, only a reasonable or average consumer.[298] The Instagram deal, and to a lesser extent the Nest deal, certainly sparked consumer objections over data privacy effects.[299] This suggests the related representations were material to consumer choice for some set of individuals. Had users known about a potential transaction selling their personal data, particularly to a company with a poor privacy track record like Facebook, it is quite possible they would have chosen not to share (or to share less) personal information with Instagram, Nest, or Onavo.

A caveat on the lack of consent to these acquisitions is that the norms around privacy policies have since evolved. The most recent policy in the Article Dataset that lacks a business continuity clause dates

---

295. FTC Policy Statement on Deception, *supra* note 89.

296. *Id*. at n.45 (citing Volkswagen Group of America, Inc., 99 F.T.C. 446 (1982); Restatement (Second) of Torts § 538 (Am. Law Inst. 1965)).

297. *Id.*

298. Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8351 (July 2, 1964) (referencing the "average consumer").

299. *See, e.g.*, Elec. Priv. Info. Ctr. (EPIC) & Ctr. for Digit. Democracy (CCD), WhatsApp, Inc., Supplemental Materials in Support of Pending Complaint, Request for Investigation and Injunction, and Other Relief; Related Commentary Concerning Commission's Surprising Expedition of Google-Nest Review ¶ 37 (Mar. 21, 2014), https://archive.epic.org/privacy/internet/ftc/whatsapp/WhatsApp-Nest-Supp.pdf [https://perma.cc/CVT4-53DQ] (arguing in a submission on a different acquisition that the "Commission clearly failed to address the significant privacy concerns presented in the Google acquisition of Nest"); Brian Fung, *Google Just Bought Nest for 3.2 Billion. What Happens to Nest's User Data?*, WASH. POST (Jan. 13, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/01/13/google-just-bought-nest-for-3-2-billion-what-happens-to-nests-user-data/ [https://perma.cc/8BFD-3MY4] (noting some objections to the deal on privacy grounds); Kevin Roose, *Why Did Google Just Buy a Thermostat Company?*, N.Y. MAG. (Jan. 13, 2014), https://nymag.com/intelligencer/2014/01/why-did-google-just-buy-a-thermostat-company.html [https://perma.cc/55WN-PKXH] (noting that as a result of the acquisition, "Google will eventually have an inroad not just into your phone, your computers, your commute (through self-driving cars), your finances (if you use Google Wallet), but your physical home").

to 2014, in Google's acquisition of Nest.[300] The twelve other policies in the Dataset — many of which are more recent — all include business continuity clauses that purport to grant consent for the target to transfer users' data to an acquiror.[301] Although the Dataset is small, this suggests the problem of missing business continuity may be more historical than current. Today, most privacy lawyers would include such a clause as standard in a privacy policy, as the more recent policies in this study reflect.

Although this specific problem of missing business continuity clauses may be historical, similar consent failures persist today. Companies continue to make broad promises that data will be kept private or not sold,[302] much like those that appeared in the policies of Nest, Onavo, and Instagram. For example, the FTC brought a 2023 case against BetterHelp, an online therapy company that expressly assured website visitors and users that their health information would "stay

300. Nest Pre-Acquisition Policy, *supra* note 277.

301. *Your Privacy Matters*, LINKEDIN (archived June 27, 2016), https://web.archive.org/web/20160627122603/https:/www.linkedin.com/legal/privacy-policy?trk=uno-reg-guest-home-privacy-policy [https://perma.cc/5GL7-32EC] [hereinafter LinkedIn Pre-Acquisition Policy]; *WhatsApp Legal Info*, WHATSAPP (archived July 28, 2014) https://web.archive.org/web/20140728222928/http:/www.whatsapp.com/legal/ [https://perma.cc/T4ZB-JCQQ] [hereinafter WhatsApp Pre-Acquisition Policy]; *Giphy Privacy Policy*, GIPHY (archived Apr. 15, 2020), https://web.archive.org/web/20200415114041/https:/support.giphy.com/hc/en-us/articles/360032872931-GIPHY-Privacy-Policy [https://perma.cc/2C38-3CBD] [hereinafter Giphy Pre-Acquisition Policy]; *Privacy*, DOUBLECLICK (archived Dec. 29, 2007) https://web.archive.org/web/20071229225755/http:/www.doubleclick.com/privacy/index.aspx [https://perma.cc/DVK9-4SA7] [hereinafter DoubleClick Pre-Acquisition Policy]; *YouTube Privacy Notice*, YOUTUBE (archived Apr. 10, 2006), https://web.archive.org/web/20060410003944/http:/youtube.com/t/privacy [https://perma.cc/NK6M-LN9S], [hereinafter YouTube Pre-Acquisition Policy]; *Waze —.Privacy Policy*, WAZE (archived May 22, 2013), https://web.archive.org/web/20130522010610/http://www.waze.com/legal/privacy/ [https://perma.cc/5ZZY-GS5Q] [hereinafter Waze Pre-Acquisition Policy (Nov. 2012)]; *Fitbit Privacy Policy*, FITBIT (archived Jan. 27, 2023), https://web.archive.org/web/20230127212741/https://www.fitbit.com/global/us/legal/previous-terms/privacy-policy-10082020 [https://perma.cc/5RHW-7EZ2] [hereinafter Fitbit Pre-Acquisition Policy]; *BrightBytes, Inc. Privacy Policies*, BRIGHTBYTES (archived Aug. 6, 2022), https://web.archive.org/web/20220806074913/https:/www.brightbytes.net/privacy-policy/ [https://perma.cc/UM5P-QDVB] [hereinafter BrightBytes Pre-Acquisition Policy]; *Shazam Terms and Conditions*, SHAZAM (archived Aug. 5, 2018), https://web.archive.org/web/20180805061211/https://www.shazam.com/terms#pp3. [https://perma.cc/2ED3-LE83] [hereinafter Shazam Pre-Acquisition Policy]; *1Life Healthcare, Inc. Privacy Policy*, ONE MEDICAL (archived Dec. 21, 2022), https://web.archive.org/web/20221221173919/https:/www.One Medical.com/privacy/ [https://perma.cc/JE72-AHFS] [hereinafter One Medical Pre-Acquisition Policy (Nov. 2022)]; *Privacy Policy*, WHOLE FOODS MARKET (archived Aug. 15, 2017), https://web.archive.org/web/20170815061416/http:/www.wholefoodsmarket.com/privacy-policy [https://perma.cc/9ZWW-LQVC] [hereinafter Whole Foods Pre-Acquisition Policy]; *Privacy Policy*, TWITCH (archived Aug. 15, 2014), https://web.archive.org/web/20140815063253/http://www.twitch.tv/www.twitch.tv/user/legal?page=privacy_policy [https://perma.cc/5EZV-5TZA] [hereinafter Twitch Pre-Acquisition Policy].

302. *See* Waldman, *supra* note 146, at 45, 75.

private between [them] and [their] counselor."[303] Despite these promises, the company shared granular data about individuals' behavioral therapy with Facebook and other firms for advertising and other purposes.[304] While not an acquisition, the promise is similar to those made in the privacy policies examined here. These elegant and general promises not to sell data may also predominate in the minds of consumers, crowding out attention to more specific terms on consent to M&A.

In sum, these consent failures are classic and clear illustrations of the potential for mergers and acquisitions to cause privacy harm. Even high-profile acquisitions like Google/Nest, Facebook/Onavo, and Facebook/Instagram (depending on the policy date) were completed without the most basic consent of the data subjects to the deal and with promises the data would not be sold.[305] These consent failures cast doubt on the M&A exceptionalism that permeates privacy law, suggesting harms from material omissions or misrepresentations can easily be found in major transactions, and highlighting a need for closer privacy scrutiny of corporate deals.

2. Several Policies Rely on Weak Consent to the Transaction

In assessing consent, modern privacy law considers not just whether consent was technically or formally extracted from individuals, but whether that consent was adequate in law.[306] The twelve remaining policies considered in this Article did contain a business continuity clause purporting to grant consent to a merger or acquisition.[307] However, many of these clauses fail to meet the FTC's requirements for adequate consent, which require that it be "specific" and "informed."[308]

Each of the twelve business continuity clauses provided notice in highly general terms that lack sufficient context to be adequate. None provide any information about the potential identity of buyers, or even their likely industry. Nor do any mention which data will be transferred in the deal — presumably all of that permitted to be collected in the policy — or any potential ability to opt out of such a transfer.[309]

---

303. Complaint ¶ 25, BetterHelp, Inc., *supra* note 19.

304. *Id.* at 5, 10, 11–12.

305. Nest Pre-Acquisition Policy, *supra* note 277; *compare* Instagram Pre-Acquisition Policy (July 2012), *supra* note 279, *with* Instagram Pre-Acquisition Policy (Aug. 2012), *supra* note 286.

306. *See supra* Section II.B for a discussion of conceptions of adequate consent.

307. *See supra* note 301 (pre-acquisition policies for various companies, excluding Fitbit, which mentions notice, but not consent).

308. *See supra* Section II.B for a discussion of the FTC standard for adequate consent.

309. For example, the Whole Foods Pre-Acquisition clause states, "[W]e may share Personal Information/Personal Data about you . . . [i]n connection with, or during negotiations of, any proposed or actual merger, purchase, sale (including a liquidation, realization,

This level of generality in business continuity clauses is understandable from the target's perspective. At the time the privacy policy is drafted, a corporation does not know and may not be able to predict whether acquirors will become interested in buying it, much less who those acquirors might be. Its goal is to provide generalized notice and obtain consent to any and all possible future M&A, to allow maximum freedom for the company to deal in the personal data.

This generality may come at the cost of adequate notice specificity and meaningful consent. It is easy to imagine that the individuals whose data is at stake would not have provided it if the notice was more specific. Factors such as the identity of the acquiror, their industry, and the type of data being transferred could all prove material to the willingness to grant consent to a corporate transaction or type of transaction. The identity of the acquiror, and its past privacy misconduct,[310] drove the privacy outcry in acquisitions like Facebook/WhatsApp and Google/Fitbit, and to a lesser extent, Google's acquisition of DoubleClick.[311] Imagine that in that transaction, instead of Google the proposed buyer was DuckDuckGo, which operates a competing browser to Google's Chrome, but stakes its reputation and corporate identity on browser privacy protection.[312] This hypothetical change in buyer may have made a material difference to the willingness of individuals to consent to the transfer of their data in the transaction. Given the identity of the acquiror, fewer individuals are likely to consent willingly to the acquisition of their personal data by a large technology company with

---

foreclosure or repossession), lease, amalgamation or any other type of acquisition of all or any portion of Whole Foods Market assets, financing, disposal, conveyance or transfer of all or a portion of our business to another company." Whole Foods Pre-Acquisition Policy, *supra* note 301. The LinkedIn Pre-Acquisition clause states, "[i]f there is a change in control or sale of all or part of LinkedIn, we may share your information with a third party, who will have the right to use that information in line with this Privacy Policy . . . We may also disclose your personal information to a third party as part of a sale of the assets of LinkedIn Corporation, a subsidiary, or division, or as the result of a change in control of the company or one of its affiliates, or in preparation for any of these events. Any third party to which we transfer or sell our assets will have the right to continue to use the personal and other information that you provide to us in the manner set out in this Privacy Policy." LinkedIn Pre-Acquisition Policy, *supra* note 301.

310. *See* Marc Rotenberg & Caitriona Fitzgerald, Written Statement for the Elec. Priv. Info. Ctr. (EPIC), *Online Platforms and Market Power, Part 4: Perspectives of the Antitrust Agencies*, 116th Cong., H. Comm. on the Judiciary, Subcomm. on Antitrust, Com., and Admin. L., (2019) (written statement of Marc Rotenberg, President, EPIC and Caitriona Fitzgerald, Policy Director, EPIC), https://epic.org/wp-content/uploads/testimony/congress/EPIC-HJC-AntitrustAgencies-Nov2019.pdf [https://perma.cc/23SU-VHS3] (describing broken privacy commitments after Facebook's acquisition of WhatsApp and warning of privacy concerns regarding Google's pending acquisition of Fitbit).

311. Ryan Singel, *Google Seals DoubleClick Deal, Learns More About You — Update*, WIRED (Mar. 11, 2008, at 10:22 ET), https://www.wired.com/2008/03/google-seals-do/ [https://perma.cc/4RGN-V63K].

312. *Your Personal Data Should be Nobody's Business*, DUCKDUCKGO, https://duckduckgo.com/about [https://perma.cc/26R8-EZZU].

a history of privacy violations than to an acquisition by a buyer with a stronger privacy reputation.

The industry of the acquiror may also be material to the willingness of consumers to allow their data to transfer from the target. Consider Amazon's acquisition of Whole Foods, one of the deals examined in this Article. Consumers might reasonably envision that their data would flow to another grocery store chain, or even a food producer who acquires Whole Foods in a horizontal or vertical merger. The acquisition of Whole Foods by the technology and e-commerce giant, Amazon, though, is wholly less within their realm of predictability or expectation. Particular types of data may also be more sensitive to disclosure outside of the target's industry. Consumers might expect or reasonably anticipate that Fitbit would be acquired by another health or health tracking company. It is less likely they would anticipate the acquisition by Google, a search company, which actually occurred. The acquiror industry may materially influence willingness to consent.

Despite this potential significance of acquiror identity, industry, and data type on the willingness to consent, none are specified in the business continuity clauses examined here. Consent is granted to any and all acquisitions and acquirors. There is room for debate over how specific notice must be for adequate consent to a transaction, but the less information that is provided, the less likely the consent is to be legally sufficient. Specifying the identity of the acquiror may be beyond what the law requires. But it is clear that these business continuity clauses provide highly general notice, and use it to solicit broad consent to all M&A, in ways that are neither very specific nor informed.

C. Changes to Policy Terms Post-Acquisition: Mixed Effects on Privacy

Post-acquisition policy changes are another important source of potential privacy impacts from mergers and acquisitions. These changes can unsettle individuals' expectations around personal data processing, particularly when the acquiror unilaterally imposes the policy change based on weak consent. This Section examines the protections afforded against such post-acquisition changes in the fifteen Dataset privacy policies, when and how target policies were modified after the acquisitions, and the likely privacy impacts of those changes.

1. Privacy Policies Offer Weak Protection: Unilateral Changes with Inadequate Consent

In evaluating transactional privacy impacts, the continuity of the target's privacy policy is important. Although such continuity will not obviate transactional harms discussed above, like a lack of consent, or

data aggregation and muddying, policy continuity can serve to limit the unsettling of individuals' expectations around data use. If the target's policy terms remain in effect after the transaction, that ought to reduce the privacy harms arising from the transaction by keeping data practices consistent.

This Section argues that in the Dataset deals, the targets' privacy policies tend to offer weak assurances of such policy continuity. Every policy permits unilateral changes, in reliance on implied consent that is not compliant with modern FTC standards. These feeble assurances of policy continuity create the risk of transactional privacy harms, by enabling the acquiror to make unexpected changes in data use post-acquisition.

Eight of the pre-acquisition target policies examined here made no promises of the continued application of the privacy policy after a corporate transaction.[313] The seven other policies in the Dataset make promises of their own continuity that vary in strength.[314] Four of those seven policies expressly provide for the continued application of the target's pre-acquisition privacy policy *after* a corporate transaction.[315] The other three provide for some degree of protection post-acquisition less than the continued application of the privacy policy comprising:[316]

(1) A promise to take "reasonable steps" to ensure the information is used consistently with the policy in effect when it was collected,[317]

(2) A promise to "take measures to protect the confidentiality,"[318] and

313. WhatsApp Pre-Acquisition Policy, *supra* note 301; Shazam Pre-Acquisition Policy, *supra* note 301; YouTube Pre-Acquisition Policy, *supra* note 301; Twitch Pre-Acquisition Policy, *supra* note 301; Whole Foods Pre-Acquisition Policy, *supra* note 301; Onavo Pre-Acquisition Policy, *supra* note 278; Instagram Pre-Acquisition Policy (Aug. 2012), *supra* note 286; Nest Pre-Acquisition Policy, *supra* note 277. This lack of provision on policy continuity in the event of a merger or acquisition is unsurprising for Onavo, Nest and Instagram, given that the pre-acquisition policies did not contain a business continuity clause that contemplated the eventuality of a merger or acquisition.

314. *See infra* notes 315–16.

315. Waze Pre-Acquisition Policy (Nov. 2012), *supra* note 301; One Medical Pre-Acquisition Policy (Nov. 2022), *supra* note 301; Giphy Pre-Acquisition Policy, *supra* note 301; LinkedIn Pre-Acquisition Policy, *supra* note 301.

316. DoubleClick Pre-Acquisition Policy, *supra* note 301; Fitbit Pre-Acquisition Policy, *supra* note 301; BrightBytes Pre-Acquisition Policy, *supra* note 301 (granting consent to transfer to a buyer agreeing to data privacy standards "no less stringent than our own").

317. DoubleClick Pre-Acquisition Policy, *supra* note 301 (providing in the case of a merger, DoubleClick will "take reasonable steps to assure that such information is used in a manner consistent with the DoubleClick privacy policy under which it was collected").

318. Fitbit Pre-Acquisition Policy, *supra* note 301 (providing in the event of a merger, Fitbit "will continue to take measures to protect the confidentiality of personal information and give affected users notice before transferring any personal information to a new entity").

(3) Limiting consent to a transfer to buyers who agree to data privacy standards "no less stringent than our own."[319]

Even when these promises of policy continuity exist, they offer weak transactional privacy protection for several reasons. First, all but one of the fifteen target policies allowed the company to make unilateral changes to the policy terms, both before and after the acquisitions.[320] The authoring company is free to modify its terms at any time. These sort of unilateral modification provisions have become ubiquitous in the terms for digital services, and so are likely to appear in the terms of targets in future deals.[321] The lone policy not to address such changes at all was Nest's pre-acquisition policy, which was silent on the potential for the company to modify it.[322] Post-acquisition, Google added a term to Nest's policy to acknowledge the potential for unilateral changes.[323]

These unilateral change clauses mean the continuity of the policy was never guaranteed by the target even before the deal. That same power and ability to modify the terms unilaterally is passed on to the acquiror. Any promise of policy continuity is just a promise that the policy could change at any time, and so not a meaningful commitment to the privacy promises made by the target.

While these policies do provide for a form of consent to such unilateral changes, it often does not meet the FTC's standard of affirmative and express consent.[324] Recall that the FTC has articulated the position that, to comply with Section 5 of the FTC Act, an acquiror must use personal data gathered pre-acquisition in a manner materially consistent with the consent provided before the transaction.[325] Beyond such uses, the acquiror must obtain consent that is affirmative and express.[326]

---

319. BrightBytes Pre-Acquisition Policy, *supra* note 301 (granting consent to transfer to a buyer agreeing to data privacy standards "no less stringent than our own").

320. *See infra* Appendix A. In some of the policies this power was express, and in others it was necessarily implied by the wording regarding notice of changes.

321. Haley, *supra* note 16, at 100–01 (finding initially that all of the terms of service of the 122 top uniquely-owned websites include a unilateral modification provision initially, but later noting DuckDuckGo does not). This study looked primarily at the broader terms of service on websites, not privacy policies specifically.

322. *See* Nest Pre-Acquisition Policy, *supra* note 277.

323. *09-18-2014 Privacy Statement — Archived*, NEST, https://nest.com/legal/privacy-statement/archive/?date=09-18-2014 [https://perma.cc/967Y-CEE7] [hereinafter Nest Post-Acquisition Policy] ("Please note that this privacy statement may change from time to time. We will provide notice of any changes on the website or by contacting you.").

324. *See, e.g.*, Decision and Order, X-Mode Social, Inc., *supra* note 137; Decision and Order, BetterHelp *supra* note 213 (defining the requirement for "affirmative express consent" as the "unambiguous indication of an individual consumer's wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a [c]lear and [c]onspicuous disclosure to the individual").

325. FTC Letter Re Facebook/WhatsApp, *supra* note 2.

326. *Id.*

Eleven of the fifteen policies examined here indicate that the continued use of the services constitutes consent to *any* policy changes.[327] Merely continuing to use a service after a change in policy constitutes implied consent at best, and is neither affirmative nor express. Affirmative consent requires some action to demonstrate agreement after disclosure of the changed terms, as the FTC has recently articulated.[328] Continued use is an action that is express, but that action may be untethered to any cognizance of the policy change or any intent to acquiesce to it. Express and affirmative consent would, for example, include

---

327. This was true for all eleven policies before and after the acquisitions, with the exception of Shazam's, which provided for continued use as consent before the acquisition but, in the post-acquisition policy, is silent on what constitutes consent to changes. *See* Waze Pre-Acquisition Policy (Nov. 2012), *supra* note 301; *Waze — Privacy Policy*, WAZE (archived Mar. 7, 2014), https://web.archive.org/web/20140307165449/https:/www.waze.com/legal/privacy/ [https://perma.cc/R26W-S87Z] [hereinafter Waze Post-Acquisition Policy]; Whole Foods Pre-Acquisition Policy, *supra* note 301; *New Privacy Notice*, WHOLE FOODS MARKET (archived Aug. 16, 2018), https://web.archive.org/web/20180816181743/https:/www.wholefoodsmarket.com/privacy-notice [https://perma.cc/RLD4-8Z83] [hereinafter Whole Foods Post-Acquisition Policy]; Twitch Pre-Acquisition Policy, *supra* note 301; *Privacy Policy*, TWITCH (archived Oct. 12, 2014), https://web.archive.org/web/20141012152716/http://www.twitch.tv/www.twitch.tv/user/legal?page=privacy_policy [https://perma.cc/3S2X-J5X8] [hereinafter Twitch Post-Acquisition Policy]; One Medical Pre-Acquisition Policy (Nov. 2022), *supra* note 301; *1Life Healthcare, Inc. Privacy Policy*, ONE MEDICAL, (archived Nov. 1, 2023), https://web.archive.org/web/20231101233255/https:/www.One Medical.com/privacy/ [https://perma.cc/DE2X-2E2U] [hereinafter One Medical Post-Acquisition Policy]; BrightBytes Pre-Acquisition Policy, *supra* note 301; *BrightBytes Privacy Policy*, BRIGHTBYTES (archived Mar. 24, 2023), https://web.archive.org/web/20230324070702/https:/www.brightbytes.net/privacy-policy [https://perma.cc/U5Z2-2TWF] [hereinafter BrightBytes Post-Acquisition Policy]; Fitbit Pre-Acquisition Policy, *supra* note 301; *Fitbit Privacy Policy*, FITBIT (archived Dec. 13, 2023) https://web.archive.org/web/20231213122329/https://www.fitbit.com/global/us/legal/previous-terms/privacy-policy-09162022 [https://perma.cc/5T4Y-N9KQ] [hereinafter Fitbit Post-Acquisition Policy]; LinkedIn Pre-Acquisition Policy, *supra* note 301; *Privacy Policy,* LINKEDIN (archived July 31, 2017), https://web.archive.org/web/20170731225528/https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv [https://perma.cc/HNG2-HHE3] [hereinafter LinkedIn Post-Acquisition Policy]; Giphy Pre-Acquisition Policy, *supra* note 301; *Giphy Privacy Policy*, GIPHY (archived Sep. 25, 2020) https://web.archive.org/web/20200925120248/https://support.giphy.com/hc/en-us/articles/360032872931-GIPHY-Privacy-Policy [https://perma.cc/E3EG-GAZM] [hereinafter Giphy Post-Acquisition Policy]; Instagram Pre-Acquisition Policy (July 2012), *supra* note 279; Privacy Policy, INSTAGRAM (archived Feb. 2, 2013), https://web.archive.org/web/20130202113040/http://instagram.com/about/legal/privacy/ [https://perma.cc/Y97X-7GS6] [hereinafter Instagram Post-Acquisition Policy]; WhatsApp Pre-Acquisition Policy, *supra* note 301; *Privacy Notice,* WHATSAPP, https://www.whatsapp.com/legal/privacy-policy/revisions/20120707 [https://perma.cc/T94T-2XVG] [hereinafter WhatsApp Post-Acquisition Policy]; Shazam Pre-Acquisition Policy, *supra* note 301; *Privacy Policy*, APPLE (archived Nov. 1, 2018), https://web.archive.org/web/20181101173552mp_/https:/www.apple.com/legal/privacy/en-ww/ [https://perma.cc/B6GB-GM6F] [hereinafter Shazam Post-Acquisition Policy] (providing that "Apple may update its Privacy Policy from time to time" but not specifying what constitutes consent to such changes).

328. *See supra* note 324 and accompanying text.

opting in by clicking a button or checking a box to acknowledge the policy amendments, or some other action much less ambiguous and implied than simply continuing to use a service whose terms have changed.[329]

Three further policies are simply silent about what constitutes consent to changes to their terms: Onavo, Nest and DoubleClick.[330] This leaves it unclear what consent standards will be applied to changes to the policy and makes it difficult to assess the adequacy of such consent based on the policy terms.

The final remaining policy — YouTube's post-acquisition policy — provides for express consent to changes to its terms. The policy indicates that "[w]e will not reduce your rights under this Privacy Policy without your explicit consent, and we expect most such changes will be minor."[331] Further, the post-acquisition policy adds that "[i]f we propose to use personal information for any purposes other than those described in this Privacy Policy and/or in the specific service privacy notices, *we will offer you an effective way to opt out of the use of personal information* for those other purposes."[332] This promise goes beyond what is required by the FTC; it extends not only to material changes but to changes for "any" purposes. These terms were a post-acquisition improvement. YouTube's pre-acquisition policy, like most of the others examined here, provided that continued use was consent.[333]

A small number of the policies examined here include other terms that serve to limit the scope of this power to unilaterally amend, and these limits should be understood alongside that power. The Giphy and One Medical policies permitted unilateral changes, both before and after their acquisition.[334] However, these policies also expressly preserve the application of the version of the policy in effect at the time the

---

329. *See, e.g.*, Solove, *supra* note 129, at 599 (contrasting the express and affirmative action such as opt-in required for consent under GDPR with the common U.S. approach of implied consent through continuing to do business with the organization).

330. Onavo Pre-Acquisition Policy, *supra* note 278; Nest Pre-Acquisition Policy, *supra* note 277; DoubleClick Pre-Acquisition Policy, *supra* note 301; Nest Post-Acquisition Policy, *supra* note 323; *Privacy Policy*, ONAVO (archived Oct. 21, 2014), https://web.archive.org/web/20141021044924/http:/www.onavo.com/privacy_policy [https://perma.cc/8SZM-WW9X] [hereinafter Onavo Post-Acquisition Policy]; *Privacy*, DOUBLECLICK (archived Aug. 27, 2008), https://web.archive.org/web/20080827211656/http://www.doubleclick.com/privacy/index.aspx [https://perma.cc/YGJ4-2B5W] [hereinafter DoubleClick Post-Acquisition Policy].

331. *Google Privacy Notice,* GOOGLE (last modified Aug. 7, 2008), https://policies.google.com/privacy/archive/20080807 [https://perma.cc/DYE9-EZAU] [hereinafter YouTube Post-Acquisition Policy].

332. *Id.* (emphasis added).

333. YouTube Pre-Acquisition Policy, *supra* note 301.

334. Giphy Pre-Acquisition Policy, *supra* note 301; Giphy Post-Acquisition Policy, *supra* note 327; One Medical Pre-Acquisition Policy, *supra* note 301; One Medical Post-Acquisition Policy, *supra* note 327.

personal data was collected.[335] The effect of these clauses is to limit the breadth of unilateral changes by ensuring they are only prospective, not retroactive.[336] This better protects data privacy in the case of post-acquisition changes to the policy terms.

Three other post-merger policies provide for advance notice of changes: Waze, One Medical and Twitch.[337] The Twitch policy promises it will make reasonable efforts to afford users a "choice" regarding those changes, but only if required by law.[338] Such notice makes the continued use more meaningful as a form of implied consent, because in theory, the notice gives users the opportunity to protect their privacy by discontinuing the use of the services and deleting their data (if possible) before the new policy terms take effect.

Finally, even if more robust promises of policy continuity were made in all of these policies, those promises could mean little after a merger or acquisition. While the FTC has warned that promises must be kept for material matters post-acquisition, this has not been enforced. Once acquired, the target who wrote the policy will often cede control over how the data is treated to the acquiror. This change in control, and its effect on the ability to protect user data, is reflected and more honestly described in several clauses of these policies that address bankruptcy. There, the target disclaims the ability to control data transfers in bankruptcy proceedings.[339] Both a bankruptcy and an acquisition can result in similar loss of the target's control over user data. Yet the promise of continued policy application is often made for one (M&A) and disclaimed for the other (bankruptcy). It would be fairer and more accurate to explain that after a merger or acquisition, the target itself may no longer control the policy's content or how user data is processed. Only one policy, that of One Medical, accurately reflects this dilemma. It warns honestly that data collected after an acquisition may be subject to "a new privacy policy adopted by the successor entity," though it also bifurcates, preserving the application of the policy

335. *Id.*

336. The FTC has brought enforcement action under Section 5 (though not in the M&A context) against retroactive policy changes, which are thought to harm privacy. *See supra* note 98.

337. *See* Waze Post-Acquisition Policy, *supra* note 327; One Medical Post-Acquisition Policy, *supra* note 327; Twitch Post-Acquisition Policy, *supra* note 327. For these three specific provisions, there were no material changes from the pre-acquisition policies.

338. Twitch Post-Acquisition Policy, *supra* note 327.

339. *See, e.g.*, WhatsApp Pre-Acquisition Policy, *supra* note 301 (disclaiming the ability "to control how your personal information is treated, transferred, or used" in the "event of our bankruptcy, insolvency, reorganization, receivership, or assignment for the benefit of creditors, or the application of laws or equitable principles affecting creditors' rights generally").

to user information collected before an acquisition,[340] which may not be enforceable.

In sum, the privacy policies at the time of these acquisitions offered weak protection. As a result, acquirors were fairly unconstrained in their power to make post-deal changes to those policies, with almost all having the unilateral power to make amendments premised on weak consent. The malleable promises made in these policies offer a poor substitute for legal oversight of the potential privacy effects of the transactions.

2. Acquirors Are Making Post-Acquisition Policy Changes

Acquirors do in fact use their post-acquisition powers to unilaterally change the privacy policies. Ten of the policies examined here changed from a moderate to significant degree in their terms post-acquisition.[341] Of the ten policies that were so revised, all but one was issued within nine months of the transaction closing.[342] The fastest of these changes occurred just over two months from the transaction closing.[343] Some of these policies were actually changed just days *prior* to the deal to provide for consent to carry out the transaction.[344] The remaining five policies were not changed in a significant way in the quality or quantity of the revisions, though a new policy was issued.[345]

---

340. The One Medical Pre-Acquisition Policy (Nov. 2022), *supra* note 301 (providing, in reference to corporate transactions, "the use and disclosure of all transferred user information will be subject to this Policy. Any information you submit or that is collected after a transfer, however, will be subject to a new privacy policy adopted by the successor entity").

341. *See* BrightBytes Post-Acquisition Policy, *supra* note 327; Nest Post-Acquisition Policy, *supra* note 330; Instagram Post-Acquisition Policy, *supra* note 327; LinkedIn Post-Acquisition Policy, *supra* note 327; Onavo Post-Acquisition Policy, *supra* note 330; One Medical Post-Acquisition Policy, *supra* note 327; Shazam Post-Acquisition Policy, *supra* note 327; Waze Post-Acquisition Policy, *supra* note 327; *WhatsApp Privacy Policy,* WHATSAPP, https://www.whatsapp.com/legal/privacy-policy/revisions/20160825 [https://perma.cc/J5GK-SCX5] [hereinafter WhatsApp Post-Acquisition Policy]; YouTube Post-Acquisition Policy, *supra* note 331.

342. *See* BrightBytes Post-Acquisition Policy, *supra* note 327; Nest Post-Acquisition Policy, *supra* note 330; Instagram Post-Acquisition Policy, *supra* note 327; LinkedIn Post-Acquisition Policy, *supra* note 327; Onavo Post-Acquisition Policy, *supra* note 330; One Medical Post-Acquisition Policy, *supra* note 327; Shazam Post-Acquisition Policy, *supra* note 327; Waze Post-Acquisition Policy, *supra* note 327; YouTube Post-Acquisition Policy, *supra* note 331. The exception to the nine-month observation is the WhatsApp Post-Acquisition Policy, which was issued 689 days after the transaction.

343. *See* Onavo Post-Acquisition Policy, *supra* note 330 (issued sixty-seven days from the merger closing date).

344. *See supra* Section IV.B.1 (discussing how several of the examined policies lack consent to the acquisition itself).

345. *See* Fitbit Post-Acquisition Policy, *supra* note 327; Twitch Post-Acquisition Policy, *supra* note 327; Giphy Post-Acquisition Policy, *supra* note 327; DoubleClick Post-Acquisition Policy, *supra* note 330; Whole Foods Post-Acquisition Policy, *supra* note 327. For two of these companies, Whole Foods and DoubleClick, the acquisitions were the evident cause

This analysis considers the likely effects of these changes on privacy and finds them to be mixed. Some of the revisions reduced the protectiveness of the policy and likely harmed privacy, by expanding the uses of data without adequate consent. Others were likely privacy-positive — meaning increasing the protectiveness of the policy terms — by improving disclosure and strengthening willingness to honor user settings.

Important prefatory context here is that certain pre-merger policies, such as those of Twitch, LinkedIn and Whole Foods, already allowed extremely broad data processing.[346] When a policy already permits extensive data processing, there is little room left for M&A to erode those already-limited protections.

a. Post-Acquisition Policy Changes that Harm Privacy: Materially Inconsistent Use Clauses

Of the fifteen policies reviewed for this Article, 40% made material changes specific to the terms governing the use of personal information after the acquisition.[347] The most glaring changes were three post-acquisition revisions that added new uses of data for advertising. Read alongside other terms, at least two of these use changes likely give rise to privacy harms, upsetting settled expectations around the purposes of data use with inadequate consent.

Facebook made policy changes to permit uses of personal data for advertising after three of its acquisitions: WhatsApp, Instagram, and Onavo.[348] The pre-acquisition policy for WhatsApp promised the opposite, that data would not be used for ads: "WhatsApp is currently ad-free and we hope to keep it that way forever. We have no intention to introduce advertisement into the product, but if we ever do, will update this section."[349] It granted permission for the use of personally identifiable information only to perform, improve or maintain WhatsApp's

---

of the revisions, but the substance of the changes were technical in nature and unlikely to have much effect on the level of privacy protection. The post-acquisition changes to the policies simply updated the entity and contact information to reflect the transaction, with no substantive changes to the terms of privacy protection afforded by the policy.

346. *See* Twitch Pre-Acquisition Policy, *supra* note 301; LinkedIn Pre-Acquisition Policy, *supra* note 301; Whole Foods Pre-Acquisition Policy, *supra* note 301.

347. Onavo Post-Acquisition Policy, *supra* note 330; WhatsApp Post-Acquisition Policy, *supra* note 341; Instagram Post-Acquisition Policy, *supra* note 327 (privacy-negative); LinkedIn Post-Acquisition Policy, *supra* note 327 (mixed); Shazam Post-Acquisition Policy, *supra* note 327; BrightBytes Post-Acquisition Policy, *supra* note 327 (privacy-positive). The remaining nine did not change the use provisions in a material way, meaning the use provisions were substantively similar or the same in their scope after the first post-acquisition policy change.

348. *Compare* WhatsApp Post-Acquisition Policy, *supra* note 341 *and* Instagram Post-Acquisition Policy, *supra* note 327 *and* Onavo Post-Acquisition Policy, *supra* note 330, *with* WhatsApp Pre-Acquisition Policy, *supra* note 301 *and* Instagram Pre-Acquisition Policy (July 2012), *supra* note 279 *and* Onavo Pre-Acquisition Policy, *supra* note 278.

349. WhatsApp Pre-Acquisition Policy, *supra* note 301.

services, and selling or sharing with third parties for "commercial or marketing" use with consent and opt-in.[350] After the deal, the policy was changed to permit Facebook and its family of companies to use information from WhatsApp to show "relevant offers and ads," and for third parties to send commercial messages.[351] Facebook revised the Onavo policy with similar changes to permit advertising, but the policy continued to expressly preserve the application for existing users and data.[352] This likely limited privacy harms.

Facebook also made post-acquisition changes to the Instagram policy that permit new uses of personal data for advertising, but in more nuanced ways. Before the deal, the policy contemplated use of data only to provide Instagram services, to protect rights and property, when required by law, and for service delivery and improvement functions.[353] The only mention of advertising was to permit placement of third-party cookies, to which the policy disclaimed any application.[354] Post-acquisition, the policy adds a new clause that permits Instagram to use information to "provide personalized content and information . . . which could include online ads or other forms of marketing."[355] It also adds that Instagram is now permitted to share "certain information," that it collects with third parties for the purpose of "deliver[ing] targeted

350. *Id.* ("The Way WhatsApp Uses Information," providing for the use of personal information to "operate, maintain, and provide to you the features and functionality of the WhatsApp Site and WhatsApp Service" and "to improve the quality and design of the WhatsApp Site and WhatsApp Service and to create new features, promotions, functionality, and services by storing, tracking, and analyzing user preferences and trends . . . . [w]e do not use your mobile phone number or other Personally Identifiable Information to send commercial or marketing messages without your consent or except as part of a specific program or feature for which you will have the ability to opt-in or opt-out.").

351. WhatsApp Post-Acquisition Policy, *supra* note 341 ("Facebook and the other companies in the Facebook family also may use information from us to improve your experiences within their services such as making product suggestions (for example, of friends or connections, or of interesting content) and showing relevant offers and ads.").

352. *Compare* Onavo Pre-Acquisition Policy, *supra* note 278 (permitting the "[u]se of Information," to provide services, develop new services, enforce terms, comply with laws, and allowing "Cookies and other trackers" to be used to facilitate services, customizing personal experience, and statistical and informational security), *with* Onavo Post-Acquisition Policy, *supra* note 330 ("Use of Information," adding additional permission "to support advertising and related activities," and adding to "Cookies and Similar Technologies" their use to "support advertising and related activities").

353. Instagram Pre-Acquisition Policy (July 2012), *supra* note 279. While unclear, the clause titled "Protection of Certain Personally-Identifying Information" seems to grant permission for several categories of use: delivering services, communications on new product features and updates, support request publication, where legally required and to protect property or rights).

354. *Id.* ("Ads appearing on any of our websites may be delivered to users by advertising partners, who may set cookies . . . . This information allows ad networks to, among other things, deliver targeted advertisements that they believe will be of most interest to you. This Privacy Policy covers the use of cookies by Instagram and does not cover the use of cookies by any advertisers.").

355. Instagram Post-Acquisition Policy, *supra* note 327.

advertisements,"[356] thereby contemplating Instagram sharing the information it collects with others for ads, rather than just allowing third-party cookies on the service.

These changes to the Instagram and WhatsApp policies likely harmed privacy by expanding to materially inconsistent data uses with inadequate consent. As described above, privacy law fundamentally relies on purpose specification, requiring the reason(s) why data is being collected to be disclosed to individuals at the time of collection. This serves as a bound to the consent provided and a limit on such use. The FTC bars uses of personal data post-transaction that are "materially inconsistent" with promises made at the time of collection, unless consent is obtained.[357] The post-acquisition purposes of use must, in other words, be materially consistent with those before the deal, or consent must be obtained for those that are not.

The new advertising uses in the Instagram and WhatsApp policies appear materially inconsistent with the original purposes specified at the time of collection. These policies allowed initial uses that were predominantly the target's own, involving the delivery and improvement of services, and some other uses like property, rights protection and legal process for Instagram.[358] None of the uses were advertising-related (except possibly WhatsApp's opt-in to selling data for marketing). Neither of the services offered advertising at the time of the acquisition. The new, added use of advertising looks materially inconsistent with these initially specified purposes. In fact, WhatsApp specifically disclaimed the use of advertising. The FTC's warning to WhatsApp/Facebook singled out ad-related use promises, implying that changes to expand advertising uses — precisely those made here — are material.[359] While not all different uses are necessarily incompatible, this use meets several of the factors that contribute to incompatibility.[360] First, there is little link between the original purposes of use for online messaging or social media and the new purpose of advertising.[361] Second, the ad-related change was likely outside of the individuals'

356. *Id.* ("Sharing of Your Information," permitting the sharing of "cookie data with third party advertising partners"). Cookies are small text files stored on your computer or other device that are used to track online activity, among other potential functions.

357. FTC Letter Re Facebook/WhatsApp, *supra* note 2.

358. *See* discussion *supra* notes 349–50.

359. FTC Letter Re Facebook/WhatsApp, *supra* note 2 ("WhatsApp's privacy policy clearly states, among other things, that users' information will not be used for advertising purposes or sold to a third party for commercial or marketing use without the users' consent. Facebook's purchase of WhatsApp would not nullify these promises and WhatsApp and Facebook would continue to be bound by them.").

360. *See* Opinion 03/2013 on Purpose Limitation, *supra* note 145, at 23–27 (describing key factors in assessing whether the original and new uses are compatible).

361. *Id.* at 24 ("[T]he *greater* the distance between the purposes of collection and the purposes of further processing, the more problematic this would be for the compatibility assessment [between the new use and the original purpose].").

reasonable expectations at the time they agreed to use these services of social media (Instagram, which at the time had no advertising) and instant messaging (WhatsApp), particularly given WhatsApp's no-ad promises. The nature of the data shared in the delivery or tracking of ads can be quite granular, such as IP addresses or locations, which contributes to the discontinuity between the original purposes for product use and the new use for ads. Finally, this unilateral policy change to expand use to include advertising was likely premised on the inadequate consent discussed above, itself provided for in the policies.

These acquisition-driven use changes for ads likely caused harm to privacy. The addition of a materially inconsistent use based on weak consent upsets settled expectations around the terms of personal data formed upon collection. Those expectations are important to control and consent; had individuals known their personal information would be used for advertising, they may not have given out their information at all, or may have provided less information. As Daniel Solove explains, these harms of use beyond the specified purposes are often dignitary in nature, "emerging from denying people control over the future use of their data, which can be used in ways that have significant effects on their lives."[362] Without the acquisition, this unsettling of expectations around advertising and the subsequent intrusion from the advertising itself would not have occurred, or perhaps would not have occurred so soon.

b. Post-Acquisition Policy Changes that Improve Privacy

Among the policy changes examined for this Article, some improved privacy protectiveness. These improvements were of two main types: clearer disclosure on data processing, or stronger expressed intent to honor settings or opt-outs that limit data use.

Both are likely to benefit individual user privacy. Since existing privacy law relies so heavily on notice and consent, clearer notice about data processing should make it easier for individuals to understand the terms to which they are agreeing, and to make better informed choices consistent with their privacy preferences. Honoring user opt-outs or settings is also likely to improve privacy by making it more likely the preferences individuals express about their data use will be effectuated by the company.[363]

In the Dataset, two policies — Shazam and BrightBytes — were revised to delete clauses that had disclaimed any obligations to honor

362. Solove, *supra* note 138, at 520.

363. This assumes the company follows its privacy policy. If not, that is a separate potential Section 5 FTC Act violation.

"do not track" settings.[364] In other words, the post-acquisition policy reflected a greater willingness to comply with users' expressed preferences not to be tracked. While modest, this change makes the policies somewhat more privacy protective post-merger. This change is likely a function not only of the acquisition, but also of changes in the law, which has made it increasingly clear that companies must honor "do not track" settings.[365]

For Shazam, the changes were wider reaching; Apple began to apply its own policy to the company after acquiring it. This had the privacy-beneficial result of effectively removing two other substantive clauses from Shazam's privacy policy: one that enabled monitoring of traffic referred to partner apps and services, and another that allowed Shazam to monitor the usage of its own services through third-party measurement companies, with user consent.[366] These changes reduce the permissions granted for monitoring by third-party companies, and so make the post-acquisition policy somewhat more privacy-protective.

Finally, LinkedIn's post-acquisition policy made several changes that likely had mixed effects on privacy. This policy was complex and dense in its language, both before and after the acquisition.[367] This made a direct comparison and evaluation of likely effects more difficult than for the more straightforward policies in the Dataset. Overall, LinkedIn's post-acquisition policy covers much of the same, very widely drawn terms of use in the pre-acquisition policy, but presents the disclosure in terms that are more streamlined and organized in the language and inclusions.[368] The descriptions of data processing also became more fulsome. For example, the post-acquisition policy added a new section that simply makes clear to users how the titular service works, explaining what connecting on LinkedIn means for data access,

---

364. *Compare* BrightBytes Pre-Acquisition Policy, *supra* note 301 *and* Shazam Pre-Acquisition Policy, *supra* note 301, *with* BrightBytes Post-Acquisition Policy, *supra* note 327 *and* Shazam Post-Acquisition Policy, *supra* note 327. For BrightBytes, this policy applies to data from the BrightBytes website only, not data used/collected through their services which is subject to a separate student data policy.

365. *See* CAL. CIV. CODE § 1798.120(d) (2024) (requiring an acquiror to comply with pre-acquisition opt-out selections); 4 COLO. CODE REGS. 904-3-6.11(B) (2023) (similarly requiring an acquiror to recognize consumers' previous opt-out selections); *see also* California v. Sephora USA, Inc., Case No. CGC-22-601380 (Cal. Sup. Ct. Aug. 24, 2022), https://oag.ca.gov/system/les/attachments/press-docs/FiledJudgment.pdf [https://perma.cc/4HEK-ZBVS] (settling charges that Sephora failed to honor opt-out requests from users as required by § 1798.120 of the CCPA).

366. *Compare* Shazam Pre-Acquisition Policy, *supra* note 301, *with* Shazam Post-Acquisition Policy, *supra* note 327 (deleting from "How We Use Your Information" two permitted uses: "(iv) to determine when you link from our app to one of our partner apps or services, so that we can monitor the level of traffic that we generate for our partner apps or services," and "(ix) to enable us to use a third party to measure the usage of our services by our users, with your consent or where otherwise permitted by applicable law").

367. LinkedIn Post-Acquisition Policy, *supra* note 327.

368. *Compare* LinkedIn Pre-Acquisition Policy, *supra* note 301, *with* LinkedIn Post-Acquisition Policy, *supra* note 327.

and how data is used by LinkedIn to suggest connections.[369] The change does not seem to reflect any actual shift in how data was being used, but this explanation was missing from the policy before the deal. Another example is the disclosure around third-party data access via application programming interfaces ("APIs"). LinkedIn's pre-acquisition policy referred opaquely to "negotiated agreements and our API and Plugin" terms as setting the parameters of such third-party data access for users.[370] Without those agreement terms, it is not clear what this means, or what type of data access it includes. Post-acquisition, the equivalent clause states more plainly that "[y]ou may link your account with others' services . . . . When you opt to link your account with other services, personal data will become available to them."[371] Overall, these changes move the policy toward clearer disclosure and with it, better privacy protection. The plain language descriptions of how the service works, and what happens when users link to third-party services enable individuals to better understand what they are consenting to, and to make more informed choices about whether to do so.

However, LinkedIn's post-acquisition policy also adds consent to certain new uses that seem privacy-eroding. First, it adds consent to allow LinkedIn bots to scan otherwise private messages sent via the service, for the purposes of enabling "productivity" tools.[372] Second, the post-acquisition policy allows new notifications to be sent to a user's network about their online activity; this was not included in the pre-acquisition policy.[373] The privacy impact of these changes may, however, be mitigated because consent is framed as subject to users' settings.[374] Finally, LinkedIn's post-acquisition policy adds that employers can now see how LinkedIn services are used by employees who are provided with LinkedIn services to carry out their work, such as recruiters.[375] While this evaluation is primarily focused on users as consumers, this change seems likely to reduce workplace privacy for employees.

---

369. LinkedIn Post-Acquisition Policy, *supra* note 327 ("2.1 Stay Connected").

370. LinkedIn Pre-Acquisition Policy, *supra* note 301 ("2.7 Third Parties Using LinkedIn Platform Services").

371. LinkedIn Post-Acquisition Policy, *supra* note 327 ("3.3 Others' Services").

372. *Id.* (providing in "2.1 Productivity" that "[s]ubject to your settings, we scan messages to provide 'bots' or similar tools that facilitate tasks such as scheduling meetings, draft responses, summarize messages or recommend next steps").

373. *Id.* (providing in "Stay Informed" that "[w]e use your content, activity and other data, including your name and picture, to provide notices to your network and others. For example, subject to your settings, we may notify others that you have updated your profile, posted a blog, took a social action, made new connections or were mentioned in the news").

374. *Id.*

375. *Id.* (providing in "3.1 Enterprise Accounts" that "[y]our employer may offer you access to our enterprise Services . . . . They can also buy access for you to our online learning products. Your employer can review and manage your use of such enterprise Services").

3. Summing Up: Acquisitions Are Privacy-Relevant

This analysis of fifteen personal data acquisitions suggests that such deals can drive privacy policy changes. Several of the policies in this Dataset were modified in substantial ways, soon after the acquisition occurred. It also indicates that those changes have variable impacts on privacy that can be more harmful than privacy law tends to assume. The modifications made after an acquisition were often based on implied consent. Some of the changes likely harmed privacy by expanding the permitted uses of data in material ways, such as adding uses for advertising purposes. Others likely improved privacy protection in modest ways, with clearer disclosure and stronger intent to honor user settings.

This analysis is at once both modest and useful. First, the fifteen acquisitions in the Dataset were selected for their likely privacy impacts, with each involving a large technology acquiror buying a target with significant personal data stores. Many of these acquirors have drawn attention for alleged or actual privacy misconduct.[376] This suggests that the Dataset offers a test case of the acquisitions most likely to give rise to privacy impacts. It also means the Dataset is slanted toward transactions that are perhaps the most likely to cause privacy harm. The research does not assess the proportion of all acquisitions, or even all technology acquisitions, that may have negative (or positive) privacy effects, which would be useful future research.

Second, the analysis relies on privacy policies, and changes to them, because those policies serve as the main mechanisms used to obtain consent to M&A in the absence of much enforcement.[377] For the reasons discussed in the introduction to the analysis, these privacy policies are a logical point at which to begin evaluating the effects of mergers and acquisitions on data privacy. However, the privacy policies examined here are one factor among many that determine the likely privacy impacts of corporate transactions, such as the actual (rather than written) data practices of the acquiror after the transaction, commitments outside of the policy, consumer behavior in using particular services and settings, and the design of online services and privacy settings, which this Article does not examine. Given these bounds of the Article's study, further research pathways to continue to build this understanding of transactional privacy harms are proposed below.[378]

Finally, this examination of policy revisions has so far assumed that the fact of the acquisition is relevant to these policy changes. An

376. *See supra* note 269.

377. Continuity promises could also be made at the time of the transaction in *fora* other than the policy itself, such as press releases or other public representations — this analysis focuses on the policies.

378. *See* Section V.B.

alternative view is that the acquisition is not germane; that if a policy revision violates privacy law, it violates privacy law regardless of any prior deal that took place. For example, Facebook's amendments to permit advertising, discussed above, may have occurred because of the acquisition but still likely violate privacy law, regardless of the deal. This seems to be the position of the FTC when it warns companies that a failure to honor privacy policies could (later) violate Section 5, even though the FTC does not intervene at the time of the transaction.

This view perpetuates M&A exceptionalism, and the missed potential of transactional privacy law. Assuming away the privacy impacts of mergers and acquisitions overlooks the insights and potential for privacy protection that can come from scrutiny of these deals. The reality is that mergers and acquisitions are privacy-relevant because they are often the driver of privacy policy changes. The timing and substance of the revisions of several policies in this study often leads to an unavoidable conclusion that there is a causal connection between the policy revision and the acquisition.

First, the timing of these policy revisions was quite speedy. Ten of the policies examined changed within nine months of the deal closing, some less than two months after, and some just days before closing to add a clause permitting the deal.[379] While not dispositive, the close timing of these revisions and the acquisition suggests that the transaction was an important factor driving the change.

Second, the substance of several of the policy changes also suggests an unavoidable inference that the transaction drove those revisions, in whole or in significant part. Post-acquisition, both Apple and Google began to apply their own privacy policy wholesale to the targets each had acquired, in place of the target's own pre-deal policy.[380] Google is well-known for this practice of collapsing its acquisitions' privacy policies into its own, and did so when it acquired YouTube in the deal examined here.[381] The causal relationship looks clear — this sort of wholesale replacement of one company's policy with that of another company would not occur absent an acquisition. In other deals, the substance of the change strongly supports an assumption that the acquisition provoked the policy revision. Facebook expanded the use of personal data for advertising after several of its acquisitions.[382] Pre-acquisition, the targets did not permit advertising. The substance of these changes leads to an almost inevitable conclusion that their cause

379. *See supra* text accompanying notes 342–46.

380. *See* YouTube Post-Acquisition Policy, *supra* note 331 (adding to a moderate revision made to YouTube's own policy, which also applied); Shazam Post-Acquisition Policy, *supra* note 327.

381. EPIC & CCD, WhatsApp, *supra* note 299.

382. *See* Instagram Post-Acquisition Policy, *supra* note 327; Onavo Post-Acquisition Policy, *supra* note 330; WhatsApp Post-Acquisition Policy, *supra* note 341.

was the acquisition by Facebook, a company that is driven by ad-revenue. While not foolproof, these factors of timing and substance are highly revealing and strongly suggest that the effects of the acquisition on privacy should not be ignored.

Of course, other factors, like changes in the law, management, or other non-deal considerations could also explain changes to a privacy policy. This appeared to be the explanation for the policy changes in three of the acquisitions studied: Fitbit, Twitch and Giphy.[383] This inference is also based on the substance of the changes. For example, Giphy added disclosure on California state rights in a change made to its policy shortly after that law came into effect, suggesting an inference that the change in law drove the policy revision.[384] Finally, it may also be that the causal factors are mixed. This appears to be the case with Google's purchase of BrightBytes. Some of the policy changes relate to the acquisition, while others appear driven by the passage of new state privacy laws.[385] M&A may not be the only reason for a policy change, but they can often be an important one. For this reason, data-driven deals are worthy of privacy attention.

By ignoring the role of mergers and acquisitions in policy changes, privacy analysis may miss important insights. Viewed more broadly, the analysis here suggests that the identity of the acquiror can be quite influential in the privacy effects of a transaction. The nature of the post-acquisition term modifications varies quite a bit based on the acquiror. Acquisitions by Facebook, an ad-driven firm, often led to revisions of the target's policy to permit the use of personal data for advertising. When a firm like Apple, which markets itself as more privacy-protective, acquires a firm, the changes to the target's policy improve privacy protections.[386]

This acquiror identity observation has implications in defining adequate consent. Nothing about the acquiror identity is disclosed in any

---

383. *See* Fitbit Post-Acquisition Policy, *supra* note 327; Twitch Post-Acquisition Policy, *supra* note 327; Giphy Post-Acquisition Policy, *supra* note 327.

384. *See* Giphy Post-Acquisition Policy, *supra* note 327.

385. BrightBytes' pre-acquisition policy was dated to 2017 and contained no disclosures specific to any state. *See* BrightBytes Pre-Acquisition Policy, *supra* note 301. After the company was acquired by Google in 2022, the policy was updated to include references to new state privacy laws in California and Virginia. *See* BrightBytes Post-Acquisition Policy, *supra* note 327. However, there were also other, significant changes in the substance of the BrightBytes policy that did not seem directly traceable to changes in state law and related to other terms of data processing discussed below.

386. *See Privacy*, APPLE, https://www.apple.com/in/privacy/ [https://perma.cc/QN9N-DTS6] ("Privacy is a fundamental human right. At Apple, it's also one of our core values . . . . We design Apple products to protect your privacy and give you control over your information."); Gary Drenik, *Apple's Fight to Protect Privacy Has Shaken Up Digital Advertising. Here's How Marketers Can Thrive in a Cookie-Less World, From An Expert*, FORBES (Jan. 11, 2023, at 10:00 ET), https://www.forbes.com/sites/garydrenik/2023/01/11/apples-fight-to-protect-privacy-has-shaken-up-digital-advertising-heres-how-marketers-can-thrive-in-a-cookie-less-world-from-an-expert/ [https://perma.cc/NC79-EQCP].

of the privacy policies studied here, which purport to obtain consent to data processing in all M&A.[387] More specific consent to the deal was not sought by the target once that acquiror's identity became known. This suggests a potential intervention for transactions with likely privacy impacts: require knowing and express consent from data subjects once the acquiror is identified.

Lastly, and perhaps most importantly, ignoring how transactions impact our privacy misses the great potential of transactional analysis to address broader problems in privacy law, by moving from ex post enforcement to certain ex ante privacy protection. This potential is discussed below.[388]

V. THE FIX: IMPROVE DETECTION OF PRIVACY RISK IN DEALS, EXPAND RESEARCH ON TRANSACTIONAL PRIVACY HARMS, AND PURSUE EX ANTE INTERVENTION

Viewed as a whole, this analysis points to a need for stronger and more contextual application of privacy law to personal data mergers and acquisitions. It shows that existing law is scant in its application to these deals, and that this M&A exceptionalism is difficult to justify theoretically at its current scope. It also shows this exceptionalism is questionable on the facts. A close examination of just fifteen high-profile personal data acquisitions turns up numerous examples of privacy erosion, and even privacy law violations. The privacy effects of these transactions are more mixed than is suggested by their lenient legal treatment.

This analysis permits two related conclusions: (1) that negative and real privacy effects are being overlooked in current privacy law, but also that they are not certain to occur in every deal, and, therefore, (2) that it is worth further inquiry on a wider scale, to scrutinize and understand the scope and nature of transactional privacy harm. This Section looks ahead to paths for achieving this. It proposes the first screening criteria for enforcers to detect transactions that create privacy risks. Then it outlines paths for future research to better understand transactional privacy harms. Finally, it highlights why such efforts are decidedly worthwhile — transactional privacy law has great potential to ameliorate problems in broader privacy law, by moving from ex post to certain ex ante protection.

---

387. *See supra* Section IV.B.2 (highlighting that none of the policies discussed the identity of potential acquirors).

388. *See infra* Section V.C.

A. Proposed Screening Criteria for Agency Detection of Transactional Privacy Risks

This Article does not seek to provide a final answer on the appropriate approach to mergers and acquisitions in privacy law, but rather to spark closer scrutiny of M&A exceptionalism and the need for change. In reconsidering the M&A exceptionalism that characterizes existing law, an important preliminary point is that data transfers or sales in M&A would not be *prohibited* if existing privacy legislation applied.[389] Rather, these transactions would become subject to the notice and consent requirements that privacy statutes require for data sales, disclosures and transfers in contexts other than M&A. Countervailing interests, like those discussed in Part III of this Article, could be edified, and privacy protected, at the cost of some efficiency and administrative ease through requirements to obtain consent to carry out the deal.

Right now, it is clear that transactional privacy harms exist, but their scope is not yet well-studied or well-defined. Given this stage of understanding, the most appropriate and readily available tool to address such harms is likely FTC enforcement of Section 5 of the FTC Act. In the immediate term, the FTC could apply its Section 5 authority to more closely scrutinize mergers and acquisitions that risk harm to privacy. This would require no legislative amendment. Section 5 of the FTC Act is written to encompass "likely" harm from unfair and deceptive practices.[390] This suggests it can be applied to harm likely to arise in future from corporate transactions, though congressional clarification of this power would still be helpful, as discussed below.

Achieving such FTC enforcement does, however, require a different type of change in enforcement practices. Right now, the FTC is either not detecting or not prioritizing harm from M&A in privacy enforcement. It is only fair to acknowledge that the FTC's resource constraints are real — the Bureau of Consumer Protection has a surprisingly sparse staff and budget relative to the scope of its privacy mandate.[391] But enforcement against M&A privacy harms is increasingly worthy of FTC attention. Personal data M&A have become more common, involve more personal data than ever before, and have the potential for greater impacts on privacy of a larger number of individuals. Many are beyond the reach of sectoral law. Enforcement in this

389. Except in those deals where sectoral laws apply to prevent transfers because there is inadequate consent.

390. 15 U.S.C. § 45(a)(4)(A)(i) (2023).

391. *See* Testimony of Chair Lina M. Khan Before the Subcomm. on Innovation, Data, and Com. of the H. Comm. on Energy and Com., 118th Cong. (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/chair-khan-testimony_7-9-2024.pdf [https://perma.cc/C3PE-H478] (referring to the agency as a whole, reporting that staffing levels are fewer than in 1980, but still account for 70% of its operating budget).

space offers an effective way for the agency to limit large-scale privacy invasions that consumers themselves have little power to prevent. It also presents a unique opportunity to stop incipient harm that is likely to occur, but may later be difficult to prove in court.

The FTC is well-positioned to identify privacy-harming deals because of its dual competition and privacy mandates. The agency already receives Hart-Scott-Rodino ("HSR") Act filings pursuant to its antitrust authority, meaning it is notified of large transactions across the economy. The HSR Act requires filing with antitrust authorities for transactions that meet certain thresholds, to enable agency review for potential harm to competition.[392] The FTC is also aware of smaller transactions, from its studies (using its other statutory powers), which recently identified more than 800 corporate deals by large technology companies.[393] The agency may require more detail to fully assess the privacy, rather than competition, impacts of transactions. Still, the FTC is made systematically aware of many transactions that are occurring across the economy, and the agency has also long engaged in privacy enforcement.[394]

The analysis in this Article suggests that to enforce effectively, the FTC may need better mechanisms to detect *which* mergers and acquisitions merit privacy intervention. The FTC recognizes that privacy policies are binding even after an acquisition occurs. It sets a fairly high bar for consent to post-transaction changes — express and affirmative consent.[395] Yet, there have not been FTC cases involving post-deal policy violations. Taken together, this looks like a detection problem, at least in part.

To aid in this detection of transactional privacy harm, this Article proposes the first set of criteria for enforcers to assess the likely privacy risks of mergers and acquisitions. These factors are meant to assist the FTC and other agencies in identifying mergers that merit privacy scrutiny under existing law. These criteria are borrowed, with several modifications, from factors developed by privacy ombudspersons, who are appointed to oversee the sales of personal data in bankruptcy

---

392. Section 7A of the Clayton Act, 15 U.S.C. § 18a (2023), added by the Hart-Scott-Rodino Act of 1976, Pub. L. 94-435, 90 Stat. 1283, provides that the parties to covered mergers or acquisitions must notify the FTC and the Department of Justice before consummating the proposed transaction, and imposes a waiting period. Whether a particular acquisition is subject to the Section 7A requirements depends upon the value of the acquisition and the size of the parties, as measured by their sales and assets, and subject to certain specific exceptions.

393. FTC, NON-HSR REPORTED ACQUISITIONS, *supra* note 46 (stating that the FTC sought information and documents from Alphabet Inc., Amazon.com, Inc., Apple Inc., Facebook, Inc., and Microsoft Corp. on the terms, scope, structure, and purpose of transactions that each company consummated between January 1, 2010 and December 31, 2019 for which the company did not file a Hart Scott Rodino Act merger notification form).

394. Also, the FTC's privacy and merger review are carried out by separate Bureaus within the agency.

395. FTC Letter Re Facebook/WhatsApp, *supra* note 2.

proceedings.[396] Bankruptcy law is one of few areas of non-sectoral legislation that addresses the privacy impacts of buying and selling personal data in corporate transactions. As such, it offers helpful context to define the privacy-relevant characteristics of deals, many of which are useful in the more general context of M&A.

In assessing the privacy risk posed by a merger or acquisition, important considerations include:

(1) What type and amount of personal data does the target plan to transfer to the acquiror (or grant access to)? This may include an evaluation of the characteristics of the data (for example, does it include financial, health, child-related, biometric or other sensitive data?), the number of individuals whose data is being sold, and known characteristics that might render those consumers more privacy-vulnerable, as informed by privacy law.

(2) Is the acquiror in the same industry or line of business in whole or in part as the target? If so, this may suggest shared industry norms around data use, that similar laws on privacy apply to both companies, and that future uses of data may be similar, though none of this is guaranteed. If the industries of the target and acquiror are different, the risk of privacy impacts from the acquisition may be correspondingly increased or decreased by the transaction.

(3) Do sectoral privacy laws govern the transaction, or certain personal data within the transaction? If so, this may diminish the privacy concerns, but see the discussion of the continuity fallacy, above.[397] If no sectoral laws apply, then the privacy policy, other company representations (within and prior to the deal), and any FTC enforcement will dictate the privacy protections post-acquisition.

(4) Were the individual data subjects of the target company notified of the transaction? If so, was the notice provided easily accessible and clear?

(5) Will the individuals whose personal data is at stake in the transaction be afforded the opportunity to opt-out of the transfer of their data to the acquiror, or to delete that data pre-acquisition? If not, will there be other enforceable controls to separate the personal data held by the target from that of the

396. *See* Bradley, *supra* note 16, at 151–54 (identifying variables considered in the reports of privacy ombuds in bankruptcy, and those relevant to privacy law as a whole).

397. *See supra* Section III.E.

acquiror (e.g., technical silos enforceable through legal process such as a consent decree), or to limit its use?

(6) Does the transaction violate the target's pre-acquisition privacy policy? If that policy purports to grant consent to the transaction (for example, by including a business continuity clause), is that consent legally adequate? As in the analysis for this Article, this evaluation should discount policy changes made immediately prior to the transaction to provide authorization for the deal, since the data held by the target was not collected under those terms.

(7) If the current privacy policy is violated by the deal, or relies on inadequate consent, will the target seek specific consent from consumers to the personal data processing required to complete the transaction? Rather than relying on the general privacy policy, as is the current practice, this would involve seeking consent to the specific transaction. This express seeking of consent to the transaction would, by definition, give consumers the opportunity to contemplate how the identity of the acquiror impacts their willingness to consent to a merger or acquisition, a relevant factor often overlooked in existing law.

(8) Are there terms in the target's privacy policy that seek to limit the processing of personal data after the transaction? For example, does the target's privacy policy purport to offer protections that would expressly remain in effect post-acquisition?

(9) Will the acquiror commit to abide by the target's privacy policy for the acquired data? If so, for how long?

(10) What protections does the target's privacy policy offer against later changes to its terms?

    (a) For example, does the policy permit unilateral change? How robust are the notice provisions for policy changes? What constitutes consent to policy changes in the terms of the policy?

(11) Beyond the protections afforded by the target's privacy policy, if any, will the acquiror agree to limit its uses of that data to the same purposes as the target (or purposes not materially incompatible)?

(12) If the acquiror does not agree to abide by the target's existing privacy policy, how and when does the acquiror plan to modify that policy?

(13) Will the acquiror agree to follow particular processes for notice and consent, if and when it seeks to modify the target's policy? Will individuals whose data is transferred be afforded the opportunity to opt out of later policy modifications? What will the process be to enable such opt-out?

(14) Will the target or privacy authorities require any binding, additional privacy protections for the transaction to occur, such as data silos or reliable anonymization of data, as appropriate to the specific transaction?

(15) Overall, is the transaction likely to be consistent with the reasonable expectations of privacy of the individuals whose data is being transferred, as informed by the above assessment?

This list seeks to evaluate the privacy impacts of a deal, but also reflects several practices that companies could adopt — or enforcers could require — to limit the expected privacy impacts of a given corporate transaction. These include maintaining the application of the target's existing privacy policy, and commitments by the acquiror to limit the use of data or future policy changes. For example, WhatsApp made a number of public statements to the effect that "nothing" would change for users, in particular, that it would continue to operate independently from Facebook and not serve any ads.[398] Companies could also go a step further, committing to keep the acquired personal data separate from their pre-existing data. As the Facebook/WhatsApp transaction illustrates, enforceability is a central challenge for these types of unilateral commitments. To address this challenge, enforcers could require legally binding commitments to sequester the target's data separately to prevent use by the acquiror. For example, in Google's acquisition of Fitbit, UK competition authorities required this sort of data silo be imposed such that Google could not use personal health data for advertising.[399]

As the FTC increases its scrutiny of potential privacy harm from mergers and acquisitions, Congress may need to clarify the scope of its authority to do so. Section 5 empowers the agency to engage in these sorts of inquiries into "likely" harm, and the FTC has been engaged in robust privacy enforcement under that section since the 1990s in areas other than M&A.[400] But it is also true that the FTC has, historically and recently, faced challenges to its authority as it expands into new

398. EPIC WhatsApp Complaint (2016) at ¶¶ 24–28, *supra* note 6 (recalling the public commitments made by WhatsApp and Facebook at the time of the acquisition).

399. *See* Press Release, European Commission, *supra* note 40.

400. *See* Hartzog & Solove, *supra* note 87.

enforcement areas.[401] This may repeat if the FTC ramps up privacy scrutiny of M&A, where it has not been actively enforcing, at least in a binding way, and where the harm may be forward-looking rather than extant as in most of the agency's privacy cases. For this reason, Congress should confirm that the FTC has authority to review and prevent privacy harm from mergers and acquisitions under Section 5, or even clarify such authority in an express and specific way.[402] While not strictly necessary, such legislative signaling would ensure the FTC could act decisively against privacy-harming corporate transactions.[403]

Another potential tool to help in detection and enforcement is advance notice to the FTC of certain mergers and acquisitions that present potential privacy risks. Such a notification requirement could be achieved in various ways. Perhaps the most narrowly tailored version would be for the FTC to include M&A reporting obligations in its Section 5 privacy settlements (whether the alleged violation is transactional or not).[404] Such reporting requirements are already fairly common for FTC consent orders in privacy cases, under the auspices of a broader obligation to notify the agency of "material changes" that may affect compliance, which may expressly include an obligation to report mergers.[405] So far these clauses have not led to any enforcement. Since this approach relies on consent agreements, it is limited to deals by acquirors that are subject to such FTC orders.

A broader version of this obligation would impose new statutory obligations to notify enforcers of M&A when those transactions meet certain criteria for privacy risk. Establishing such a privacy pre-merger notification regime would require legislative action. A detection system along similar lines is used in antitrust law, which statutorily mandates

---

401. Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935, 1954 (2000) (reflecting on the congressional and industry pushback when the FTC was perceived to have "reached too far" in its unfairness in the late 1970s); Ryan, LLC v. Fed. Trade Comm'n, 746 F. Supp. 3d 369, 390 (N.D. Tex. 2024) (holding unlawful and setting aside an FTC rule banning non-competes on the grounds it exceeds the FTC's statutory authority and is unconstitutional, arbitrary and capricious).

402. Challenging but important questions in the design of such an express amendment would include: the appropriate standard for incipient harm to trigger the FTC's transactional privacy powers, and the extent of remedial powers to condition or even block privacy-harming mergers.

403. This clarity of mandate has become increasingly important as the Supreme Court erodes deference to federal agencies, including the FTC specifically, when the empowering legislation is not adequately explicit in its delegation of powers. *See, e.g.*, Loper Bright Enters. v. Raimondo, 603 U.S. 369 (2023) (overturning longstanding precedent, Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984) (granting deferential review to agency action)); AMG Cap. Mgmt., LLC v Fed. Trade Comm'n, 593 U.S. 67, 77–78 (2021) (limiting FTC remedial authority based on statutory interpretation of Congressional intent).

404. Solove & Hartzog, *supra* note 87, at 606.

405. *Id.* at 619 (observing the FTC has "usually" imposed such an obligation in its then 170 consent orders in privacy cases; providing the example of the HTC Consent Order, which requires any material change that may affect compliance to be reported to the agency including a "merger") (citing HTC Am. Inc., 155 F.T.C. 1617 at 1636 (2013)).

that advance notice be filed with antitrust agencies before certain transactions that raise competition risks may be completed.[406] In privacy law, such filings could be limited to certain personal data-heavy industries, parties, or types of transactions that pose the greatest privacy risk. This potential for advance notification of deals is not raised here as a recommendation, or even an immediate possibility, but only to frame the types of tools that could enable stronger detection of transactional privacy harms. It is too early in the study of transactional privacy harms to know whether the not-insignificant administrative costs of a pre-merger filing system would be worthwhile. This would require further investigation and research into those costs, and more importantly, into the scope and frequency of transactional privacy harms, the characteristics of deals likely to create those harms, and what agencies need to detect them.

While this Section focuses on FTC intervention, it is also possible that state privacy enforcers could begin policing transactional privacy risks in their jurisdictions. The criteria proposed above would also be useful for such state action. State privacy review of transactions would likely require legislative change, but such change is not beyond contemplation. States have been actively passing privacy legislation in recent years. Several states already review certain healthcare transactions, and, more recently, there has been a flurry of new state antitrust legislation requiring state merger filings akin to federal HSR Act filings, to enable states to assess the competitive effects of deals in their jurisdictions.[407]

B. Future Research on Transactional Privacy Harms

As this Article illustrates, M&A has gone largely unaddressed in privacy scholarship, enforcement, and law, other than in occasional sectoral regulation. This Article shows that it only takes an examination of fifteen personal data acquisitions in the technology sectors to show that privacy effects of transactions are more mixed than privacy law seems to assume. This suggests further inquiry is needed to test assumptions about transactional privacy harm on a broader scale.

To assess the existence, nature, and prevalence of transactional privacy harms, future inquiry should consider M&A in other technology

406. *See, e.g.*, HTC Am., 155 F.T.C. at 1636. This obligation to file in advance of a deal was created pursuant to the Hart-Scott-Rodino Antitrust Improvement Act to help antitrust agencies detect transactions across the economy, and to give the agencies the chance to identify deals that violate antitrust law before they occurred.

407. Washington and Colorado recently adopted "mini" HSR Acts that require merger notification filing at the state level. Other states like Connecticut have pending bills to similar effect. *See* Washington Uniform Antitrust Pre-Merger Notification Act, S.B. 5122, 69th Leg., Reg. Sess. (Wash. 2025); Colorado Uniform Antitrust Pre-Merger Notification Act, S.B. 25-126, 75th Gen. Assemb., 1st Sess. (Colo. 2025).

transactions large and small, and in other personal data-driven industries like hospitality, grocery, other retail, and financial services. It should also expand beyond consideration of the privacy policies examined here to consider other factors that determine how corporate transactions affect privacy, such as the terms of the agreement for the merger or acquisition, legal practice in addressing privacy during those deals, public commitments made by merging parties beyond their policies, the actual (rather than written) data practices of the acquiror after the transaction, consumer behavior in using particular services and settings, and the design of online services and privacy settings, which are not examined by this Article.

As potential harms become better understood, the inquiry should consider whether existing law, which leans heavily on notice and consent, is adequate to protect against privacy harms from corporate transactions. Although this Article looks primarily at existing law, it also raises theories of how transactions could harm our privacy in ways that notice and consent are ill-suited to address, such as data aggregation harms.[408] The broader normative questions about the adequacy of notice and consent weigh heavily on the horizon as scholars and lawmakers press for new paradigms of privacy protection, and future transactional privacy analysis belongs squarely in their midst.

C. Realizing the Potential of Transactional Privacy Law: From Ex Post to Ex Ante

The analysis frames transactional privacy law as a nascent area in which existing law could improve. Its potential is much greater. Existing law treats M&A as a non-event, in which the harms that are caused are addressed later, at least in theory. This misses the fact that corporate transactions offer a point of legal intervention with significant potential to improve privacy protection. Transactional privacy law offers an underappreciated legal lever to address weaknesses in privacy law *as a whole*. This is because transactional privacy law presents an opportunity to shift from ex post to ex ante intervention.

The FTC's common law of privacy is largely applied ex post, waiting for harms to occur before intervening. But by their nature, many privacy harms call out for prevention ex ante rather than cures after the fact. As mentioned above, privacy harms can be difficult or impossible to undo once they occur. There may be no erasing the effects once an identity is disclosed, an invasive ad is served, or data is aggregated in ways that reveal sensitive information to a new company after a deal. The law also has trouble recognizing privacy harms given their nature,

408. *See supra* Section III.E (discussing the potential for aggregation harms to arise from personal data mergers and acquisitions).

which often involves the risk of reputational or future injury, often lacking direct financial or physical impacts that are firmly recognized in law.[409] This judicial difficulty in recognizing privacy harms has been labeled "one of the biggest challenges in privacy law,"[410] and its result is that "[c]ountless privacy violations are left unremedied not because they are unworthy of being addressed but because of the law's failure to recognize harm."[411]

These difficulties of remediation and recognition all point to the value of preventing, rather than fixing, certain privacy harms. I argue elsewhere that privacy law has, at its edges, begun to do exactly that — to impose more prospective rules (in place of mere notice and consent) that prevent or limit certain personal data uses, with the goal of reducing privacy harm from the outset.[412] Such thinking on how to guard against privacy harms before they occur echoes across influential concepts at a broader level, such as privacy by design, and minimizing data collection to guard against the potential for later data loss and harms.

Transactional privacy law, better developed, offers a prime opportunity to stop incipient privacy harms.[413] It can be used prospectively to limit the substantial and likely privacy harms in certain mergers and acquisitions, creating a powerful opportunity to address gaps in privacy law more broadly. M&A intervention under Section 5 of the FTC Act could prevent likely future harm to individuals' privacy where sectoral laws do not apply. Deal intervention could also preempt the exploitation of weak privacy policies that would otherwise allow unilateral, material changes to data uses — changes that may not be detected and addressed later. Such interventions could also move the law away from its heavy and often problematic dependence on consent, toward more models of privacy that are protective from the outset, and that rely less on individual comprehension or action that is increasingly impossible in the digital world.[414] In these ways, transactional privacy law has

409. Citron & Solove, *supra* note 180, at 796 (observing that courts "refuse to recognize privacy harms that do not involve tangible financial or physical injury"); *id.* at 814 (discussing the FTC's emphasis on financial and physical harms); *id.* at 816–18 (discussing the features of privacy harms that often make them difficult for the law to recognize); *see also* Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361 (2014) (discussing the challenges of privacy harm recognition); Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477 (2010).

410. Citron & Solove, *supra* note 180, at 796.

411. *Id.*

412. Douglas, *supra* note 26.

413. This raises questions for future research on the appropriate standard for intervention: how substantial, how likely and how imminent must the privacy harm be before the law intervenes? For comparison, the standard in antitrust law is that the effect of the transaction "may" be to "substantially" lessen competition, and the timeline over which this is assessed often depends on specific characteristics of the industry. 15 U.S.C. § 18 (2023).

414. Douglas, *supra* note 26, at 844–56 (tracing the movement of privacy law from notice and consent to more proscriptive models of privacy protection).

great potential, consonant with fundamental shifts underway as the new generation of privacy laws looks beyond notice and consent.

VI. CONCLUSION

Privacy law and scholarship have missed the relevance of mergers and acquisitions to modern privacy protection. Massive corporate transactions regularly transfer our personal data, with questionable consent, and growing privacy effects that are overlooked in privacy law and enforcement.

This Article pushes for definition, dialogue, and change in this privacy ideology toward mergers and acquisitions. First, it identifies a prevailing M&A exceptionalism in privacy law, wherein the data processing that occurs in mergers and acquisitions is often excluded or ignored by privacy law and enforcement. It examines the likely reasons for this M&A exceptionalism, and argues that with the rise of the digital economy, such reasons are often inadequate to justify the current scope of these exclusions from privacy law.

Then, the Article adds a data-driven analysis of fifteen high-profile technology acquisitions involving targets with vast stores of personal data. It finds that the effects of these M&A on privacy are mixed — often harmful, but sometimes beneficial. These impacts are often driven by the characteristics of the specific deal, in ways that privacy law has yet to appreciate. This analysis demonstrates that mergers and acquisitions are impacting our privacy in ways that are greater and more variable than privacy law assumes.

This analysis points to a need for stronger and more contextual application of privacy law to M&A involving personal data. To achieve this, the Article proposes the first screening criteria for enforcers to detect mergers and acquisitions that pose privacy risks. It also outlines paths for future research to build our understanding of transactional privacy harms and argues that a reevaluation of M&A exceptionalism has great potential to advance privacy law as a whole.

APPENDIX A: PERSONAL DATA ACQUISITIONS IN PRIVACY POLICY ANALYSIS

	Acquiring Company	**Target Company**	**Target's Main Services**	**Deal Closing Date**	**User Data Estimates at Deal Closing**
1	Facebook	WhatsApp[415]	Peer-to-peer messaging app	10/6/14	450 million monthly active users globally[416]
2	Facebook	Instagram[417]	Photo and video sharing social media app	9/6/12	30 million active users; 400 million photos[418]
3	Facebook	Onavo[419]	Smartphone app usage and optimization service	10/13/13	Not publicly available
4	Facebook	Giphy[420]	Graphic interchange format ("GIF") search engine	5/15/20	GIF usage trends across social media apps[421]

415. Facebook, Inc., Current Report (Form 8-K) (Oct. 4, 2014), https://www.sec.gov/Archives/edgar/data/1326801/000132680114000037/fb_8-kxclosingxofxwhatsapp.htm [https://perma.cc/92Q5-C26F].

416. *Facebook to Acquire WhatsApp*, META (Feb. 19, 2014), https://about.fb.com/news/2014/02/facebook-to-acquire-whatsapp/ [https://perma.cc/6R98-78R8].

417. Wortham, *supra* note 286.

418. Alexei Oreskovic & Gerry Shih, *Facebook to Buy Instagram for $1 Billion*, REUTERS (Apr. 10, 2012, at 13:10 ET), https://www.reuters.com/article/us-facebook-idUSBRE8380M820120410/ [https://perma.cc/24F5-JPM8].

419. Ingrid Lunden, *Facebook Buys Mobile Data Analytics Company Onavo, Reportedly for Up To $200M . . . And (Finally?) Gets Its Office in Israel*, TECHCRUNCH (Oct. 13, 2013, at 23:41 PT), https://techcrunch.com/2013/10/13/facebook-buys-mobile-analytics-company-onavo-and-finally-gets-its-office-in-israel/ [https://perma.cc/RSR5-BTN6].

420. Abram Brown, *Facebook Buys Giphy For $400 Million*, FORBES (May 15, 2020, at 11:11 ET), https://www.forbes.com/sites/abrambrown/2020/05/15/facebook-buys-giphy-for-400-million/ [https://perma.cc/9RXE-2PFR].

421. Kate O'Flaherty, *What Is Facebook Going To Do With 700 Million Giphy Users' Data?*, FORBES (May 17, 2020, at 6:25 ET), https://www.forbes.com/sites/kateoflahertyuk/2020/05/16/facebook-just-gave-700-million-giphy-users-a-reason-to-quit/ [https://perma.cc/U2H5-VMK2].

5	Microsoft	LinkedIn[422]	Professional networking platform	12/8/16	433 million members; 45 billion profile views quarterly[423]
6	Google	Double Click[424]	Digital advertising and ad management service	3/11/08	Ads seen by 80–85% of internet users; tracks user behavior across websites[425]
7	Google	YouTube[426]	Video-sharing platform	11/13/06	20 million unique monthly users; 100 million videos viewed daily; 65,000 daily video uploads[427]
8	Google	Waze[428]	Crowd-sourcing navigation app	6/11/13	Estimated 50 million users globally;[429] 90 million user traffic reports, 500 million user map edits as of 2012[430]

422. LinkedIn, Inc., Current Report (Form 8-K) (Dec. 8, 2016), https://www.sec.gov/Archives/edgar/data/1271024/000110465916161289/a16-22816_18k.htm [https://perma.cc/JA36-93BW].

423. *Microsoft to acquire LinkedIn*, MICROSOFT (June 13, 2016), https://news.microsoft.com/source/2016/06/13/microsoft-to-acquire-linkedin/ [https://perma.cc/K9PY-5S6X].

424. Eric Schmidt, *We've officially acquired DoubleClick*, GOOGLE BLOG (Mar. 11, 2008), https://googleblog.blogspot.com/2008/03/weve-officially-acquired-doubleclick.html [https://perma.cc/3B2H-ZG28].

425. *Privacy? Proposed Google/DoubleClick Merger*, EPIC, https://epic.org/documents/privacy-proposed-google-doubleclick-merger/ [https://perma.cc/P66C-MRK6].

426. Google, Inc., Current Report (Form 8-K) (Nov. 13, 2006), https://www.sec.gov/Archives/edgar/data/1288776/000119312506238320/d8k.htm [https://perma.cc/FF2R-QWQG].

427. *YouTube serves up 100 million videos a day*, NBC NEWS (Jul. 16, 2006, at 15:18 ET), https://www.nbcnews.com/id/wbna13890520 [https://perma.cc/4L2Y-WS3S].

428. Dominic Rushe, *Google Buys Waze Map App for $1.3bn*, THE GUARDIAN (June 11, 2013, at 13:10 ET), https://www.theguardian.com/technology/2013/jun/11/google-buys-waze-maps-billion [https://perma.cc/H8BS-SAEK].

429. Rip Empson, *WTF Is Waze and Why Did Google Just Pay A Billion+ For It?*, TECHCRUNCH (June 11, 2013, at 21:01 PT), https://techcrunch.com/2013/06/11/behind-the-maps-whats-in-a-waze-and-why-did-google-just-pay-a-billion-for-it/ [https://perma.cc/MNN4-32GR].

430. Catherine Shu, *Nav App Waze Says 36M Users Shared 900M Reports, while 65K Users Made 500M Map Edits,* TECHCRUNCH (Feb. 6, 2013, at 20:00 PT), https://techcrunch.com/2013/02/06/nav-app-waze-says-36m-users-shared-900m-reports-while-65k-users-made-500m-map-edits/ [https://perma.cc/7UVK-J4E2].

9	Google	Nest[431]	Smart-home devices (thermostats, smoke detectors)	2/7/14	Estimated sales of 100,000 thermostats per month[432]
10	Google	Fitbit[433]	Wearable fitness tracking devices	1/14/21	30 million users; 181 billion hours of heart rate data; 9 billion nights of sleep; 457 billion minutes of exercise; 10 million data points on menstrual cycles and fertility[434]
11	Google (Alphabet)	Bright Bytes[435]	Educational data analytics platform	10/11/22	Student performance metrics and technology use in 125,000 schools[436]
12	Apple	Shazam[437]	Music recognition	9/24/18	1 billion app downloads; 20 million songs recognized per day[438]
13	Amazon	One Medical[439]	Membership-based medical care	2/22/23	815,000 members and 214 medical offices across

431. Lance Whitney, *Google closes $3.2 billion purchase of Nest*, CNET (Feb. 12, 2014, at 5:00 PT), https://www.cnet.com/tech/services-and-software/google-closes-3-2-billion-purchase-of-nest/ [https://perma.cc/X4XV-PCTR].

432. *What's Next for Nest at Google?*, PRODUCT HABITS, https://producthabits.com/whats-next-nest-google/ [https://perma.cc/73XD-QBCV].

433. Fitbit, Current Report (Form 8-K), *supra* note 34.

434. Griebeler da Motta, *supra* note 9.

435. *Alphabet Inc. acquired BrightBytes Inc.,* MARKETSCREENER (Oct. 10, 2022), https://www.marketscreener.com/quote/stock/ALPHABET-INC-24203373/news/Alphabet-Inc-acquired-BrightBytes-Inc-42007362/ [https://perma.cc/3QNP-J6VC].

436. Ian Daly, *Google is Taking a Silent Step Into the Ed Data Space By Buying BrightBytes*, E3D NEWS (Oct. 17, 2022), https://e3dnews.com/2022/10/17/google-is-taking-a-silent-step-into-the-ed-data-space-by-buying-brightbytes/ [https://perma.cc/7ZX8-GK5S].

437. *Apple acquires Shazam, offering more ways to discover and enjoy music*, APPLE (Sep. 24, 2018), https://www.apple.com/newsroom/2018/09/apple-acquires-shazam-offering-more-ways-to-discover-and-enjoy-music/ [https://perma.cc/XKE6-JNE4].

438. *Id.*

439. 1LifeHealthcare, Inc., Current Report (Form 8-K) (Feb. 22, 2023), https://www.sec.gov/Archives/edgar/data/1404123/000119312523044883/d468299d8k.htm [https://perma.cc/8VZD-C7UC].

					more than 20 U.S. markets[440]
14	Amazon	Whole Foods[441]	Organic groceries	8/28/17	Grocery purchase data of millions of customers;[442] 460 stores across U.S. Canada, & Britain[443]
15	Amazon	Twitch.tv[444]	Interactive streaming platform for video gaming	9/25/14	55 million viewers; 15 billion minutes of video content; 1 million broadcasters[445]

440. *Id*.

441. Amazon, Current Report (Form 8-K) (Aug. 28, 2017), https://www.sec.gov/Archives/edgar/data/1018724/000119312517269093/d448689d8k.htm [https://perma.cc/UC28-KGMJ].

442. *How Whole Foods Got Its Data Intelligence Strategy Right*, MERIT, https://web.archive.org/web/20230426065750/https://www.meritdata-tech.com/resources/blog/retail-data/whole-foods-data-intelligence/ [https://perma.cc/F76U-QYKC].

443. Nick Wingfield & Michael de la Merced, *Amazon to Buy Whole Foods for $13.4 Billion*, N.Y. TIMES (June 16, 2017), https://www.nytimes.com/2017/06/16/business/dealbook/amazon-whole-foods.html [https://perma.cc/5ACY-47ME].

444. Amazon, Current Report (Form 8-K) (Sep. 25, 2014), https://www.sec.gov/Archives/edgar/data/1018724/000101872414000046/amzn-2014september22x8k.htm [https://perma.cc/Z62H-3GEB].

445. *Amazon.com to Acquire Twitch*, AMAZON (Aug. 25, 2014), https://press.aboutamazon.com/2014/8/amazon-com-to-acquire-twitch [https://perma.cc/YKU9-UZ2M].