Privacy for Sale: The Law of Transactions in Consumers' Private Data

Christopher G. Bradley†

Lawmakers, regulators, consumer advocates, and the business community have focused increasing attention on the policy issues that arise at the intersection of privacy, technology, and commerce. Yet the law governing what businesses can do with consumer data remains unsettled and unclear. The United States has no dedicated and comprehensive privacy law, relying instead on a patchwork of general consumer protection laws and industry-specific regulations like HIPAA. The FTC has created what scholars have called a "common law of privacy" through its enforcement actions and published guidance, but how privacy law applies to business practices often remains uncertain.

This Article uncovers a large new trove of privacy law, elaborating the jurisprudence of privacy with reports submitted to courts in which hundreds of millions of consumers' private information has been put up for sale. A unique provision of bankruptcy law requires the appointment of a privacy expert when consumer information is put up for sale, to report on the sale's legality. These expert reports constitute an unrecognized but substantial body of privacy law. The Article presents and analyzes reports submitted from 2005 to 2020—a hand-collected dataset gathered from 141 court dockets. The reports dramatically increase what is known about how the "common law of privacy" applies in practice to sales of consumer data in a legal forum, and what the future of privacy law may hold.

The reports generally advocate a pro-transactional view and permit sales to proceed in spite of existing privacy promises so long as the purchasers' use of consumer data will be roughly consistent with the sellers'. They rely on aspects of the traditional "notice and choice" regime that has guided privacy law, but

† Wyatt, Tarrant & Combs Associate Professor, University of Kentucky Rosenberg College of Law. This paper benefitted from the work of excellent research assistants, without whom this empirical study would not be possible: Timothy Lovett (Kentucky Law '19), Marina Kirtland Carrier (Kentucky Law '20), Alexys Bardonaro (Kentucky Law '22), Michaela Hood (Kentucky Law '23), Shawn Harkins (Kentucky Law '23), Breanna Carper (Kentucky Law '23), and Justin Potter (Kentucky Law '24). Thanks also to Chris Hoofnagle, Josh Douglas, Ted Janger, Ethan Mirkin, Dan Schwarcz, Beau Steenken, Katherine Strandburg, David Treacy, and Ari Ezra Waldman; commentators at workshops convened by the Privacy Law Scholars Conference, the AALS Section on Law and Social Science, the International Association of Consumer Law, the University of Florida, and the University of Kentucky; and the editors of the *Yale Journal on Regulation*. I appreciate the United States Bankruptcy Court for the District of Massachusetts for locating and providing historical materials related to the *Toysmart.com* case. Finally, I am grateful to my children, L. and E., for allowing me to work on this project for some of our many pandemic days together at home.

they also include substantive consideration of the reasonable expectations that consumers may have formed or of the sensitivity of the information to be transferred. Thus, the reports reflect privacy law's shift beyond strictly consent-based contractarian models and toward more substantive and context-based approaches.

The reports also speak to the institutional context of regulation of commerce in consumer information. On the one hand, the reports impose significant limits on companies selling private data, which suggests that expert oversight and supervision mechanisms, such as the legal regime that generated these reports, can play an important role in privacy regulation on the ground. But the reports are, on the whole, timid and formulaic, hewing closely to existing precedent and showing little inclination to adapt or develop it even when novel circumstances might justify a change in course. This hesitancy indicates that privacy law's continuing development requires leadership from federal and state policymakers.

Introduction

> Facebook became a five-hundred-and-sixty-billion-dollar company . . . by devising the most successful system ever for compiling and purveying consumer data.
>
> – Louis Menand, *The New Yorker*[1]

> I'd like you to think about data as the next natural resource.
>
> – Ginni Rometty, CEO of IBM, to the Council on Foreign Relations[2]

Consumers entrust increasing amounts of personal data to companies. As artificial intelligence and "Big Data" analytics permit companies to do more with that data, concerns over the collection, protection, and monetization of consumers' private data have grown more prominent. Congress convenes high-profile hearings,[3] successive occupants of the White House promise action, news outlets churn out hand-wringing articles,[4] and legal and policy experts continue to produce work on how to regulate companies' treatment of data.[5] The National Conference of State Legislatures reports that "[a]t least 38 states introduced more than 160 consumer privacy related bills in 2021 (compared to 30 states in 2020

1. Louis Menand, *Why Do We Care So Much About Privacy? Big Tech Wants to Exploit Our Personal Data, and the Government Wants to Keep Tabs on Us*, NEW YORKER (June 18, 2018), https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy [https://perma.cc/9PPP-UQBD].

2. *A Conversation with Ginni Rometty*, COUNCIL ON FOREIGN RELS. (Mar. 7, 2013), https://www.cfr.org/event/conversation-ginni-rometty [https://perma.cc/MXF2-LNEY]. On this metaphor, see Lauren Henry Scholz, *Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 TENN. L. REV. 863 (2018).

3. *See, e.g.*, *Protecting Consumer Privacy: Hearing Before the S. Comm. on Com., Sci., and Transp.*, 117th Cong. (2021); *Holding Big Tech Accountable: Legislation to Build a Safer Internet*, *Hearing Before the Subcomm. on Consumer Prot. & Com. of the H. Comm. on Energy & Com.*, 117th Cong. (2021).

4. *See, e.g.*, Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019); David McCabe, *Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight*, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html [https://perma.cc/E5C4-77Q7] ("Republicans and Democrats in Congress, as well as the Trump White House, all said they wanted a new federal law to protect people's online privacy."); Office of the Press Secretary, *We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online*, WHITE HOUSE (Feb. 23, 2012), https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights [https://perma.cc/6EWF-YZGZ].

5. *See, e.g.*, Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573 (2021); Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733 (2021); Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327 (2021); Lauren E. Willis, *Deception by Design*, 34 HARV. J.L. & TECH. 115 (2020); Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age*, 30 J. CONSUMER PSYCH. 736 (2020); Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773 (2020); Neil M. Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019); Ryan Calo, *Privacy Law's Indeterminacy*, 20 THEORETICAL INQUIRIES L. 33 (2019); Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653 (2019); Daniel J. Solove & Danielle Keats Citron, *Risk & Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018).

and 25 in 2019),"[6] and there is similarly intense interest in consumer privacy at the federal level, both in Congress[7] and at the Federal Trade Commission (FTC).[8]

Despite wide acknowledgement of its importance, the actual law of privacy remains famously unclear and incomplete: it has been described as a "patchwork,"[9] a "hodgepodge,"[10] a "kludge,"[11] and a "smorgasbord"[12]—a "piecemeal"[13] and "scattershot"[14] law, "[held] together with duct tape,"[15] but left with "gaps."[16] There are two aspects of the privacy-law problem in the United States: there is no comprehensive legislative or regulatory framework, and there is a lack of case law applying the law that does exist. Outside of a few narrow areas of clearer and more traditional regulation,[17] interested parties have to glean the law governing companies' use of consumers' private data from various settlements and consent decrees, broad and nonbinding guidelines from regulators, and a snippet of statutory language inserted in 1938 to a statute originated in 1914.[18] Because enforcement actions nearly always involve either egregious violations or prominent defendants, and nearly always settle, there is often little guidance for how to apply this makeshift framework to particular fact scenarios.[19] A company that wishes to know, "Is what we are planning to do

6. *2021 Consumer Data Privacy Legislation*, NAT'L CONF. STATE LEGISLATURES (Dec. 27, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx [https://perma.cc/D5Y6-DMMJ]; *see also* Chander et al., *supra* note 5, at 1769 (describing recent, "unprecedented volume of legislative proposals that would regulate data privacy at the state level").

7. *See* Müge Fazlioglu, *U.S. Federal Privacy Legislation Tracker*, INT'L ASS'N PRIV. PROS. (Apr. 2022), https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker/ [https://perma.cc/RF25-W6JA] (reflecting the dozens of bills filed in the 117th Congress).

8. Andrea Vittorio, *FTC Sees Growing Pressure for Data Privacy Rule as Pick Stalled*, BLOOMBERG L. (Feb. 8, 2022, 5:00 AM), https://news.bloomberglaw.com/privacy-and-data-security/ftc-sees-growing-pressure-for-data-privacy-rule-as-pick-stalled [https://perma.cc/884N-ZXNJ] (noting the addition of consumer privacy law to the rulemaking agenda in December 2021).

9. Viljoen, *supra* note 5, at 585 n.14; Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 258 n.32 (2011) (collecting sources).

10. Edward J. Janger, *Privacy Property, Information Costs, and the Anticommons*, 54 HASTINGS L.J. 899 (2003).

11. WOODROW HARTZOG, PRIVACY'S BLUEPRINT 56 (2018).

12. William McGeveran, *Friending the Privacy Regulator*, 58 ARIZ. L. REV. 959, 973 (2016).

13. William Magnuson, *A Unified Theory of Data*, 58 HARV. J. ON LEGIS. 23, 23 (2021).

14. Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1057 (2021).

15. HARTZOG, *supra* note 11, at 56.

16. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 145 (2016).

17. *See infra* notes 229-239 and accompanying text.

18. Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2018); *see* Eugene R. Baker & Daniel J. Baum, *Section 5 of the Federal Trade Commission Act: A Continuing Process of Redefinition*, 7 VILL. L. REV. 517, 517 n.1 (1962) (noting the insertion of "unfair or deceptive acts or practices in commerce" in 1938).

19. McGeveran, *supra* note 12, at 1001 ("FTC enforcement targets the big guys, the bad guys, and those who harm kids."); HOOFNAGLE, *supra* note 16, at 107 (noting FTC's focus on "egregious" cases); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 610-11 (2014) (noting that as of 2014, "the FTC has issued over 170 privacy-related complaints against companies" and "virtually every complaint has either been dropped or settled").

legal?," or a consumer who wants to know, "How could this company legally use my data?," will have little guidance as to many common scenarios.[20]

Despite privacy law's somewhat crude and makeshift assemblage, experts have sought to provide a coherent account of current privacy law by identifying some of the major sources of its content and by investigating its implementation on the ground by regulators and within companies. Daniel Solove and Woodrow Hartzog used the FTC's enforcement actions and other "privacy jurisprudence" to outline what they called "the new common law of privacy."[21] Kenneth Bamberger and Deirdre Mulligan argued that U.S. privacy policy depends on a body of experts, including both corporate privacy officers and regulators, who are tasked with adapting and applying the overarching principles and norms of privacy law to the new challenges presented "as new types of products, technologies, and business models evolve."[22] Subsequent work has built on these influential accounts of privacy law, extending, refining, and critiquing them based on new data, theories, and developments in technology and society.[23]

This Article uncovers a large new trove of privacy law, elaborating the jurisprudence of privacy with reports submitted to courts in which hundreds of millions of consumers' private information has been put up for sale. Under a 2005 law, a privacy expert must be appointed in bankruptcy proceedings when consumer information is put up for sale to report on the sale's legality. This unique provision has generated an unrecognized but substantial body of privacy law. The Article presents and analyzes privacy reports submitted from 2005 to 2020, creating a hand-collected dataset gathered from 141 court dockets. These reports, written by government-appointed experts with the involvement of regulators, apply the law of privacy to the facts of specific commercial transactions. The reports dramatically increase what is known about how the "common law of privacy" applies in practice to sales of consumer data in a legal forum.

In addition, because these reports arose in the context of consensual dealings and not regulatory enforcement actions, they open a larger window into the development of what Bamberger and Mulligan characterized as the "robust substantive definitions of privacy and the processes and protections they are beginning to produce" among a wide range of private- and public-sector actors.[24] In other words, the Article speaks not only to the black-letter law of privacy but

20. *See* Waldman, supra note 5, at 797 ("[B]y the FTC's own count, the agency averages only ten privacy-related cases per year, limiting the sources lawyers have from which to glean lessons and find clarity."); *id*. at 833 (reporting on interview responses of privacy professionals who invited "clearer guidance" and "specific statements" of privacy law).

21. *See* Solove & Hartzog, *supra* note 19.

22. Bamberger & Mulligan, *supra* note 9, at 266; *see id*. at 271 ("[T]he definitional ambiguity inherent in privacy regulation requires companies to embrace a dynamic, forward-looking outlook towards privacy."); *see also* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015).

23. *See, e.g.*, McGeveran, *supra* note 12; Waldman, *supra* note 5; Ryan Calo, *Privacy and Markets: A Love Story*, 91 NOTRE DAME L. REV. 649 (2016).

24. Bamberger & Mulligan, *supra* note 9, at 248.

also to that law's implementation in commercial life by companies, privacy officers and other experts, and regulators. This body of law increases the guidance available to companies as well as to consumers and their advocates. In addition, it provides a more solid basis for future lawmaking, permitting advocates and policymakers to proceed based on a precise knowledge of the scope of the current law in a new collection of concrete cases.

Part II of this Article summarizes privacy law in the United States. The primary focus of U.S. privacy law has been the laissez-faire "notice and choice" framework, under which companies provide some notice of their data protection practices to consumers. Companies must also offer consumers an opportunity to consent to those policies by declining to use a company's product or by opting out of a given program or form of communication. But the notice-and-choice approach has been subject to sharp criticism because companies can manipulate this framework, and consumers' consent is not always knowing, voluntary, or in the public interest. Accordingly, over time, regulators have tried to modify the model. For example, they have sought to establish substantive baseline norms that apply regardless of whether a company has pledged to follow them. And they have looked beyond explicit privacy promises to customers' reasonable expectations of privacy. According to at least some regulators and experts, then, custodians of consumer data may not merely go through a rote exercise of providing unread disclosures, obtaining nominal consent, and acting as they will: they must adhere to reasonable privacy practices and be attuned to consumers' privacy expectations. This shift in regulatory approach remains contested and incomplete, but the data reported in this Article reflects its influence.

Part II also discusses the challenges of enforcing privacy laws when violations can be accomplished easily and all-but-undetectably, and it notes that sanctions for breaches of privacy promises likely under-deter bad behavior. Finally, this Part discusses the *Toysmart* case, in which a failed dot-com sought—in direct violation of its own privacy policies—to market consumer data to the highest bidder as part of a going-out-of-business sale. After public outcry, the sale was scuttled, but the *Toysmart* controversy prompted Congress to pass the consumer privacy ombudsman provisions of bankruptcy law and ultimately led to the creation to the new body of privacy law presented in this Article.

Part III summarizes the new body of privacy "common law." The source of this law is reports prepared by privacy experts called "consumer privacy ombudsmen"—or simply "ombuds"[25]—who are appointed when companies

25. Terminology about ombuds is unsettled. Modern sources tend to the less cumbersome, gender-neutral terms "ombuds" or "ombud" rather than "ombudsman," but there is disagreement over whether the singular should be "ombuds" or "ombud" (which this Article uses). *See, e.g.*, CHARLES L. HOWARD, A PRACTICAL GUIDE TO ORGANIZATIONAL OMBUDS: HOW THEY HELP PEOPLE AND ORGANIZATIONS 3 (2022); Amanda Robert, *What Are Ombuds? The ABA Provides a Primer on Special Day*, AM. BAR ASS'N (Oct. 9, 2019, 6:30 AM CDT), https://www.abajournal.com/web/article/what-are-ombuds-the-aba-provides-a-primer-on-special-day [https://perma.cc/G7YE-KPAQ] (providing examples); Varda Bondy & Margaret Doyle, *'Manning' the Ombuds Barricades*, OMBUDS RSCH. (June 9, 2015), https://ombudsresearch.org.uk/2015/06/09/manning-the-ombuds-barricades/ [https://perma.cc/

propose to sell consumer data contrary to an existing privacy policy.[26] By law, ombuds are tasked with evaluating the proposed sale and producing a recommendation to the court on whether to approve the sale.[27] Federal and state regulators regularly weigh in on these recommendations, and parties and courts generally accept them. In practice, ombuds' reports provide a record of the law of privacy as applied to individual cases.

While a few academic publications have discussed the consumer privacy ombudsman regime,[28] there are no systematic and comprehensive studies of it. This Article, together with a companion article focused on the institutional and bankruptcy-specific aspects of the ombud regime,[29] provide the first. In addition, and unlike most other studies,[30] this Article explores the implications of the reports for privacy law, taking advantage of the transparency that this unique legal regime brings to actual transactions in consumer data.

My research team hand-collected information from every case in which an ombud filed a report from the time the law went into force in 2005 through July 2020—141 in total.[31] We then analyzed each report to determine what it contributes to privacy law.[32] The reports form a previously overlooked body of privacy law concerning sales of consumers' private information and can serve as a valuable resource for privacy experts, corporate decision makers, consumer advocates, and policymakers.

6GF3-36HJ] (providing linguistic discussion of both "ombud" and "ombuds" as singular forms of word in recognized institutional contexts); James Harbeck, *Ombud*, SESQUIOTICA (May 2, 2018), https://sesquiotic.com/2018/05/02/ombud/ [https://perma.cc/TUT5-A4AM] (providing linguistic and historical analysis and endorsing "ombud" as singular form); David Rasch, *A Meatball by Any Other Name*, 11 J. INT'L OMBUDSMAN ASS'N, no. 6, 2018, at 1, 1-4 (endorsing "ombuds" in lieu of "ombudsman" in the organizational name on gender-equity grounds). On the role of ombuds in historical and modern legal and institutional settings, see Kenneth Culp Davis, *Ombudsmen in America: Officers to Criticize Administrative Action*, 109 U. PA. L. REV. 1057 (1961) (discussing the introduction of ombuds in the United States); and McKenna Lang, *A Western King and an Ancient Notion: Reflections on the Origins of Ombudsing*, 2 J. CONFLICTOLOGY 56 (2011) (discussing historical origins).

26. *See* 11 U.S.C. §§ 332, 363(b)(1) (2018); *infra* notes 140-144 and accompanying text.

27. *See infra* notes 140-144 and accompanying text.

28. *See, e.g.*, Laura M. Coordes, *Unmasking the Consumer Privacy Ombudsman*, 82 MONT. L. REV. 17 (2021); Diane Lourdes Dick, *The Bankruptcy Playbook for Dealing with Valuable Data Assets*, 42 BANKR. L. LETTER 1, 3-4 (Jan. 2022); Kayla Siam, *Coming to a Retailer Near You: Consumer Privacy Protection in Retail Bankruptcies*, 33 EMORY BANKR. DEV. J. 487, 510-12 (2017); Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 426 B.C. L. REV. 423, 475-83 (2018); Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 WM. & MARY L. REV. 1801, 1873-77 (2003) (critiquing the proposed regime before it was passed into law).

29. Christopher G. Bradley, *Privacy Theater in the Bankruptcy Courts*, 74 HASTINGS L.J. (forthcoming 2023) (on file with author). It is of course possible that the "common law of privacy" developed by ombuds is somehow misrepresentative of privacy law in general because it arises in bankruptcy proceedings. But the Bankruptcy Code does not instruct ombuds to take into account anything about the particularities of a business in bankruptcy into account, and the reports do not give the impression that the context of bankruptcy has distorted their analysis of privacy law. *See* 11 U.S.C. §§ 332, 363(b)(1) (2018).

30. *See* Coordes, *supra* note 28; Dick, *supra* note 28; Janger, *supra* note 28; Siam, *supra* note 28.

31. Technically, there are 141 cases in which reports were filed; because some cases featured multiple reports, the number of reports is higher. *See infra* note 153 and accompanying text.

32. *See infra* Section III.A (explaining the components of analysis).

The reports generally permit sales to proceed even when contrary to privacy promises made to consumers, though subject to guidelines intended to keep purchasers' use of the data roughly consistent with the sellers'. They impose guardrails modeled on the FTC's position in *Toysmart*, permitting sales to so-called "qualified buyers." No sales to data brokers are permitted by these reports,[33] and few reports permit "stand-alone" sales of the data. Instead, most reports require that the buyer purchase the seller's entire business, including customer data, to engage in the same type of business as the seller; that the buyer use the information for the same purpose as the buyer; that the buyer abide by the seller's privacy policy; and that some form of notice and opportunity to "opt out" of the transaction be provided. Most provide some restriction on future modifications of privacy policies. And reports tighten their restrictions somewhat when sensitive information—such as health, financial, or other highly personal information—is involved, but they still generally permit the transfer.

Notably, these guardrails are often put in place even when companies' policies arguably permit less restricted sales. In doing so, the reports appear to look beyond the explicit text of a company's privacy policies and rely on a more holistic and substantive conception of reasonable consumer expectations of privacy, such as that increasingly endorsed by the FTC.

Part III then shows that the reports compare favorably with other sources of privacy jurisprudence. The limited breadth of the reports' circulation stands as their primary weakness as sources of privacy law—a problem this Article begins to remediate. Compilation and publication of the reports, which could be undertaken by the FTC or by the Department of Justice's bankruptcy supervisor—the United States Trustee—would be another positive step to ensure the work of ombuds and bankruptcy courts can be appropriately considered by privacy experts and decision makers.

Finally, Part III turns to the doctrinal and institutional implications of this study for the development of consumer privacy law. What is most striking is the pervasiveness of the "qualified buyer" approach to transfers of consumer data, both in situations where privacy policies would seem to permit less restrictive transfers and where the policies would bar all transfers. This approach essentially moves much of consumer privacy protection outside of the contractarian framework and into one more focused on the provision of substantive protections based on consumer expectations and overarching norms of reasonable commercial behavior. The fact that expert ombuds apply this framework to so many factual scenarios suggests that it may be an increasingly appealing and feasible approach to privacy law.

Institutionally, policymakers should consider reforms drawing on the success of the consumer privacy ombudsman regime—success demonstrated by the fact that the sales in the reports included significant consumer protections and avoided, for instance, stand-alone sales of private information to data

33. On data brokers, see *infra* notes 74-76 and accompanying text.

brokers. Obligating companies to abide by a core set of privacy protections, involving an independent expert to report on compliance with those protections, and requiring that transactions be subjected to public scrutiny seem to deter at least some abusive business practices. Perhaps similar regimes should govern commerce in private information outside of the narrow context of bankruptcy sales.

The reports also suggest that privacy law's ad-hoc, common-law style of development has serious limits. On the one hand, the reports support the claim that the FTC has developed a significant common law of privacy that experts continue to develop through application to particular fact scenarios. On the other hand, ombuds' heavy reliance on a few crucial FTC decisions and documents demonstrates the continuing importance of centralized, top-down guidance concerning basic privacy-law principles. Even the most insightful and creative experts are profoundly limited in the materials they have before them and in the lawmaking they can do. Significant shifts in the law depend on "policy entrepreneurs" such as legislators and regulators, who can chart new courses and set larger-scale changes in motion. Such policy entrepreneurs have superior capacity to gather information concerning current practices, study consumer preferences, evaluate the economic impact of current and proposed laws, and work with and mobilize public support for policy changes.

In addition, the privacy law in the reports lends some support to a more critical viewpoint on the entire modern privacy-law framework: at times, the reports seem to prioritize commerce in data over consumer protection and to promote a vision of privacy law as a routinized exercise in empty, "tick the box" corporate compliance.[34] Closer study of the work of ombuds may help expose these weaknesses in modern privacy law.

I. An Evolving and Incomplete Law of Consumer Privacy

Public concern with consumer privacy has been stoked not only by the periodic disclosure of massive leaks, breaches, or misuses of data,[35] but also by daily, unavoidable realities of modern, digitally connected life.[36] Ever more intimate information passes through the hands of businesses, from shopping and media-consumption data collected through websites and applications to health

34. *See, e.g.*, Waldman, *supra* note 5, at 776 (arguing that "[c]orporate privacy practices today . . . prioritize innovation over regulation, efficiency over social welfare, and paperwork over substance").

35. *See, e.g.*, Joseph Marks, *The Cybersecurity 202: There Was Another Massive Data Breach*, WASH. POST (Aug. 19, 2021), https://www.washingtonpost.com/politics/2021/08/19/cybersecurity-202-there-was-another-massive-data-breach-people-will-probably-forget-it-week/ [https://perma.cc/D83U-Y5Z5] (describing the breach of personal information of "40 million current, former and prospective T-Mobile customers").

36. *See* Magnuson, *supra* note 13, at 30-33.

data collected by smartphones and "wearable tech."[37] Businesses rely on consumer information to generate their profits. Digital advertising now constitutes nearly two-thirds of total advertising expenditures, and consumer data is crucial to the industry.[38] As the *Wall Street Journal* reported in December 2021:

> Many consumer-facing businesses, including retailer Walmart Inc., healthcare company CVS Health Corp. and food-ordering and delivery platform DoorDash Inc., are offering advertisers more ways to reach consumers using data they store on shoppers' purchases. . . . [M]edia advertising with retailers will grow 47% in 2021 to reach $77 billion globally. That comes after the segment grew 24% in 2019 and 53% in 2020.[39]

Consumer data is crucial to this large, fast-growing industry. The tools of artificial intelligence and "Big Data" analytics enhance its value by uncovering and exploiting the particular vulnerabilities revealed by data that consumers have—knowingly or not—surrendered.[40]

Despite widespread conviction about the importance of setting policy at the intersection of privacy, technology, and commerce, the law in this area remains unsettled at best. Consumer privacy in the United States is governed by a patchwork of laws, with the FTC playing the role of primary privacy regulator. Historically, privacy law has been dominated by a much-criticized "notice and choice" model, which prioritizes disclosure over more substantive rules of consumer protection. Regulators have increasingly turned to a regime based on a fuller understanding of reasonable consumer expectations, although the transition remains incomplete and contested. Privacy law has also been criticized for lack of sufficient enforcement mechanisms. Existing causes of action are widely considered adequate to deter wrongdoing, and wrongdoers often evade detection since transactions in consumers' private information can be accomplished easily and invisibly.

After summarizing current privacy law and regulation, this Part provides background on the *Toysmart* case, in which a failed dot-com sought to sell consumers' private information in contravention of its privacy promises. The *Toysmart* controversy prompted Congress to pass the consumer privacy

37. *See, e.g.*, Jacob Gallagher, *From the Apple Watch and Ray-Ban Stories to Oura: How Wearable Tech Got Stylish*, WALL ST. J. (Oct. 6, 2021), https://www.wsj.com/articles/wearable-tech-11633548732 [https://perma.cc/6NYV-A4XR] (noting the "onslaught of data" from "wearables" and warning that "[i]f privacy is paramount to you beware . . . companies do gather your personal data tracked on these devices"); Elvy, *supra* note 28, at 435-39 (describing the Internet of Things "gold rush").

38. *See* Megan Graham, *Advertising Market Keeps Growing Much Faster Than Expected, Forecasters Say*, WALL ST. J. (Dec. 6, 2021), https://www.wsj.com/articles/advertising-market-keeps-growing-much-faster-than-expected-forecasters-say-11638784800 [https://perma.cc/2K9U-SUZW].

39. *Id.*

40. Willis, *supra* note 5, at 121-51; *see also* Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 43-44 (2021); Roger Allan Ford, *Data Scams*, 57 HOUS. L. REV. 111, 183 (2019); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014).

ombudsman provisions of bankruptcy law and ultimately led to the creation to the new body of privacy law presented in this Article.

A. Privacy Law and Consumer Protection

There are no comprehensive federal statutory or regulatory regimes governing privacy in the United States. Several international authorities, such as Canada and the European Union, have dedicated and comprehensive privacy laws,[41] and several states have regulated privacy more thoroughly in recent years.[42] But the United States relies on sector-specific laws and regulations, such as those governing financial institutions, healthcare providers, or websites directing their activities to children.[43] Large swathes of commercial activity are not covered by privacy-specific legislation or regulation at the federal level, leaving the Federal Trade Commission to fill in the sizeable gaps.

1. The FTC as Primary Privacy Regulator

The FTC has been left to do much of the work of regulating consumer privacy.[44] The FTC Act broadly allows the FTC to "to prevent persons . . . from using . . . unfair or deceptive acts or practices in or affecting commerce."[45] This provision reaches all sorts of commercial activity, including the gathering and use of consumers' private data.

But this broad language belies the strict limitations that the FTC faces in exercising its power under the FTC Act.[46] Due to worries about FTC overreach, Congress sharply curtailed the FTC's ability to regulate and imposed onerous administrative requirements on its rulemaking.[47] These restrictions have deterred

41. *See* STEPHEN MULLIGAN & CHRIS LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 43-44 (2019) (discussing European data protection); Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357, 378-82, 391-93 (2005) (describing Canadian law).

42. *See, e.g.*, California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.100-1798.199 (West 2022).

43. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.); 45 C.F.R. Parts 160, 164 (2021); Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.); Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6506 (2018); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 502(b), 113 Stat. 1338, 1437 (1999); 17 C.F.R. § 160.1-160.9 (2021); Video Privacy Protection Act of 1988, Pub. L. No. 100-619 (1988) (codified at 18 U.S.C. § 2710).

44. *See* HOOFNAGLE, *supra* note 16, at 75 (noting that the FTC was "poised to fill the legal gaps between sectoral privacy statutes, tort, and privacy promises" as Congress had left many gaps in privacy law protections).

45. Federal Trade Commission Act of 1914 § 5, 15 U.S.C. § 45(a)(2) (2018); MULLIGAN & LINEBAUGH, *supra* note 41, at 30-35; HOOFNAGLE, *supra* note 16, at 119-41.

46. *See* HOOFNAGLE, *supra* note 16, at 131.

47. Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, § 202, 88 Stat. 2183, 2193-95 (1975); Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, §§ 7-12, 15, 21, 94 Stat. 374, 376-80, 388-90, 393-96; Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, sec. 9, § 5(n), 108 Stat. 1691, 1695 (codified at 15 U.S.C. § 45(n)).

formal rulemaking[48] outside of particular areas where Congress has empowered it to engage in a more streamlined process.[49]

Accordingly, the FTC has relied largely on its investigative and enforcement powers,[50] but these too are limited. It lacks broad authority to impose financial sanctions or injunctive relief.[51] Moreover, the FTC Act's definition of "unfair" excuses an act or practice unless it causes "substantial injury to consumers which is not reasonably avoidable by consumers themselves."[52] This leaves open arguments that injuries are not substantial or could be avoided, such as by clicking to "opt out" of a proposed use of one's private information. The FTC likewise interprets "deceptive" to mean acts or practices that would mislead reasonable consumers in a material way to their detriment,[53] providing a defense that any consumer harm is immaterial or that *reasonable* consumers would not be fooled by a given practice.[54]

Despite these limitations, the FTC retains considerable power to stop ongoing abuses in the realm of privacy. It can investigate and sue companies engaged in prohibited practices. Indeed, it pursued numerous companies for inadequate data-protection practices.[55] Its complaints usually lead to widely publicized settlements that require companies to pay fines or restitution and to submit to lengthy—sometimes decades-long—and expensive monitoring regimes.[56] The FTC affects not only the targets of enforcement but also the many other companies who wish to avoid becoming targets.[57] Privacy experts

48. *See* HOOFNAGLE, *supra* note 16, at 56 ("Burdensome procedures is one of the main reasons why the FTC has not sought to promulgate rules for privacy—the thought is that by the time the procedures are satisfied, any privacy rule would be out of date."); Waldman, *supra* note 5, at 828-29 (discussing the FTC's lack of rulemaking).

49. *See, e.g.*, COPPA, 15 U.S.C. §§ 6501-6506 (2018).

50. *See* HOOFNAGLE, *supra* note 16, at 98-107. Recently, the FTC has indicated increased interest in rulemaking, including in the privacy sphere. *See, e.g.*, 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.).

51. *See, e.g.*, 15 U.S.C. § 57b (2018) (imposing procedural requirements on the FTC's seeking monetary damages); AMG Cap. Mgmt. v. FTC, 141 S. Ct. 1341 (2021) (determining that the FTC lacks ability to pursue monetary recoveries under general "equitable" theories); FTC v. Advocare Int'l, L.P., No. 19-CV-715, 2020 WL 6741968, at *3-6 (E.D. Tex. Nov. 16, 2020) (holding that the FTC lacks authority to seek injunctive relief where wrongdoing has ceased and there is no specific "reason to believe" it will be repeated).

52. 15 U.S.C. § 45(n) (2018).

53. *See FTC Policy Statement on Deception*, FED. TRADE COMM'N (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/EYD4-47DE].

54. To be fair, the FTC has taken the view that if a practice injures "a significant minority of reasonable consumers," it could be considered deceptive. POM Wonderful, LLC v. FTC, 777 F.3d 478, 490 (D.C. Cir. 2015) (quoting *In re* Telebrands Corp., 140 F.T.C. 278, 291 (2005)); *see also* HOOFNAGLE, *supra* note 16, at 125-26 (discussing the test); Firestone Tire & Rubber Co. v. FTC, 481 F.2d 246, 249 (6th Cir. 1973) (indicating that 10-15% of the "buying public" might be sufficient to sustain a cause of action).

55. *See* HOOFNAGLE, *supra* note 16, at 98-99; Solove & Hartzog, *supra* note 19, at 598-99.

56. *See* HOOFNAGLE, *supra* note 16, at 98-99; Solove & Hartzog, *supra* note 19, at 606 (noting that auditing frequently lasts more than twenty years).

57. *See, e.g.*, Bamberger & Mulligan, *supra* note 9, at 274 (quoting a corporate privacy officer as "describ[ing] the threat of FTC oversight as a motivating 'Three-Mile Island' scenario").

scrutinize these complaints, settlement documents, and accompanying statements, which effectively constitute the "common law of privacy."[58] The FTC also deploys a sizeable staff, including expert lawyers and economists, to analyze areas of concern, make policy statements, issue warning letters, and take other informal actions, all of which outline the general principles of privacy law as the FTC understands them.[59]

Thus, the FTC has put general principles of privacy law in place, but the law takes a diffuse and scattered form.[60] In most areas, the rules of federal privacy law derive from a patchwork of statements, consent decrees, and other documents interpreting the FTC Act.[61] For many disputed or borderline cases, the regime remains more a set of standards and rough guidelines than a set of legal rules that can be applied with certainty or relied upon to protect consumer privacy.

2. The Notice and Choice Model

Historically, the "notice and choice" paradigm has been the centerpiece of privacy regulation, and it still plays an important role in privacy law.[62] Under this model, regulators focus on whether companies abide by promises they make to consumers, and disclosure, coupled with an opportunity for consumer consent, cleanses most practices.

Consent is thought of as coming in two flavors, "opt-out" and "opt-in."[63] In an *opt-out* arrangement, consumers are deemed to consent unless they take an affirmative step to object to data privacy practices. The *opt-in* standard is more strict: consumers must take some action to accept or invite the proposed uses of their information. Consumers prefer opt-in regimes, but companies have resisted them, and opt-out remains dominant.[64]

The lived reality of these standards is more complicated than this simple rubric suggests; the distinction can become quite blurred, and each standard has gradations.[65] For instance, while the opt-in standard is sometimes treated as a gold standard for consent, an opt-in can take the form of simply clicking "I agree

58. Solove & Hartzog, *supra* note 19, at 606-08 (noting the great attention paid by privacy experts to "every FTC consent order" along with its other privacy-related writings).

59. *See id.* at 625-26 (describing some of these materials as "soft law").

60. *See* HOOFNAGLE, *supra* note 16, at 145 (stating that the "FTC has been a key force for the protection of online privacy because it fills the gaps left by the US 'sectoral' regulatory approach").

61. *See* Solove & Hartzog, *supra* note 19, at 606-27. To be sure, there are a range of egregious behaviors that are clearly unlawful under governing sector-specific laws and under criminal laws. *See, e.g.*, *id.* at 643-48 (describing FTC actions under some "sectoral" regimes); *id.* at 655-56 (describing HIPAA as "one of the most specific data security laws"). But the coverage of these laws is limited.

62. The FTC's approach was guided by "fair information practices." *See* HOOFNAGLE, *supra* note 16, at 152-53; Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882-83 (2013).

63. *See* Solove, *supra* note 62, at 1898-99.

64. *See* HOOFNAGLE, *supra* note 16, at 236-40, 296-97.

65. *See, e.g.*, Fracassi & Magnuson, *supra* note 5, at 374 (posing hypotheticals concerning the limits of consent).

to these terms and conditions," a statement characterized as "the biggest lie on the Internet" because nearly no one reads or understands the terms and conditions to which they are supposedly agreeing.[66] In addition, privacy terms to which the consumer "agrees" are often bundled with other terms and services or are presented to make "opting in" all but inevitable.[67]

The laissez-faire notice-and-choice approach to privacy regulation focuses on ensuring that companies disclose their data-protection practices and honor those promises. A contractual paradigm underpins the approach: the consumer and the company have reached an agreement—often implicit, not actual, since consumers rarely know the terms of service and privacy policies—and the agreement should be enforced.[68] Even if this paradigm would be sufficient to govern relations between consumers and companies, it would be no panacea because the agreement rarely governs every use of private data. Data merchants, criminal actors, credit reporting agencies, and many others often acquire private data without any real possibility of consumer consent.[69] Still, within its proper scope, a consent regime can be a powerful tool for shaping privacy principles in accordance with individual preferences, without inhibiting commerce through over-regulation or forcing consumers with heterogenous preferences into a one-size-fits-all regime.[70]

Merchants' reputational interests offer an additional justification for privileging consent in the law of privacy.[71] Proponents of a consent-based approach argue that companies can generally be trusted to honor their word, rather than manipulate consumers and risk their relations with existing customers

66. Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO., COMMC'N & SOC'Y 128, 129 (2020); *id.* at 140-42 (summarizing findings that support the conclusion that terms of service and privacy policies provide little effective notice); Fracassi & Magnuson, *supra* note 5, at 374 ("The problem . . . is that it is remarkably easy to get consumers to consent to anything on the internet.").

67. *See* Solove, *supra* note 62, at 1898 ("[M]any organizations will have the sophistication and motivation to find ways to generate high opt-in rates. They can do so simply by conditioning products, services, or access on opting in. . . . [A]greeing to clickwrap contracts and end-user license agreements is often a prerequisite for obtaining access to a website or to use a product or service."). Thus, weak-form opt-in requirements largely differentiate only between active and inactive users; they hinder "cold-contacting" of inactive consumers. *See, e.g.*, Michael E. State & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 DUKE L.J. 745, 766-67 (2003). Consent can usually be obtained from active customers by obtaining a clicked "agreement" at some point. Some jurisdictions apply higher and more refined standards of consent. *See, e.g.*, Richards & Hartzog, supra note 5, at 1472 ("Consent within Europe's data protection frameworks is more rigorous than in parts of US privacy law.").

68. *See* Stephanos A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 606-11 (1994).

69. This is described as the "third-party problem." *See, e.g.*, HOOFNAGLE, *supra* note 16, at 146-47.

70. *See* Fracassi & Magnuson, *supra* note 5, at 375-76; Bibas, *supra* note 68, at 609-11.

71. Bamberger & Mulligan, *supra* note 9, at 280 (quoting a privacy officer as commenting, "[t]he biggest value to privacy is it's a part of brand"); HOOFNAGLE, *supra* note 16, at 166 (noting the "tremendous public relations cost of FTC enforcement actions"); *see also infra* Section II.B.6 (Reputation as Protection).

or their ability to attract future customers.[72] This constraint is not necessarily sufficient on its own to protect consumers,[73] and it is unlikely to play any role in constraining companies that are not consumer-facing and do not rely on good public image. The most important example of such actors are data or information brokers.[74] Commercial data brokers are companies whose business is the aggregation, analysis, and sharing of personal information about individuals.[75] The reach and detail of the data they possess is astonishing; they are poorly regulated; and, largely lacking direct relationships with the individuals whose data they hold, they have little incentive to care about the impact of their activities on consumer well-being.[76]

In any case, despite these limitations, reputational constraints play a role in evaluating privacy regulation.

3. Modern Privacy Law Beyond Notice and Choice

The notice-and-choice model has held considerable sway. Yet this consent-based approach fits poorly with privacy regulation, as a growing body of scholarship has made clear.[77] The degree to which more substantive norms should be superimposed on the notice-and-choice framework has become one of the most important questions in modern privacy law.[78]

The problems with the notice-and-choice model can be summarized as follows. First, the consent obtained from consumers in most technical settings is superficial at best. Consumers do not read privacy policies and other agreements,

72. *See* HOOFNAGLE, *supra* note 16, at 166. Protecting privacy from perceived encroachments has been characterized as a way of building reputation as well. *See, e.g.*, Klint Finley, *Apple's Noble Stand Against the FBI Is Also Great Business*, WIRED (Feb. 17, 2016, 9:24PM), http://www.wired.com/2016/02/apples-noble-stand-against-the-fbi-is-also-great-business/ [https://perma.cc/9BDX-XYKP]; Will Oremus, *Irate DOJ Dismisses Apple's Fight with the FBI as a "Brand Marketing Strategy,"* SLATE (Feb. 19, 2016, 6:02 PM), https://www.slate.com/blogs/future_tense/2016/02/19/department_of_justice_motion_mocks_apple_s_fbi_fight_as_a_brand_marketing.html [https://perma.cc/KM5L-G5SS].

73. *See* Willis, *supra* note 5, at 152-53 (casting doubt on the sufficiency of reputational constraints). *See generally* Yonathan A. Arbel, *Reputation Failure: The Limits of Market Discipline in Consumer Markets*, 54 WAKE FOREST L. REV. 1239 (2019) (same).

74. *See* HOOFNAGLE, *supra* note 16, at 146-47.

75. McKay Cunningham, *Exposed*, 2019 MICH. ST. L. REV. 375, 395-403; Amy J. Schmitz, *Secret Consumer Scores and Segmentations: Separating "Haves" from "Have-Nots,"* 2014 MICH. ST. L. REV. 1411, 1419-25; Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 362-64.

76. HOOFNAGLE, *supra* note 16, at 146-47; Douglas MacMillan, *Data Brokers Are Selling Your Secrets. How States Are Trying to Stop Them*, WASH. POST (June 24, 2019, 5:54 p.m. EDT), https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them/ [https://perma.cc/MPE5-WTTR]; FEDERAL TRADE COMMISSION, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014).

77. *See, e.g.*, Elizabeth Edenberg & Meg Leta Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, 21 NEW MEDIA & SOC'Y 1804, 1804-05 (2019); Woodrow Hartzog & Neil Richards, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1197-98 (2017); Elvy, *supra* note 28, at 486 n.324 (collecting sources).

78. *See, e.g.*, Richards & Hartzog, *supra* note 5, at 1500-02; Fracassi & Magnuson, *supra* note 5, at 373-76 (noting difficulties of the consent model and proposing guidelines for an effective consent regime).

and there is no realistic way to change this.[79] Traditional notions of consent to terms arrived at through bargaining and a "meeting of the minds" cannot be fitted well to modern consumer contracting practices.[80]

Second, even when key terms are sufficiently conspicuous, consumers do not understand the full ramifications of those terms.[81] They overestimate the degree to which their privacy will be protected.[82] For instance, they assume that existing regulations backstop privacy agreements more than they do.[83] They do not understand the breadth of the information being collected or the ease with which it can be shared and used to identify them (even if supposedly anonymized).[84] Or they fail to understand that small and seemingly innocuous pieces of information can be assembled to form a detailed portrait of intimate aspects of individual identity and behavior.[85]

Third, consumers may have little choice but to consent to terms offered them by merchants whose services are essentially ubiquitous in modern life.[86] Children using school computers, employees using devices for work, and patients accessing health services are often required to consent to policies without any true chance to refuse.[87]

Fourth, one individual's consent affects the privacy of those who have not consented. Data about one individual often reveals information about others. Consent might be beneficial to an individual consumer but detrimental to others or to society as a whole.[88]

---

79. *See, e.g.*, Bamberger & Mulligan, *supra* note 9, at 297.

80. *See* Dee Pridgen, *ALI's Proposed Restatement of Consumer Contracts—Perpetuating a Legal Fiction?*, CONSUMER L. & POL'Y BLOG (June 8, 2016, 4:00 PM ET), https://pubcit.typepad.com/clpblog/2016/06/dee-pridgens-important-guest-post-update-on-the-alis-proposed-restatement-of-consumer-contracts-will.html [https://perma.cc/7DDR-QJDT].

81. *See* Elvy, *supra* note 28, at 445 (providing an example of connections between wearable tech devices and social media apps).

82. *See, e.g.*, Willis, *supra* note 5, at 132-42; Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, 80 U. CHI. L. REV. 1155, 1164-65 (2013).

83. *See, e.g.*, HOOFNAGLE, *supra* note 16, at 293 (noting that with respect to privacy notices for financial institutions, "the basic problem remains that regardless of clarity of notices, most Americans think their banks cannot sell personal information").

84. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Elvy, *supra* note 28, at 446-47; Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703 (2016).

85. *See, e.g.*, Benjamin Wittes & Wells C. Bennett, *Databuse and a Trusteeship Model of Consumer Protection in the Big Data Era*, BROOKINGS INST. 4-5 (June 2014), https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Bennett_Databuse.pdf [https://perma.cc/8D4H-7GUN] (noting that consumers "often give . . . information away with the understanding, implicit or explicit, that it will be aggregated and mined for what it might say about us").

86. *See, e.g.*, Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 248-49 (2007).

87. *See id.* at 286 & n.264.

88. *See* Viljoen, *supra* note 5, at 573 (advancing "a theoretical account of data as social relations"); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989) (connecting the protection of privacy's social value to tort-law principles). *See generally* ANITA L. ALLEN, UNPOPULAR PRIVACY (2011) (emphasizing the collective and social benefits of privacy); PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995) (discussing common, public, and collective aspects of the social value of privacy).

Finally, there is the problem of modification. Policies often include a unilateral right to change the policy merely by posting new terms on the company's website.[89] If consumers consent prior to the change, they might feel "locked in" to the business such that even in the unlikely event that they became aware of the change, the cost of switching to another provider would be less desirable than accepting the revision.[90]

In sum, the notice-and-choice model can be easily exploited by the companies collecting consumer data. They are repeat players with advantages over consumers. They can draft broad policies from the start, or narrow policies with liberal rights of amendment. Whichever path they choose, they can call these "privacy policies," knowing that consumers will assume they are more protected than they are,[91] and that they would underestimate the likelihood of harm even if they were aware of the terms.[92]

Due in part to these objections, the role of consent in the realm of privacy has diminished over time.[93] As one leading privacy expert writes, "[i]t is no longer the case that companies can simply point to a privacy policy and justify any kind of data practice."[94] The FTC has brought actions against companies for "deceptive" or "unfair" practices based on consumer expectations, industry standards, and public policy.[95] For instance, the FTC deems practices unlawful if they are not disclosed with sufficient conspicuousness in light of their cost to privacy[96] or if they are sought to be imposed retroactively.[97] Likewise, the FTC imposes a duty on companies to observe "reasonable" security practices to protect consumer information once it has been gathered.[98]

In sum, privacy law appears increasingly to be shifting from a focus on procedural compliance with rudimentary disclosure norms to "a substantive measure: the vindication of consumer expectations regarding the treatment of

89. *See* Elvy, *supra* note 28, at 482.

90. In addition, companies sometimes try to make the changes retroactive, so that no consent would be necessary at all. The FTC has attacked such practices. *See infra* notes 218-223.

91. *See, e.g.*, Waldman, *supra* note 5, at 811 n.239; Janger, *supra* note 28, at 1875 ("Although some privacy policies contain a promise of confidentiality, many, if not most, would be better described as data disclosure policies . . . .").

92. *See supra* notes 81-85 and accompanying text.

93. *See* Bamberger & Mulligan, *supra* note 9, at 296, 300-02; Solove & Hartzog, *supra* note 19, at 667-72.

94. HOOFNAGLE, *supra* note 16, at 146; Bamberger & Mulligan, *supra* note 9, at 296 (noting that "while the FTC's early actions focused on enforcing the bargains between individuals and corporations—regardless of their content—later actions found certain practices to be unreasonable regardless of individual 'consent' by means of the standard click-wrap processes generally upheld by courts").

95. *See* Solove & Hartzog, *supra* note 19, at 628, 638-40, 667-69.

96. *See* Solove & Hartzog, *supra* note 19, at 634-36 (discussing regulatory actions based on an insufficient notice of privacy-related business practices).

97. *See* HOOFNAGLE, *supra* note 16, at 165.

98. *See, e.g.*, HOOFNAGLE, *supra* note 16, at 217.

personal information."[99] The fine-print disclosures do not govern on their own. Consumer expectations are established by the overall practical impressions formed across their entire interaction with a company, and their background assumptions and beliefs, which likely include overarching substantive norms concerning how reasonable companies will protect or use data. The introduction of more substantive standards requires regulatory guidance to evolve alongside data-related business practices[100] and concrete examples that flesh out these standards on an ongoing basis. The transition to this more substantive model remains incomplete and contested, but as explained below, the data in this Article provides reason to believe that a shift has occurred and could affect a wide swath of cases.

B. Privacy Law in Action

In addition to uncertainties in the content of the law, privacy law presents challenges of enforcement. Legal doctrine helps foster a climate of impunity, stacking the odds against effective enforcement of consumers' rights in their private information. Experts have argued that neither tort law nor existing regulatory sanctions provide adequate remedies to deter data protection related abuses.[101] They claim that lawmakers, including legislators, regulators, and courts, have failed to understand the nature of the dangers presented to consumers both as individuals and collectively,[102] and accordingly, they have relied on outdated notions of harm to bar plaintiffs from bringing claims.[103] Once a party obtains lawful possession of consumers' data, it is usually governed by a liability and not a property regime.[104] In essence, if someone misuses or transfers data without authorization, the remedy sounds in contract or negligence law, or under consumer protection regulations, but not as conversion or theft.[105]

---

99. Bamberger & Mulligan, *supra* note 9, at 295; Solove & Hartzog, *supra* note 19, at 628 (describing the FTC as having developed "a more holistic and robust theory of privacy-related deception" that "considers the entirety of a company's dealings with the consumer, not just the specific promises made in the company's privacy policy"). Privacy law has, in other words, "evolved into a law of unwelcome consumer surprise." HOOFNAGLE, *supra* note 16, at 146.

100. HOOFNAGLE, *supra* note 16, at 120 (summarizing the opinion of FTC attorneys that Section 5 "cannot be defined in terms of constants . . . . [I]t is a recognition of an ever-evolving commercial dexterity and the personal impact of economic power as important dimensions of trade").

101. *See, e.g.*, Neil M. Richards, *The Limits of Tort Privacy*, 9 J. ON TELECOMM. & HIGH TECH. L. 357 (2011); Citron, *supra* note 86, at 246-60.

102. *See* Citron, *supra* note 86, at 255-61.

103. *See, e.g.*, Solove & Citron, *supra* note 5 (arguing that the issue of harm has confounded courts in data-breach lawsuits). On the importance of private rights of action for privacy violations, see generally Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639 (2022).

104. *See, e.g.*, Janger, *supra* note 10, at 908-14.

105. *See* Janger, *supra* note 10, at 914 ("Where an entitlement is protected by a liability rule, the defendant may choose to violate the right and pay damages . . . . [Granting a property right] changes the order of this interaction. Either through criminal sanction, affirmative judicial order, or prohibitively high (and/or punitive) fines, a property rule makes a non-consensual taking infeasible."); HOOFNAGLE, *supra* note 16, at 355 (noting lack of common-law remedies); *id.* at 343 ("Lawyers representing

Again, the notion of consent is relevant and problematic. The legal regime seems predicated on the principle that when consumers consent to sharing information with a company, they consent to transferring *ownership* (albeit shared ownership) of that information to the company.[106] But consumers may view themselves as sharing information for a circumscribed and temporary use only, more akin to a narrow license of the information than to a broad transfer of ownership.[107] Privacy policies often encourage this conception by couching their promises as circumscribing what the company will do with "your information." Consumers might understand such policies as recognizing that the underlying information remains *theirs*—their property—giving at best a short-term lease or a limited license to the company. The law may lag behind consumer expectations in this respect.

Practically speaking, even if the law were to provide serious sanctions, enforcement would likely be ineffective given the realities of data storage. Information is often held in the form of a spreadsheet or database and could be transferred untraceably, by a thumb drive or by an encrypted message on a mobile app.[108] Once transferred, unless it includes purchase or browsing history or some other information specific to a particular merchant, it cannot effectively be traced back to its source.[109] Holders of data can usually share or transfer data undetectably and with impunity.[110]

Another limitation of the current enforcement regime is that data harm is diffused over many customers, whereas benefits are concentrated on the violator. No individual consumer is likely to have the motivation to invest the time and money to investigate and seek legal redress for a breach. Collective remedies such as class actions are expensive and their availability is limited.[111] Regulators can bring enforcement actions, but their resources are constrained and investigations are often initiated only by complaints, which consumers lack awareness or incentive to bring. In addition, some regulators may be reluctant to intervene in what they perceive as a private matter between companies and consumers.[112]

information-industry companies argue for a return to the common law, but, in so doing, they cherry-pick from history. These lawyers do not, for instance, argue to reinvigorate the idea that difficult-to-detect frauds on the public should be criminally punished."); Citron, *supra* note 86 (arguing based on historical common-law analogies for stronger legal responses to abusive data-related business practices); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614 (2018) (describing current tort law on privacy and advocating for strict liability).

106. *See* Magnuson, *supra* note 13, at 60-63.

107. *See, e.g.*, Elvy, *supra* note 28, at 508.

108. *See* Magnuson, *supra* note 13, at 40-41.

109. *See* HOOFNAGLE, *supra* note 16, at 223.

110. *See* Magnuson, *supra* note 13, at 40-41; HOOFNAGLE, *supra* note 16, at 223.

111. *See* Janger, *supra* note 10, at 910-11.

112. *See, e.g.*, HOOFNAGLE, *supra* note 16, at 148-49 (discussing the FTC's traditional "privacy control approach").

As mentioned above, the reputational risk of being known as a violator of privacy is sometimes thought to keep companies in line.[113] Some might argue that stronger sanctions will bring unnecessary risks to merchants who generally seek in good faith to serve customers' interests. It is true that reputational constraints may provide some consumer protection, mitigating some of the risks of underenforcement. But the ease with which transfers can be accomplished without detection lowers the plausibility of any reputation-based optimism in the realm of privacy protection.[114]

As Part III explains, the data presented in this Article speaks to the problem of enforcement of privacy law. It suggests that regimes such as the consumer privacy ombudsman may effectively deter at least some unlawful transactions in consumer data, but that ultimately, without stronger and clearer laws and remedies for breach of those laws, protection will remain weak and inconsistent.

C. The Sale of Consumer Information and the Origins of the Privacy Ombud

> When you register with toysmart.com, you can rest assured that your information will never be shared with a third party.
> – Toysmart.com's Privacy Policy[115]

Toysmart.com was an internet toy retailer that took off in the boom times of the late 1990s.[116] Disney acquired a majority stake in August 1999 and Toysmart seemed poised to soar, but like many other products of that era's dot-com bubble, it went bust.[117] By May 2000, it was preparing to liquidate its assets.[118] It placed ads in prominent newspapers and on its website offering to sell, among other things, the information that it had collected about its customers—in some cases information from or about children.[119] Reports

113. *See supra* notes 71-74 and accompanying text; *infra* Section II.B.6 (Reputation as Protection).

114. *See supra* notes 109-110 and accompanying text.

115. Toysmart.com, Privacy Policy, attached as Ex. 1 to Stipulation and Order Establishing Conditions on Sale of Customer Information [hereinafter *Toysmart* Stipulation], attached as Ex. A to Motion to Approve Stipulation with Federal Trade Commission and for Authority to Enter into Consent Agreement, *In re* Toysmart.com, No. 00-13995 (Bankr. D. Mass. July 20, 2000), ECF No. 113 [hereinafter *Toysmart* Motion]. The stipulation is available in full at *Stipulation and Order Establishing Conditions on Sale of Customer Information in* In re *Toysmart.com*, FTC (July 20, 2000), https://www.ftc.gov/sites/default/files/documents/cases/toysmarttbankruptcy.1.htm [https://perma.cc/BP7V-62LF].

116. *See* William M. Bulkeley, Joseph Pereira & Bruce Orwall, *Toysmart, Disney Deal Hit Snags in a Web of Conflicting Goals*, WALL ST. J. (June 7, 2000), https://www.wsj.com/articles/SB960327605839275507 [https://perma.cc/HX2E-LLQD].

117. *See id.*

118. *See Toysmart* Stipulation, *supra* note 115; Complaint at ¶ 10, Fed. Trade Comm'n v. Toysmart.com, No. 00-11341 (D. Mass. July 10, 2000) [hereinafter *Toysmart* Complaint], https://www.ftc.gov/sites/default/files/documents/cases/toysmartcomplaint.htm [https://perma.cc/H7JN-HZAT].

119. *See Toysmart* Stipulation, *supra* note 115; *Toysmart* Complaint, *supra* note 118, ¶¶ 19-20; Matt Richtel, *F.T.C. Moves to Halt Sale of Database at Toysmart*, N.Y. TIMES (July 11, 2000), https://www.nytimes.com/2000/07/11/business/ftc-moves-to-halt-sale-of-database-at-toysmart.html [https://perma.cc/B63W-7EFS].

indicated that the personal information of approximately 190,000 customers was on offer.[120]

Notably, Toysmart invested heavily in customer acquisition. The *Wall Street Journal* reported that by the end of 1999, "Toysmart was spending nearly $200 for each customer acquired, and those customers were spending only $44 each."[121] Having paid so extravagantly to obtain their customers, it is unsurprising that Toysmart—and its majority owner, Disney[122]—wanted to see some return on that investment. Shortly after Toysmart began its liquidation efforts, it ended up in bankruptcy[123] and sought bankruptcy-court approval of the asset sale.[124] But Toysmart's privacy policy contained expansive promises that it would not transfer customer information to others.[125] In a headline-grabbing lawsuit, the FTC sought to enjoin the sale of consumer data on the grounds that the sale constituted an "unfair or deceptive act or practice" in light of the privacy policy and the background law of consumer protection.[126]

Less than two weeks after the FTC filed its lawsuit, Toysmart and the FTC announced an agreement and filed it with the bankruptcy court for approval.[127] Under the agreement, Toysmart could sell the data, but only to a "qualified buyer": a company in the same general line of business as Toysmart, which agreed to be bound by Toysmart's privacy policy and to serve as "successor-in-interest" as custodian of that data, and which purchased the data along with more of the company's core assets, such as its name, trademarks, URLs and website content.[128] In addition, any changes the buyer made to the privacy policy would not apply to customer information acquired prior to the change unless the customer opted into the new policy after receiving notice of it.

The idea behind the "qualified buyer" framework is that the sale of data as part of the overall sale of the relevant line of business doesn't threaten consumer privacy in the same way as a stand-alone sale or licensing of data to a "true" third party.[129] The data is still only held by one party—the buyer who "'stands' in the

120. *See* Michael Brick, *Judge Overturns Deal on Sale of Online Customer Database*, N.Y. TIMES (Aug. 18, 2000), www.nytimes.com/library/tech/00/08/biztech/articles/18toys.html [https://perma.cc/B63W-7EFS].

121. Bulkeley et al., *supra* note 116.

122. In particular, its creditors filed an involuntary bankruptcy petition against it, and Toysmart subsequently consented to staying in bankruptcy. Brick, *supra* note 120.

123. *See Toysmart* Stipulation, *supra* note 115.

124. *See id.*

125. *See* Privacy Statement, Ex. 1 to *Toysmart* Stipulation, *supra* note 115.

126. *Toysmart* Complaint, *supra* note 118; *see* Richtel, *supra* note 119. The proposed sale appears to have come to the attention of regulators due to the fact that Toysmart had participated in the program of a "privacy seal service" by the name of Trust-e, which entitled it to display Trust-e's seal of approval because it abided by certain consumer-protective policies. Janger, *supra* note 28, at 1820. The proposed sale violated those promises to consumers, drew Trust-e's ire, and caused it to report the violation to the FTC. *Id.*

127. *See Toysmart* Motion, *supra* note 115.

128. *Toysmart* Stipulation, *supra* note 115.

129. *See* Letter from Jessica L. Rich, Dir. of Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka 5 (May 16, 2015), https://www.ftc.gov/system/files/documents/public_statements

shoes" of the original party—and will be used in the same general way as it was when the consumer agreed to provide it.[130] Sale of data as part of a "qualified buyer" transaction can be analogized in its privacy impact to the sale of the company's equity to a new owner, which would not generally violate a privacy policy (even a strict one that prohibits transfer of data to a third party). Thus, the qualified-buyer framework is a sort of "realist" interpretation of the terms of a privacy policy, excusing strict compliance on grounds that the transfer conforms with the overall substance of consumer expectations.

As Part III of this Article shows, the qualified-buyer framework has now become the dominant approach to data sales by failing companies. But in *Toysmart*, the agreement didn't end the controversy. Two of the five FTC commissioners dissented from the settlement, asserting that because of the absolute language in the privacy policies, Toysmart should have to obtain customer consent to transfer the assets.[131] The attorneys general of no fewer than forty-four states filed an objection with the court, arguing that Toysmart should only be allowed to sell the information of customers who affirmatively opted in to the transfer.[132] The bankruptcy judge refused to throw Toysmart a line; she reserved judgment on approval of the FTC-Toysmart settlement, opting to let the auction proceed and to consider approval if and when there was an actual bidder before her.[133]

/643291/150518radioshackletter.pdf [https://perma.cc/QH29-NRWX] (defending the "qualified buyer" framework because it "protect[s] consumer interests by ensuring that the data would be used consistent with Toysmart's promises by an entity that was essentially operating as a new owner of the business, as opposed to a 'third party' who was merely the highest bidder in a winner-take-all auction that may not have a reputational interest in handling the information in the same manner"). Frejka was ombud in the RadioShack bankruptcy case, and Rich was Director of the FTC's Bureau of Consumer Protection. *Id.* at 1.

130. *See Statement of Commissioner Mozelle W. Thompson,* Toysmart.com*, File No. X00 0075*, FED. TRADE COMM'N (July 21, 2000), https://www.ftc.gov/sites/default/files/documents/cases/toysamrtthompsonstatement.htm [https://perma.cc/K7UQ-3C8D].

131. *See Statement of Commissioner Sheila F. Anthony,* Toysmart.com, Inc. *File No. X00 0075*, FED. TRADE COMM'N (July 21, 2000), https://www.ftc.gov/sites/default/files/documents/cases/toysmartanthonystatement.htm [https://perma.cc/A9TJ-MXSW]; *Dissenting Statement of Commissioner Orson Swindle in* Toysmart.com, Inc.*, File No. X00 0075,* FED. TRADE COMM'N (July 21, 2000), https://www.ftc.gov/sites/default/files/documents/cases/toysmartswindlestatement_0.htm [https://perma.cc/RA5W-W4JM]. Oddly, although the issue was a well-known one by that point, neither of these dissenting statements clarifies whether an "opt-out" opportunity prior to sale would suffice or whether customers would have to opt in to the transfer. Even one of the commissioners who approved the settlement promulgated a separate statement expressing a "reservation" about the agreement, noting he thought "that consumers would benefit from notice and choice before a company transfers their information to a corporate successor." That commissioner would have preferred to impose an opt-out requirement. *Statement of Commissioner Mozelle W. Thompson*, *supra* note 130.

132. *See* Objection of the Commonwealth of Massachusetts and 46 States to the Debtor's Motion to Approve Settlement with Federal Trade Commission and for Authority to Enter into Consent Agreement at 1-2, 6-7, *In re* Toysmart.com, LLC, No. 00-13995 (Bankr. D. Mass. Aug. 3, 2000), ECF No. 180. The attorneys general of the District of Columbia, the Northern Mariana Islands, and the U.S. Virgin Islands also joined the objection. *Id.* at 1 n.1.

133. *See Bankruptcy Judge Passes on Toysmart*, N.Y. TIMES (Aug. 17, 2000), https://www.nytimes.com/2000/08/17/continuous/bankruptcy-judge-passes-on-toysmartcom.html [https://perma.cc/3F4W-QGDL].

The auction failed. Toysmart's attorney claimed the contentious atmosphere deterred bidders: "No one wanted to walk into a lawsuit."[134] Ultimately, Toysmart proposed to allow a subsidiary of its majority owner, Disney, to pay $50,000 to have the information destroyed.[135] Disney's motivation, presumably, was to "do the right thing" and mitigate its reputational damage. Toysmart noted that it had received no firm bids higher than Disney's. It had received a "preliminary proposal" for $100,000, but in light of the anticipated objections and the associated delays and costs of "overcoming such opposition," the higher bid wasn't worth pursuing.[136] The court approved the destruction of the records.[137]

Toysmart amounted to a very visible debacle for all involved.[138] At the end of the day, the assets went unsold, the public was outraged, the various regulators sharply disagreed, and the law remained unclear. *Toysmart* would hardly be expected to form a major part of the story of privacy law. Yet its effects continue to reverberate throughout privacy law.

Around the time that *Toysmart* was grabbing headlines, Congress was considering major revisions to the Bankruptcy Code.[139] The uproar over *Toysmart* prompted a change to the law intended to raise the protections for consumers whose information is for sale. The law generally provides that if consumers' "personally identifiable information"[140] is going to be sold in a bankruptcy[141] and that sale would violate an existing privacy policy, then an ombud must be appointed "to assist the court in its consideration of the facts, circumstances, and conditions of the proposed sale."[142] The ombud is chosen by the U.S. Trustee, a Department of Justice appointee known as the "bankruptcy watchdog."[143] After the ombud reports back, the court must decide whether to

134. *Id.*

135. *See* Motion by Debtor to Destroy Customer Information ¶¶ 12-13, *In re* Toysmart.com, LLC, No. 00-13995 (Bankr. D. Mass. Jan. 10, 2001), ECF No. 313; Victoria Shannon, *Tech Brief: Toysmart Paid Off*, INT'L HERALD TRIB. (Jan. 11, 2001), https://www.nytimes.com/2001/01/11/business/worldbusiness/IHT-tech-brieftoysmart-paid-off.html [https://perma.cc/PTD5-29JR].

136. Motion by Debtor to Destroy, *supra* note 135, ¶¶ 19-21.

137. *See* Handwritten Order Granting Motion by Debtor to Destroy Customer Information, *In re* Toysmart.com, LLC, No. 00-13995 (Bankr. D. Mass. Jan. 25, 2001), ECF No. 325.

138. Perhaps with some exceptions: in true Silicon Valley fashion, Toysmart's CEO pivoted shortly thereafter to a new company, a well-funded online ticket-scalping venture based in Beverly Hills, called RazorGator. Robert Johnson, *A Dot-Com Die Hard*, N.Y. TIMES (Apr. 14, 2005), https://www.nytimes.com/2005/08/14/business/yourmoney/a-dotcom-diehard.html [https://perma.cc/E3CP-HWP8]. The company apparently lasted about thirteen years. *See* Sean Burns, *Reports: RazorGator Ceases Payments to Brokers, Shuts Doors*, TICKET NEWS (Feb. 27, 2018), https://www.ticketnews.com/2018/02/razorgator-out-of-business/ [https://perma.cc/AWH7-YL6S].

139. Corinne Ball & Jacqueline B. Stuart, *The Battle over Bankruptcy Law for the New Millenium*, 55 BUS. LAW. 1487, 1487-92 (2000).

140. 11 U.S.C. § 101(41A) (2018).

141. *Id.* § 363(b)(1).

142. *Id.* § 332.

143. *See infra* notes 300-309 and accompanying text; *see also, e.g.*, P. Matthew Sutko & Saleela Khanum Salahuddin, *United States Trustees—Bankruptcy Watchdogs and Appellate Advocates*, EXEC. OFF. U.S. TRS. 1 (2008), https://www.justice.gov/archive/ust/articles/docs/2008/abi_200811.pdf [https://perma.cc/7DTQ-ASDQ] (using the term "bankruptcy watchdog").

approve the sale, by "giving due consideration to the facts, circumstances, and conditions of such sale," and by "finding that no showing was made that such sale or such lease would violate applicable nonbankruptcy law."[144]

Congress's intervention did not actually resolve very much. As the *Toysmart* situation revealed, it is not at all clear when a sale of consumer data will or won't "violate applicable nonbankruptcy law." The regulator with the most obvious authority to interpret "applicable nonbankruptcy law," the FTC, had voted to approve the sale in *Toysmart* subject to conditions that fell short of strict compliance with the privacy policy.[145] State authorities, relying on their own state laws, which are also "applicable nonbankruptcy law," disagreed.[146] None of these positions have been litigated to a decision in any court.

Thus, the law remains subject to considerable uncertainty, which ombuds have had to grapple with as they make recommendations in particular cases. In doing so, ombuds have generated a significant body of privacy law: reports in 141 cases presenting expert analyses of privacy law as applied to specific proposed transactions, filed in court proceedings and subject to regulatory oversight. The next Part summarizes the law to be discovered in those reports.

II. A New Body of Consumer Privacy Law

This Part focuses on my empirical study of the consumer privacy law generated by ombuds' reports. My findings show that *Toysmart* motivated the legal regime's creation and provided the basis for most approved transactions, loosely modeled on the FTC settlement. These reports analyze the complex privacy issues arising from the sale of consumers' private data across a wide range of businesses. Section II.A describes the methodology by which these reports were studied, and Section II.B outlines the law of privacy that they present.

A. Structure and Methodology of This Study

This Section describes the study and the data in this Article.[147] Using the Bloomberg Law platform's docket search function, the research team ran broad searches on all U.S. bankruptcy dockets for "Consumer Privacy Ombudsman" and "11 U.S.C. § 332" (the main statutory provision on the appointment of ombuds) from the time the law was passed through July of 2020. This search yielded many false positives.[148] Ultimately, we culled the many hundreds of

144. 11 U.S.C. § 363(b)(1)(B) (2018).

145. *See supra* notes 127-128 and accompanying text.

146. *See supra* note 132 and accompanying text.

147. Having gathered and organized this data with the great help of a number of excellent research assistants, I would be happy to make it available to researchers conducting further work in this area.

148. These search terms were mentioned in passing in a number of cases that were not relevant, for instance those involving somewhat analogous Bankruptcy Code provisions regarding the appointment of a "patient care ombudsman." *See* 11 U.S.C. § 333 (2018).

results and identified dockets in which ombuds (1) were appointed and (2) filed a written report. We omitted cases in which an appointment was sought but denied; cases in which an appointment was made but the ombud never filed a report, usually because a sale fell through; and cases that involved reports that were given only in open court. Later in the process, we also omitted cases in which written reports indicated that no personally identifiable information was proposed for sale. Among these, several reports focused not on evaluating a commercial transaction but on protecting educational or health data to be preserved or disposed of pursuant to sector-specific laws.

Our search was intended to be broad and inclusive, and it appears to have missed few if any qualifying cases. To ensure this, we cross-referenced our body of cases against other sources, including references contained within the reports we analyzed,[149] references on ombuds' resumes, online profiles or other biographical documents, and web search results. These searches yielded several additional cases that were then included in the data set.

Several documents were downloaded from each case in the dataset. We downloaded the order instructing the U.S. Trustee to appoint the ombud, the document reflecting the U.S. Trustee's having done so (and identifying the ombud), the report filed by the ombud, the ombud's fee application, the order approving the ombud's fees, and any attachments to these documents.[150] Although reports were gathered in every case, one or more of the other documents was missing in some cases, whether because it was never filed with the court or because researchers were unable to locate it.[151]

This Article focuses on the ombuds' reports.[152] Sometimes, ombuds file multiple reports. When an ombud files more than one report, the subsequent reports usually either revise or supplement prior reports, based on a change to the proposed sale or because the debtor has multiple lines of business for sale.[153] Ultimately, because partial, preliminary, or supplementary reports analyzed independently might skew the data, it made more sense to analyze all the reports in a given case as a unit, and it is that combined analysis that is reported here.

149. To support their own findings and analysis, ombuds often provide string-citations to other cases in which similar recommendations were made.

150. There is a possibility that some documents were missed in the course of collecting documents. In the electronic filing system used by federal bankruptcy courts, there is considerable but not complete uniformity in how documents are titled and entered on the dockets of various courts by the various actors who submit them.

151. Although electronic filing has been "nearly universal" in federal bankruptcy courts since 2007, *see 25 Years Later, PACER, Electronic Filing Continue to Change Courts*, U.S. CTS. (Dec. 9, 2013), https://www.uscourts.gov/news/2013/12/09/25-years-later-pacer-electronic-filing-continue-change-courts [https://perma.cc/PW7M-RBMR], docket entry practices remain nonuniform across districts, and not all text within filings is accurately searchable.

152. A companion piece, Bradley, *supra* note 29, analyzes ombuds' qualifications and expenses and explores their role within the bankruptcy system in particular.

153. *See, e.g.*, Second Report of the Consumer Privacy Ombudsman at 2, *In re* The Great Atl. & Pac. Tea Co., No. 15-23007 (Bankr. S.D.N.Y. Sept. 11, 2015), ECF No. 872 [hereinafter *Great Atlantic & Pacific* Report].

Thus, the study involved the analysis of 141 cases, in which somewhat more than that number of reports were filed.

Reports were coded for multiple variables. We developed the variables inductively after an initial reading of most of the reports and consideration of the issues relevant to privacy law as a whole. The research protocol and coding practices are on file with the *Yale Journal on Regulation*, along with the resultant data for all variables reported in this Article. The areas of inquiry were as follows:

- Date and length of report, and ombud's name;
- Industry of the debtor in bankruptcy;
- Number of customers whose data was to be sold;
- Sources of information identified as the basis for factual findings;
- Basic characteristics of the consumer information on offer, and whether it included financial, health, child-related, or otherwise sensitive data;
- Whether the report finds that the transfer complies with federal, state, and international law;
- Whether the transfer violated the governing privacy policy;
- The report's sources of law, such as Section 5 of the FTC Act, the *Toysmart* case, and other ombuds' reports;
- Whether the report discusses the debtor's security practices or recordkeeping;
- Whether the involvement of the ombud appears to have affected the course of negotiations (for instance by separating out the privacy assets from the sale of the debtor's other assets or by causing some bidders to withdraw); and
- The content of the recommendations, including:
    - Whether the buyer would have to agree to abide by the seller's old privacy policy, and what process it would have to follow if it sought to modify that policy;
    - Whether the buyer would have to be in the same industry as the seller;
    - Whether the buyer would have to agree to use the information for the same purpose as the seller;
    - Whether notice of the transfer would have to be provided to consumers, and if so, by what method (website, email, physical mail, posting at physical locations, etc.), and whether the form of notice would be provided to or approved by the ombud or another neutral party;
    - Whether consumers would have an explicit right to opt out of the transfer, whether consumers had to opt in to the

transfer, or whether consumers had no right to refuse consent;
- Whether the ombud weighs the value of the data to the bankruptcy estate in crafting the recommendations;
- Whether the report relies on data anonymization to protect consumers' data;
- Where specific bodies of regulation such as HIPAA apply, how these bodies of regulation affect the recommendation;
- Whether the report contains recommendations relating to data security; and
- Whether the transfer of the data is stated to include provision of services only (and not, for instance, marketing).

These variables by no means exhaust the reports' contributions to the law of privacy, but they provide the basis for some conclusions and implications for privacy law, which the rest of the Article presents.

B. The Common Law of Consumer Privacy

This Section traces the basic contours of the law governing the sale of consumers' private information. It seeks to outline some ways in which the reports analyze the issues in sales of private information, both to provide summary data from the reports as a whole and to identify some aspects of the reports that may be worth future research. There is much nuance in the hundreds of pages of reports that is not captured here, but there is also much commonality among reports. Most reports fall into the same general pattern. Remarkably, a thirty-page report analyzing the data of a large public company often ends up in nearly the exact same place as a two-page report concerning a relatively small local business (although of course, the longer report may be more useful for legal research purposes in revealing more of the reasoning behind the decision).

First, this Section provides background concerning the sellers' businesses, the number of consumers affected, and the type of information for sale. Then it outlines the most common privacy recommendations covering the most common scenarios faced by ombuds. Finally, it turns to security and recordkeeping concerns, which tend to be relegated to the margins, if they are discussed at all.

1. Background on Sellers and Proposed Transfers

i. Industry of Seller

Each seller's primary area of business was coded based on information in the reports or, where the reports were not clear, independent online research. Several sellers are difficult to characterize because they straddle more than one

area (such as a health spa that sells clothing in person and through e-commerce). Where businesses seemed to engage in substantial activities in more than one category, they were included in both categories. A summary is presented in Figure 1 below.

Figure 1. Industries of Businesses in Reports

Industry	*Number of Cases*	*Percent of Total*
Total Retail	85	60.3%
General retail	*67*	*47.5%*
Retail and hospitality or services	*2*	*1.4%*
Health-related retail	*9*	*6.4%*
Automotive-related retail	*7*	*5.0%*
Media/technology[154]	15	10.6%
Health-services[155]	13	9.2%
Hospitality	11	7.8%
Financial[156]	10	7.1%
Education	2	1.4%
Other service businesses not included above	8	5.7%

Most notable is the dominance of retail. The sizeable number of health-related and financial businesses is also notable, given the sensitivity of the information held by such businesses. Because this data originates only from the consumer privacy ombudsman regime, it cannot be taken as representative of American businesses as a whole, of businesses in bankruptcy, or of businesses that transact in consumer information. It is not clear how the dominance of retail and the significant presence of other categories of business might affect this study's overall findings. One possibility: ombuds view the "harm," and correspondingly, the stakes, as relatively low in retail cases, compared to cases involving the potential compromise of more intimate or intrusive data. In any case, given this selection bias, conclusions cannot necessarily be drawn about industries and business that are not present in significant numbers in this study.

ii. Number of Consumers Affected

Fewer than half (43.97%) of the reports provide any indication of the number of consumers affected, and when provided, the numbers vary widely. On the upper end, *RadioShack* deals with the transfer of information of 117 million customers and *Sears* with the information of 86 million customers. On the other

154. This figure includes some businesses also coded as health-related retail and health-services.

155. This figure includes some businesses also coded as health-related retail and media/technology.

156. This figure includes some businesses also coded as automotive-related.

end, a wine storage company near New York City has the information of only 436 customers—although the report notes that these tended, unsurprisingly, to be "high net-worth individuals," who are, according to the debtor's management, "typically very concerned about protecting their personal information and information about their wine collections."[157] In the aggregate, out of those that provide information, the median number of customer records was 425,000, the mean was 8.73 million, and the standard deviation was almost 22 million.

iii. Sensitivity of information

The sensitivity of the information to be transferred affects judgments regarding whether and how it may be transferred. Findings concerning information sensitivity are summarized in Figure 2.

Figure 2. Reports' Findings on Sensitivity of Information

Report's Statement	*Number of Cases*	*Percent of Total*
Sensitive information is to be transferred	52	36.9%
Health information	*20*	*14.2%*
Financial information (mostly credit cards)	*21*	*14.9%*
Other[158]	*11*	*7.8%*
Information from/about children was collected but is to be destroyed	2	1.4%
Sensitive information never collected or is to be deleted	87	61.7%

157. Report of the Consumer Privacy Ombudsman at 3, 5, *In re* Winecare Storage, LLC, No. 13-10268 (Bankr. S.D.N.Y. Mar. 27, 2014), ECF No. 240 [hereinafter *Winecare* Report].

158. This category includes educational information, identity-related information (including biometric), and other sensitive information. *See also supra* note 157 and accompanying text (discussing heightened privacy sensitivity of wealthy patrons of wine storage company). One unusual report, for a seller of lingerie, explains the assessment of the potential sensitivity of the information as follows:

> Agent Provocateur is a luxury brand, with US stores in locations like The Forum Shops at Caesars in Las Vegas, Rodeo Drive in Beverly Hills, and Madison Avenue in New York City. . . . The customer information should be considered somewhat more sensitive than typical retail store purchase information. Given the product being sold, and the locations of the stores, it is likely that some customers have purchased items for people other than their spouses, and with locations in Vegas and Beverly Hills, it is also likely that the store has publicly known clientele. Particular care is appropriate to ensure that the customer information provided is used solely for the purposes expected by customers.

Report of the Consumer Privacy Ombudsman at 12-13, *In re* Agent Provocateur, Inc., No. 17-10987 (Bankr. S.D.N.Y. June 10, 2017), ECF No. 145. The report appears to suggest, in other words, that at least one privacy expert considers "what happens in Vegas stays in Vegas" to be part of federal consumer protection law.

Usually, consumer data is marketed for sale together with all other assets or at least all other intangible property such as copyrights and trademarks, trade secrets, and so on. Reports are not always clear on the issue, but many reports note that the material to be transferred is limited—it does not include the full range of data actually held by the seller.[159] Commonly, the information to be transferred is private—containing email and mailing addresses, birthdays, clothing preferences, etc.—but other highly sensitive categories of information are to be omitted from the transfer (for instance health information, financial information, information concerning sexual habits, or information collected from or about children).[160]

2. Transfers Under General Privacy Law

Reports approach transfers under generally applicable privacy law somewhat differently than those under more closely regulated areas like health and finance, or those involving particularly sensitive information. This Section focuses on generally applicable requirements. By far the most frequent recommendation is that sales be approved subject to "qualified buyer" requirements borrowed from *Toysmart*. Reports also commonly require that affected consumers be provided with notice and the opportunity to opt out of a transfer.

i. "Qualified Buyer" Requirements

Reports nearly always recommend that the buyer should meet—or find that the proposed buyer already meets—at least some characteristics of a "qualified buyer," as initially laid out in the *Toysmart* FTC settlement. Figure 3 shows the remarkable pervasiveness of this framework in the reports.

159. *See* Report of Consumer Privacy Ombudsman at 4, *In re* Adinath Corp., No. 15-16885 (Bankr. S.D. Fla. July 29, 2015), ECF No. 427 [hereinafter *Adinath* Report].

160. *See, e.g.*, Consumer Privacy Ombudsman Report to the Court at 9-10, *In re* QSL of Medina, Inc., No. 15-52722 (Bankr. N.D. Ohio Mar. 21, 2016), ECF No. 260 (noting that numerous categories of sensitive information will be deleted and not transferred).

Figure 3. Reports' Application of Qualified-Buyer Restrictions

Ombud's Recommendation	*Number of Cases*	*Percent of Total*
Qualified-buyer requirements (explicitly or implicitly)	119	84.4%
Hybrid of qualified buyer and heightened requirements for different parts of data	8	5.7%
Qualified-buyer restrictions generally, but materially loosened	5	3.5%
Only anonymized transfer allowed	1	0.7%
Transfer allowed with no qualified-buyer restrictions	1	0.7%
Qualified-buyer restrictions generally, but materially heightened	3	2.1%
Unclear what requirements would apply	4	2.8%

As Figure 3 demonstrates, this framework is applied, at least as a starting point, in nearly every case. It effectively functions as a "cleansing" mechanism for sales no matter what the privacy policy provides and, in many cases, even despite the transferred information being highly sensitive. And, it acts as a baseline, even when its guidelines are ultimately tightened or somewhat loosened due to particular factual circumstances.

Although there was some variation, the three primary characteristics of a "qualified buyer" were as follows: (1) The buyer is in the same industry as the seller; or if the buyer is larger or is in multiple lines of business, at least one of its lines of business coincides with the seller's; (2) The buyer agrees to use the information for the same purpose as the seller; (3) The buyer agrees to comply with the seller's privacy policy. These three requirements form a common core, though some reports impose additional "qualified buyer" characteristics as well.[161] The requirements are discussed in detail below.

161. *See, e.g.*, Report of Consumer Privacy Ombudsman at 19, *In re* The Rugged Bear Co., No. 11-10577 (Bankr. D. Mass. Mar. 31, 2011), ECF No. 239 (including a requirement that the buyer purchase debtor's "goodwill" and that it agree to be "successor-in-interest" to the transferred information).

(1) The buyer is in the same industry as the seller, or if the buyer is in multiple lines of business, at least one of its lines of business coincides with the seller's.

Mostly, this was straightforward in the reports: for example, one car dealership buying the data of another.[162] The requirement was stretched a bit at times, such as when the shared line of business actually involved a shift from a brick-and-mortar seller to an ecommerce-only buyer.[163] In a few other cases, the buyer was or appeared to be a private-equity firm that intended to use the data in service of a company in which it was invested or to license it out to third parties in that type of business.[164] Arguably, the transfers in these contexts are not as protective as sales in which the buyer itself is carrying on the same type and manner of business as the seller. Most reports seemed unbothered by these stretches of the qualified-buyer requirement. But one report found that a buyer's "present intention" to use the transferred information in a going-concern context was insufficient to meet this aspect of the qualified-buyer standard.[165] Several others, confronted with buyers that were engaged in several different lines of business at once, expressly restricted the use of the consumer data to the brand that was intended to operate as a successor to the seller.[166] Other reports did not grapple with such nuances.

(2) The buyer agrees to use the information for the same purpose as the seller did.

One report provides, for example, that the transferred consumer information may be used only for "continuing business operations and continuing to provide similar goods and services to consumers, including marketing the products and services related to the Purchased Assets."[167] The requirement appears to mean that if the data was collected from buyers of widgets, it will not be used for data

162. *See, e.g.*, Consumer Privacy Ombudsman Report to the Court at 1, *In re* Northern Blvd. Automall LLC, No. 19-41348 (Bankr. E.D.N.Y. Aug. 7, 2019), ECF No. 177 [hereinafter *Northern Blvd*. Report].

163. *See* Consumer Privacy Ombudsman's Report at 24, *In re* Vanity Shop of Grand Forks, No. 17-30112 (Bankr. D.N.D. Nov. 17, 2017), ECF No. 495 [hereinafter *Vanity Shop of Grand Forks* Report].

164. *See, e.g.*, Consumer Privacy Ombudsman's Report to the Court at 11, *In re* Storehouse, Inc., No. 06-11144 (Bankr. E.D. Va. Sept. 7, 2007), ECF No. 910 [hereinafter *Storehouse* Report] (private-equity buyer plans to license information to a user in the same line of business); Report of Alan Chapell, Consumer Privacy Ombudsman at 2, *In re* The Rockport Co., No. 18-11145 (Bankr. D. Del. July 12, 2018), ECF No. 371 [hereinafter *Rockport* Report] (apparent private-equity company deemed qualified buyer).

165. Consumer Privacy Ombudsman's Interim Report to the Court at 17, *In re* Steve & Barry's Manhattan, LLC, No. 08-12579 (Bankr. S.D.N.Y. Nov. 20, 2008), ECF No. 1119 [hereinafter *Steve & Barry's* Report].

166. *See, e.g.*, Report of Consumer Privacy Ombudsman at 7-8, 19, *In re* Urban Brands, Inc., No. 10-13005 (Bankr. D. Del. Oct. 27, 2010), ECF No. 427; Report of Consumer Privacy Ombudsman at 9, *In re* Eddie Bauer Holdings Inc., No. 09-12099 (Bankr. D. Del. July 22, 2009), ECF No. 487 [hereinafter *Eddie Bauer* Report].

167. Report of the Consumer Privacy Ombudsman at 8, *In re* Craftworks Parent, LLC, No. 20-10475 (Bankr. D. Del. May 29, 2020), ECF No. 550.

mining concerning insurance pricing—even if the buyer also happens to participate in the insurance industry, such as through a subsidiary.[168] But the report's broad language (and similar language used in other reports) calls into question the strength of the limits imposed.

A few reports draw sharp distinctions. For example, ombuds have refused to allow a sale of data provided to obtain the benefits of a loyalty program that the purchaser had no intention to continue. These reports theorize that, because customers had not provided the data to receive general marketing, it should not be sold for that purpose. One of the more expansive discussions states:

> Buyer shall not attempt to use the database for any affiliated businesses that are not directly tied to the Debtor's "core business." Historically, the "core business" of Robb & Stucky has been the retail sale of high end, interior-design driven, home furnishings. In other words, Buyer will only use the customer database for marketing to prospective customers looking for home furnishings. For instance, if Buyer happens to own a sister business that is involved in sales of gardening related items, Buyer would not attempt to use the database for marketing for that business.[169]

Generally, however, the reports do not analyze purpose continuity with much nuance. For instance, ombuds have been satisfied if the data is originally collected for marketing by a brick-and-mortar company and the buyer intends to use it in an ecommerce or a third-party licensing context, despite the obvious distinctions that could be drawn.[170]

(3) The buyer agrees to comply with the seller's privacy policy.

Sometimes, the language of this requirement is less specific, such as when it requires that the buyer's policy be "at least as protective" as the seller's,[171] or that the protections in the old and the new policies be "substantially" the same.[172] These provisions might invite opportunism by allowing wiggle room that could be exploited by an opportunistic buyer. On the other hand, it might be administratively difficult for buyers and confusing for consumers to have multiple privacy policies in place for different groups of consumers.

168. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 119 (2004) (arguing that privacy law should regulate information based on use). The lines are not always this clear, of course. If the seller was only in the gun industry, can the buyer use the list for marketing other sporting goods as well as guns? This seems to be an area where the buyer retains discretion to interpret the agreement liberally in its own favor.

169. Report of Consumer Privacy Ombudsman at 6, *In re* Robb & Stucky Ltd., No. 11-02801 (Bankr. M.D. Fla. May 20, 2011), ECF No. 561.

170. *See, e.g.*, *Storehouse* Report, *supra* note 164, at 1; *Rockport* Report, *supra* note 164, at 15.

171. Report of the Consumer Privacy Ombudsman at 2, *In re* Bristlecone, Inc., No. 17-50472 (Bankr. D. Nev. July 27, 2017), ECF No. 189 [hereinafter *Bristlecone* Report].

172. Consumer Privacy Ombudsman's Report at 6, *In re* Advanced Sports Enters., No. 18-80856 (M.D.N.C. Jan. 14, 2019), ECF No. 392.

ii. Existing Privacy Policies

Technically, unless a transfer would violate an existing privacy policy, an ombud need not be appointed at all. Surprisingly, however, ombuds have been appointed in a number of cases where the proposed transfer arguably complies with the privacy policy. In these cases, the U.S. Trustee moved for appointment of an ombud, and the court complied, despite the fact that an existing policy arguably permitted the transfer—sometimes pursuant to a "business continuity" clause.[173] Obviously, the court makes this determination prior to the ombud's appointment, and there is little incentive for the ombud to revisit it. Still, ombuds often consider whether the transfer likely violates the privacy policy in determining whether the transfer violates privacy law as a whole.

Although ombuds' determinations on this score are not always clear, the reports often find that the transfer would violate the policy, even when the sale is to a "qualified buyer." The reports then commonly follow the *Toysmart* model and bless the sale as conforming to applicable law. Most often, a privacy policy provides that consumer information will not be sold or shared with third parties absent certain conditions not relevant to the bankruptcy (for instance, the information could be shared with law enforcement). Determining whether and to what degree a transfer violates the existing privacy policy requires the exercise of judgment. Reports were not always clear on their findings on this issue, nor did they apply consistent standards.

Many policies typically permit the transfer either pursuant to a dedicated business-continuity clause that allows a transfer "in connection with the sale or reorganization of all or part of its business or operations,"[174] pursuant to broad language permitting transfers to third parties at will, or because there is simply no policy in place at all.

Sometimes, the policy permits only part of the data to be transferred, because a different policy applies to some data (e.g., a frequent buyers' club), or because at some point in the past, the business changed its policies so that the transfer is permitted by the policy applicable at one time but not another.[175]

In some cases, reports note that a lack of recordkeeping made it impossible to know which policy applied at a given time or to a given body of data or what the content of the policy was. In such situations, most reports err on the side of consumer protection, applying the strictest policy to all of the data. Others, by contrast, seem to assume that likely no policy was in place and therefore few restrictions need to be applied.

Significantly, even if policies clearly or arguably permit the transfer, that is not the end of the story. Under a pure consent-based model, such policies might

173. *See, e.g., Northern Blvd.* Report, *supra* note 162, at 7.

174. *See, e.g.*, *id.* at 11 n.9.

175. *See, e.g.*, Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman at 21, *In re* Borders Grp., Inc., No. 11-10614 (Bankr. S.D.N.Y. Sept. 21, 2011), ECF No. 1380 [hereinafter *Borders* Report] (noting that more than one privacy policy was applicable because there was a change in the policy and pre-change customers weren't notified and given proper opportunity to consent to the change).

lead to sales being permitted so long as they comply with policy provisions. But most ombuds do not seem to adopt a pure contractarian view and instead limit the application of these policy terms. Ombuds do not always spell out their reasons for imposing such limits, and in some instances, it appears to be done as a matter of custom. But some reports provide their rationales for imposing limitations. For example, in several instances, a report references the fact that a policy change potentially falls afoul of the FTC's position concerning retroactive changes to privacy policies.[176] In other cases, where the specific terms of the policy arguably allowed the transfer, the ombud nonetheless imposed restrictions on the grounds that allowing unrestricted transfer would fall afoul of more general provisions of the policy or background norms of privacy law, including those based on consumer expectations.

The incorporation of background norms and the consideration of the entire context of the sale accords with the trends in privacy law and regulation under the FTC Act and similar consumer protection rules. The legal analysis is essentially that even if a specific provision might seem to allow the transfer, it might be misleading and/or unfair to enforce (1) because it contradicts the overall impression given by the policy as a whole, (2) because the permissive terms were insufficiently clear and conspicuous, (3) because the permissive terms are in tension with the general, reasonable expectations formed by consumers doing business with the seller, or (4) because the policy should be read in light of the background norms of "applicable law," including the FTC Act and other privacy laws that would not permit a transfer absent some restrictions. In many cases, even when policies are unclear or the privacy policy seems to permit the sale, reports nonetheless implicitly or explicitly make a finding that at least some part of the data should be protected to some extent.

A significant area of disagreement among ombuds concerned the statement, contained in many privacy policies, that a business "will not sell, rent, or transfer your information to third parties." Notwithstanding the apparent clarity of such a guarantee, privacy experts and regulators disagree as to whether this provision includes a sale in the context of a transfer of the business itself to a successor taking over the debtor's business. Some ombuds reason that in such a transfer (and perhaps subject to the "qualified buyer" restrictions discussed below), the successor is effectively standing in the shoes of the debtor and, from the point of transfer forward, is not a true "third party."[177] One ombud explained his views on this point as follows:

> Customers are unlikely to view their relationship with the Debtors as being with a firm, but instead view it as being with a brand. Customers providing information

176. *See, e.g.*, *In re* Gateway Learning Corp., 138 F.T.C. 443, 475-76 (2004); *infra* notes 218-228 and accompanying text.

177. *Cf.* HOOFNAGLE, *supra* note 16, at 146-47 (discussing the "third-party problem" in privacy policy: once it comes into their possession, "information brokers who have no relationship with the consumer are free to sell personal information"); *supra* notes 74-76 and accompanying text.

> through the websites, or in a . . . store, are unlikely to know, or even care, what the form of corporate entity is that technically holds the information.[178]

Many reports implicitly concur. Others, however, consider this language ambiguous.[179] Ombuds generally—though not universally—read policies in a consumer protective manner when there is ambiguity as to the policy's application in a particular case. In any case, however, ombuds rely on the *Toysmart* qualified-buyer framework to "cleanse" even sales in violation of privacy policies.

iii. Notice and Choice

The reports also reflect the ongoing influence of the traditional notice-and-choice model of privacy regulation. In most cases, the reports require that consumers receive notice of the transfer of their data and an opportunity to opt out of the transfer. Although these requirements were not included in the *Toysmart* case,[180] they accord with the traditional notice-and-consent model of privacy law; some ombuds even include them in the definition of "qualified buyer."[181]

Notice-and-choice requirements appear pervasive in reports. The requirement of notice is expressly mentioned in ninety-six cases (68.09%) and implied in many more, such as when the agreed-to privacy policy requires such notice.

The implementation of the requirements varies considerably. Take the timing of the notice and opportunity to opt out. Most reports simply state that sellers should provide notice and opportunity to opt out, but they do not require it prior to the date of the transfer. By contrast, stricter reports require that the seller, or even a neutral third-party intermediary, provide notice in advance of the transfer of information to the buyer and give consumers some reasonable time to send their opt-out requests.[182] This approach keeps the data of nonconsenting consumers out of the buyer's hands completely.

Advance notice and consent is a significant demand given the compressed timing of many of the sales. Most bankruptcy sales are structured as auctions, with a "stalking horse bidder" providing a floor for the bidding. Closings usually occur shortly after the completion of an auction. Parties and courts alike fear delays, which strain already tight budgets. Generally, records suggest that courts

178. Report of the Consumer Privacy Ombudsman at 22-23, *In re* Jo-Jo Holdings, No. 16-44337 (Bankr. N.D. Tex. Feb. 27, 2017), ECF No. 187 [hereinafter *Jo-Jo Holdings* Report].

179. *See, e.g.*, Joel R. Reidenberg, Jaspreet Bhatia, Travis Breaux & Thomas Norton, *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. LEGAL STUD. S163, S163 (2016).

180. *See Toysmart* Stipulation, *supra* note 115.

181. *See, e.g.*, Consumer Privacy Ombudsman Report to the Court for the Second Sale of Consumer Data at 28-31, *In re* Circuit City Stores, Inc., No. 08-35653 (Bankr. E.D. Va. Aug. 27, 2009), ECF No. 4648 [hereinafter *Circuit City* Report].

182. *See, e.g.*, Consumer Privacy Ombudsman Report to the Court at 18-22, *In re* Roomstore Inc., No. 11-37790 (Bankr. E.D. Va. May 1, 2012), ECF No. 533.

appoint ombuds late in the process, with little time to complete their report and to implement any suggestions before the sale is closed and the transfer completed. Even when ombuds are appointed well in advance, the results of an auction may not be known, and therefore detailed notice may not be possible, until shortly before the time of transfer. In a few cases, to deal with the time crunch, reports propose intermediate mechanisms, such as an emergency, limited-purpose transfer to be effective immediately together with an undertaking by the buyer to destroy all information if the sale isn't ultimately permitted or if consumers opt out; or the maintenance of the customer information on the seller's systems until the opt-out opportunity has been provided; or the use of a neutral intermediary, essentially to hold the customer information in escrow pending court approval or consumer opportunity to opt out.

The *content* of the notice is specified by the ombud, is subjected to ombud approval, or is given significant guidance by the ombud in only 22 cases (15.60%). In the remainder, any notice is left to be drafted by the seller and buyer, perhaps subject to considerable mischief. As with the requirement of pretransfer notice and opportunity to opt out, the specification of the form and content of notice, as well as the requirement of ombud preapproval of notice, are ways of bolstering the protection for consumers while remaining within a consent-based, contractarian framework. That said, even these steps do not address all of the pathologies of the notice-and-choice regime.[183] Nor do they protect the remaining consumers who fail to opt out from having their data privacy abused once the ombud and bankruptcy court are safely in the rear-view mirror. There is some tension, in other words, when we impose strong, externally derived restrictions at the time of transfer that leave consumers at the mercy of the custodian of their data once the transfer is completed.

In fifteen cases (10.64%), notice is required but the *form* of notice is not specified. In another eighty-one cases (57.45%), the form is indicated, and it takes a bewildering variety. Most commonly, notice is to be provided by some combination of notice on the buyer and/or purchaser's websites, posting at physical store locations, and email. Often, ombuds require more than one form of notice or provide different forms as alternatives depending on what information is available about a given consumer. Figure 4 summarizes these recommendations:

183. *See* discussion *infra* Section I.A.2 (outlining critiques of the notice-and-comment regime).

Figure 4. Forms of Notice Recommended in Reports

Form of Notice (One report may require multiple forms of notice)	*Number of Reports*	*Percent of Total (of the 96 Reports that Require Notice*
Web	53	55.2%
Email	61	63.5%
Mail (usually only if email is unavailable)	26	27.1%
Posting at physical locations	17	17.7%

Some reports specified that notice be provided by less common means, such as on social media postings,[184] with store receipts,[185] or in the *New York Times*.[186]

In addition to notice, some reports do not state explicitly that companies must provide an opt out to consumers.[187] With the exception of healthcare and financial institutions (dealt with below),[188] the reports' silence on this omission goes unexplained. Ombuds may reason that such a right was implicit, either because it is contained in the privacy policy being honored or because it is otherwise a part of applicable law as a mandatory, background legal principle.

Notably, even where reports mention the opportunity to opt out, they rarely specify what exactly constitutes a sufficient opportunity to opt out. Reports are unclear on this point, but in many cases a sufficient opportunity appears to mean that certain marketing emails will be halted, not that information will necessarily be deleted.

Many reports recommend that the court require a document to be filed certifying that the notice and opt-out process has been followed. Several also require the filing to include information concerning how many consumers opted out of the transfer. We were able to locate four cases with filings that indicate opt-out numbers. The data from these four cases are summarized in Figure 5.

184. Report of Consumer Privacy Ombudsman at 5, *In re* Brookfit Ventures LLC, No. 18-46224 (Bankr. E.D.N.Y. May 19, 2019), ECF No. 126 (requiring notice by social media, among other forms).

185. Report of the Consumer Privacy Ombudsman Regarding Successful Bid of Food Emporium Acquisition Corp. with Respect to Store Number 36706 at 3, *In re* The Great Atl. & Pac. Tea Co., No. 15-23007 (Bankr. S.D.N.Y. Nov. 4, 2015), ECF No. 1727.

186. *Winecare* Report, *supra* note 157, at 6.

187. Exact totals are unavailable because so many reports were ambiguous on this point that we determined not only that coding this variable would be difficult, but also that the results might be unclear or misleading.

188. *See infra* notes 229-239 and accompanying text.

Figure 5. Reported Opt-Out Rates

Debtor Name	*Number of Consumers Notified*	*Number of Opt-Out Requests*	*Percent Opt Out*
Choxi.com, Inc. [189]	2,190,000	31,505	1.4%
The Loot Co., LLC[190]	5,300,000	29,068	0.5%
QSL of Medina, Inc. [191]	82,782	1,492	1.8%
Coach American Group Holdings[192]	97,000	1,466	1.5%

Data such as this could be useful for policymakers considering the effectiveness of the notice and opt-out regime. In whatever form it takes, the "notice and opt-out" process is considered to qualify as consumer "consent" to the transaction. This is despite the criticisms of consent-centered regimes generally[193] and the evidence of low opt-out rates,[194] of which this data provides another example. These low opt-out rates might cause some to conclude that consumers are not exercising meaningful choice. The less cynical might focus more on the differences among these debtors. For example, why were QSL of Medina's customers over three times more likely to opt out than The Loot Company's? Was notice in one case substantially better? Were both sets of consumers actually able to exercise meaningful control of their data? The differences in these opt-out results could lie in the nature of the business, different levels of customer loyalty to the debtors' respective companies, or in

189. *See* Consumer Privacy Ombudsman Report to the Court at 2, *In re* Choxi.com, Inc., No. 16-13131 (Bankr. S.D.N.Y. Jan. 19, 2017), ECF No. 71; Certification by Licensee Concerning Opt Out Process at 2, *In re* Choxi.com, Inc., Case No. 16-13131 (Bankr. S.D.N.Y. May 26, 2017), ECF No. 119.

190. *See* Consumer Privacy Ombudsman Report to the Court at 3, *In re* Old LC, Inc., No. 19-11791 (Sept. 26, 2019), ECF No. 241 [hereinafter *Loot Crate* Report]; Certification of the Loot Company with Respect to Opt-Out Procedures and Compliance with Consumer Privacy Ombudsman Report to the Court at 2, *In re* Old LC, Inc., No. 19-11791 (Bankr. D. Del. Nov. 11, 2019), ECF No. 301.

191. *See* Certification of Compliance with the Report of the Consumer Privacy Ombudsman at 2, *In re* QSL of Medina, Inc., No. 15-52722 (Bankr. N.D. Ohio Apr. 13, 2016), ECF No. 304. This certification covers only some of the information that was transferred; whether notice was provided to other consumers, and if so how many consumers opted out, is not apparent from the record in the case.

192. *See* Consumer Privacy Ombudsman Report to the Court at 7-8, *In re* Coach Am. Grp. Holdings Corp., No. 12-10010 (Bankr. D. Del. June 7, 2013), ECF No. 1583; Certification of the Sellers and Purchaser Pursuant to Consent Order Authorizing and Governing Use of Personally Identifiable Information at 2, *In re* Coach Am. Grp. Holdings Corp., No. 12-10010 (Bankr. D. Del. Oct. 16, 2012), ECF No. 1154; Certification of the Purchaser Pursuant to Consent Order Authorizing and Governing Use of Personally Identifiable Information at 2, *In re* Coach Am. Grp. Holdings Corp., No. 12-10010 (Bankr. D. Del. May 13, 2013), ECF No. 1548.

193. *See supra* notes 79-92 and accompanying text.

194. *See, e.g.*, HOOFNAGLE, *supra* note 16, at 296 (reporting that opt-out rates of required annual notices from banks ranged from a high of 5% to below 1%); Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230 (2002).

the form or content of the notice provided. The data is too limited to draw conclusions without further research. But if more courts and ombuds were to require detailed certifications, they could yield valuable information concerning whether and how different noticing regimes enable consumers to exercise control over their data.

iv. The Limits of the *Toysmart* Framework and of Notice and Choice

The *Toysmart* framework is dominant in this body of cases. But it is important to note that the nature of the bankruptcy sale process impairs any direct causal claims about the effects of ombuds. In fact, in a significant number of cases, the ombud's appointment and report *followed* identification of the buyer, and the plan for the sale to meet the qualified-buyer restrictions appears already to have been in place.[195] Most reports are simply silent on the question of whether the ombuds' involvement had any effect. The reports imply or state that the ombud's work somehow changed the plan in only eight cases (5.67%), and these changes may not have been particularly substantial. Generally, then, the evidence in this study provides no way to determine whether the involvement of ombuds affected particular transactions or whether parties would include these protections without the ombud—for instance, because of concerns for reputation, or because of what they anticipate an ombud will say or a court will hold. The terms of sales in bankruptcy are often negotiated long in advance of the bankruptcy filing. Parties negotiate "in the shadow of the law," including the privacy law, that they think the bankruptcy court will apply in their case. Thus, in many cases, the effects of ombuds' work may often be exerted indirectly and over time as lawyers come to understand the contours of what ombuds typically approve. In addition, because the ombud regime only applies to certain sales within bankruptcy, it is also possible that distressed companies wishing to engage in non-compliant sales practices simply avoid triggering the appointment of an ombud.[196]

Generally, reports are content to note that the qualified-buyer requirements are met, and do not further opine as to whether a sale should be approved if they are not. In the vast majority of cases, debtors simply do not force the issue. And, in several cases, ombuds concluded that the qualified-buyer requirements are met, at least in part, even where the privacy policy or applicable law arguably permits unfettered transfer.[197]

On the other hand, most reports are silent as to what standard applies if a qualified buyer is not found. In thirty-three cases (23.40%), the reports add at least some alternative for a sale to a *non*qualified buyer for any consumers who

195. *See, e.g.*, Report of the Consumer Privacy Ombudsman at 3, *In re* Liberty State Benefits of Del., Inc., No. 11-12404 (Bankr. D. Del. Jan. 31, 2013), ECF No. 711.

196. *See* Bradley, *supra* note 29, at Sections I.C and II.A.

197. *See, e.g.*, Report of Consumer Privacy Ombudsman at 6, *In re* Altrec, Inc., No. 14-30037, (Bankr. D. Or. Feb. 13, 2014), ECF No. 162 (noting that the information to be transferred likely fails to meet the Bankruptcy Code's definition of personally identifiable information).

opt in, but it appears rare for ombuds to face more difficult decisions. In one case, after an initial sale to a "qualified buyer" fell through, the ombud filed a revised set of recommendations imposing stronger limits on a "standalone" sale of the data because such a sale would be contrary to "customers' reasonable expectations, and, as such, would be considered a violation of the FTC Act."[198] Looking to the privacy policies in place at different dates, the report recommended that some consumer data only be transferred if consumers opted into the transfer; other consumers would be provided with the opportunity to opt out prior to the transfer.[199] This case exemplifies the mix of "reasonable expectations" and "privacy policy fine print" that appears to still characterize privacy law in this area.

In only one case, a report recommends that the court permit a completely unfettered transfer. The case involved "an on-line sports gaming site wherein consumers would purchase cards and place odds on which teams would prevail in various sporting events."[200] The report recommends "that the Bankruptcy Court approve the proposed sale and transfer of the Debtors' assets and related customer lists and other customer-related information without limitation as such sale is consistent with the Debtor's privacy policy."[201] Filed by a frequently serving ombud, this rare report is one of the few reports that cites neither *Toysmart* nor section 5 of the FTC Act nor any other nonbankruptcy law. The finding also appears to be in some tension with the actual privacy policy, which provides that customer information may be sold in "a bankruptcy, merger, acquisition, reorganization or sale of assets," but also provides that "[t]he promises in this privacy policy will apply to your information as transferred to the new entity."[202] Notably, even in this case, it is not clear that the data was ultimately sold on a standalone basis. The sale appears to have been of "[s]ubstantially all of the . . . [a]ssets," apparently to a single buyer, for the price of $100,000; the docket does not appear to offer any further information about how the data was to be used or whether the buyer even intended to use it.[203]

In several other cases, the reports appear to loosen the qualified-buyer restrictions based on lax privacy policies. For instance, in a case in which the privacy policy included a typical business-continuity clause, the report does not require a qualified buyer, although it does require the buyer to have at least as protective a privacy policy as the seller.[204] It also finds that some records should be deemed nontransferable because the consumers had at some earlier point

198. Consumer Privacy Ombudsman's Supplemental Report to the Court at 2, *In re* Ritz Camera Ctrs., Inc., No. 09-10617 (Bankr. D. Del. July 23, 2009), ECF No. 834.

199. *Id.* at 2-3.

200. Report of Consumer Privacy Ombudsman at 2, *In re* Avaago, Inc., No. 17-12926 (Bankr. S.D.N.Y. Feb. 18, 2018), ECF No. 39.

201. *Id.* at 1.

202. *Id.* at 5.

203. *See id.* at 2.

204. *See* Report of the Consumer Privacy Ombudsman at 1-2, 7-8, *In re* The Wet Seal, LLC, No. 17-10229 (Bankr. D. Del. Mar. 2, 2017), ECF No. 221 [hereinafter *Wet Seal* Report].

opted out of the transfer.[205] In another example, the report notes that the privacy policy is weak in that it can be modified at will at any time by mere notice on the seller's website. While the enforceability of such provisions is uncertain under privacy law,[206] the report relaxes the qualified-buyer requirements in light of the clause. It recommends that if the buyer is not a qualified buyer, the transfer should be approved, albeit with the requirement that the buyer agree to the seller's privacy policy and provide consumers with an opt-out option.[207]

The *Circuit City* report also features some loosening of the qualified-buyer requirements. The report in that case finds that a significant amount of data—"records of approximately 33,000,000 Circuit City consumers who made purchases in a retail store or by telephone"—are unprotected by any privacy policy.[208] Accordingly, the report permits that data to be sold twice by the debtor, in the latter case to a buyer called Micro Center. Although the report emphasizes the ombud's finding that there is "no legal requirement or Privacy Policy to enforce," it notes that Micro Center otherwise "meets the qualified buyer requirements" and has "voluntarily" agreed to extend specified privacy protection to consumers.[209] It adds the following explanation:

> Micro Center plans to lease sections of the consumer data to a "very limited number of reputable marketing partners who provide special services or products" that may be of interest and value. Consumers will be notified in these mailings of their right to opt out of future mailings, but not of their right to opt out of having their information ever shared with third parties. However, the extent of the harm is minimal because they can readily dispose of whatever mail they receive if they are not interested in receiving it. With no legal requirement or Privacy Policy to enforce, on balance, the voluntary actions of Micro Center to extend privacy protections to these consumers is welcome and should be commended.[210]

On that basis, the report recommends approving the sale of many millions of consumers' data. Reasonable minds could disagree on this, and critics might offer it as an example of the light-touch, business-driven approach to regulation that, they claim, has failed to protect consumer data privacy.[211]

These examples illustrate the limits of the *Toysmart* framework. When confronted with what they interpret as lax privacy policies, some ombuds do not hesitate to weaken the protections that they might otherwise apply. But these cases are in the minority, and most ombuds appear to adopt a moderately more consumer-protective stance. They generally take the position that unfettered or

---

205. *See id.* at 8.

206. *See infra* notes 218-228 and accompanying text.

207. *Adinath* Report, *supra* note 159, at 15 ("The Debtor's privacy policy is relatively weak in that it permits 'update' at any time by posting a notice on the Debtor's main website page.").

208. *Circuit City* Report, *supra* note 181, at 6.

209. *Id.* at 22-23.

210. *Id.* at 23.

211. *See, e.g.*, Waldman, *supra* note 5, at 778 (arguing that "privacy's managerialization" threatens to "undermin[e] the capacity for law to achieve more robust privacy protections for users").

less fettered transfers must clear a high bar. Most ombuds appear to apply the *Toysmart* framework liberally even when information might arguably be less protected than the information in *Toysmart* was. Some reports explicitly reference consumer expectations and seek to analyze the transfers based upon a contextualized understanding of the likely contours of such expectations.[212]

3. Barriers to Modification

Whether the governing privacy policy could be amended after transfer is controversial, and the reports sharply divide on this issue. Many privacy experts, and many reports, consider the issue important because if a buyer can simply modify a policy later, then its promise to abide by the seller's privacy policy at the time of sale is meaningless. A purchaser need only wait a month, promulgate a new and more liberal policy, and then use or sell the data as it likes.[213]

To prevent this type of end run, just under a majority of the reports require some form of consent prior to a material modification of existing privacy policies, as Figure 6 reflects.

Figure 6. Reports' Recommendations Concerning Future Modifications

Modification Requirement	*Number of Reports*	*Percent of Total*
Not mentioned	73	51.8%
Restriction on modification	68	48.2%
Notice and opt in	*18*	*12.8%*
Notice and opt out	*31*	*22.0%*
Hybrid restrictions (depending on applicable policies or sensitivity of information)	*7*	*5.0%*
Gateway discussion (implied opt in)	*7*	*5.0%*
Consult with ombud	*5*	*3.5%*

Some reports require that purchasers give consumers an opportunity to opt out of modifications.[214] Some require that consumers opt in.[215] Others recommend that the ombud clear any modifications.[216] Finally, some take a

212. *See, e.g.*, *Bristlecone* Report, *supra* note 171, at 3 (departing from the qualified-buyer framework due to a lax privacy policy but excluding numerous categories of information in order to ensure the transfer "aligns with consumer expectations and is consistent with best practices").

213. *See* Elvy, *supra* note 28, at 482.

214. *See, e.g.*, *Adinath* Report, *supra* note 159, at 14-15 (providing for modifications with only an opt-out right, due to the "weak[ness]" of the privacy policy that permitted modification at will).

215. *See, e.g.*, *Bristlecone* Report, *supra* note 171, at 3.

216. *See, e.g.*, Report of the Consumer Privacy Ombudsman at 7, *In re* Max & Erma's Rest., Inc., No. 09-27807 (Bankr. W.D. Pa. Aug. 17, 2010), ECF No. 965. This recommendation fits awkwardly

hybrid approach, which could include permitting modification freely, granting opt-out rights, or requiring opt in, depending on factors such as the sensitivity of the information.[217]

Some reports do not include an explicit recommendation on this issue but do include a substantial discussion of the *Gateway* case,[218] which may carry an implicit opt-in message. In *Gateway*, the FTC complained that the defendant company reversed its policy from one in which it would not share or transfer information to one in which it would.[219] It notified users only by posting the revised policy on its website and by providing email and mailing addresses for consumers who wished to opt out.[220] Even though the original privacy policy stated that such changes could take place,[221] the FTC argued that the change was an "unfair and deceptive act[] or practice[]" because it was material, applied retroactively to consumers who volunteered their information under the prior policy, and was posted silently and without sufficient notice.[222] Ultimately, Gateway and the FTC entered into a consent decree entitling customers to opt in before any future "material changes" applied to them.[223]

Reports produced by one frequently serving ombud, Luis Salazar, nearly always include a discussion of *Gateway*, which implies that modifications would require an opt-in. For instance, one of his reports states that modifications must be made "in accordance with applicable law" and also includes a substantial discussion of *Gateway*.[224] He interprets that case to establish a broad-based bar on retroactive changes to privacy policies without opt in.

Other privacy experts are more divided on this question—a division reflected in the numerous reports that require only an opt-out opportunity for modifications.[225] For instance, another report suggests that the FTC's position is not widely followed and recommends an opt-out policy instead.[226] The report claims that "companies have not followed this FTC guidance strictly," and offers two reasons: "One reason is that opt-in rates are extremely low, exacerbated by the fact that a consumer who receives a notice may disregard it. This can be

with bankruptcy law. For one thing, there is no clear way by which service of the ombud could be compensated after the case is closed.

217. *See, e.g.*, *Borders* Report, *supra* note 175, at 46.

218. *In re* Gateway Learning Corp., 138 F.T.C. 443 (2004); Solove & Hartzog, *supra* note 19, at 640-41 (describing *Gateway*).

219. *See Gateway*, 138 F.T.C. at 443.

220. Apparently, Gateway actually began sharing before posting the change to its website. *Id.* at 446.

221. *See id.* at 445-46 ("If at some future time there is a material change to our information usage practices that affect your personally identifiable information, we will notify you of the relevant changes on this Site or by email. You will then be able to opt-out of this information usage by sending an e-mail . . . .").

222. *Id. at* 449-50; *see* HOOFNAGLE, *supra* note 16, at 161.

223. *Gateway*, 138 F.T.C. at 469.

224. Consumer Privacy Ombudsman's Report at 33, *In re* HearUSA, Inc., No. 11-23341 (Bankr. S.D. Fla. July 25, 2011), ECF No. 342.

225. *See, e.g.*, *id.*

226. Report of the Consumer Privacy Ombudsman at 8-9, *In re* Life Unif. Holding Corp., No. 13-11391 (Bankr. D. Del. July 22, 2013), ECF No. 245 [hereinafter *Life Uniform* Report].

devastating to a company's legitimate business conduct. Another important reason is that the opt-in requirement does not effectively account for consumers' desire for convenience and continuity in receiving services."[227] The ombud instead recommends following "an accepted industry practice in addressing material, retroactive changes," namely, "provid[ing] consumers with a dedicated, robust notice of the changes and an opportunity to opt out."[228] Again, this provides some support for the notion that, even when applied by independent experts, current privacy law has a decidedly pro-commerce bent.

Finally, some reports are silent on the issue. This does not necessarily mean there is no restriction on modification in those cases. Reports may omit a discussion because a restriction is included in the governing privacy policy already, or because they believe that mandatory background legal norms sufficiently prevent this sort of bait-and-switch. But its absence may also indicate a lack of concern with this issue, a *caveat consumer* attitude toward actions taken by custodians of data after the sale.

4. Transfers Under "Sectoral" Regimes

As noted above in Figure 2, fifty-two cases (36.88%) involve particularly sensitive data to be transferred, as identified either by the ombuds or by the research team. The most common forms of sensitive information are health information, implicated in twenty cases (14.18%), most of which are subject to the Health Insurance Portability and Accountability Act (HIPAA) guidelines discussed in Section II.B.4.i below; and financial (21 cases, 14.89%), most of which are subject to the financial institution's restrictions discussed in Section II.B.4.ii below. In the remainder of cases involving sensitive information, reports express some concern but ultimately apply the "qualified buyer" framework above, and in all but a small number of cases, permit the transfer to proceed.

In some cases, sensitive information is recommended for destruction or is determined never to have been collected by the debtor. Most commonly, this is information from or about children, as discussed in Section II.B.4.iii below.

i. Healthcare Providers

Many healthcare businesses and service providers qualify as "covered entities" under HIPPA and its associated regulations, including the HIPAA "Privacy Rule."[229] This status subjects them to extensive regulations concerning the privacy and security of healthcare data.[230]

227. *Id.* at 8.

228. *Id.* at 8-9.

229. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996); 45 C.F.R. pts. 160, 164 (2021).

230. *See Fast Facts for Covered Entities*, HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/covered-entities/fast-facts/index.html [https://perma.cc/VE9T-PBV2]; MULLIGAN & LINEBAUGH, *supra* note 41, at 10-12.

In sixteen cases (11.35%), reports find that HIPAA applies and protect the data. But this doesn't mean that the transfer itself cannot be accomplished. The HIPAA Privacy Rule permits the use of HIPAA-protected information for treatment, payment, or health care operations,[231] and it defines "health care operations" to 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."[232]

The upshot of these regulations is that so long as the transferee is a "covered entity," many reports conclude that no further consumer protection is needed.[233] They deem the independently applicable safeguards of HIPAA sufficient to protect consumers and thus relieve the parties of otherwise applicable notice-and-consent restrictions.

Of the sixteen cases implicating HIPAA, eight reports do not require any notice to be provided to affected consumers. Four reports require notice but no opt-out opportunity. Finally, two require that notice and an opportunity to opt out be provided, and two require notice and an opportunity to opt in. In one of the opt-in cases, the debtor is St. Vincent's hospital in New York. The recommendations in this report are based in significant part on New York state requirements for treatment of patient data, which are in some respects "more stringent" than HIPAA and therefore not preempted by it.[234] The other report does not mention the "health care operations" exception and thus considers the burden of opt in to be appropriate for such sensitive information.[235]

Thus, the reports generally place their regulatory hopes in HIPAA's data protection requirements, freely permitting transfers under the broad "health care operations" exception, usually without any requirement of notice (much less consent). Whether this trust in the HIPAA regime is warranted is beyond the scope of this Article, but its pervasiveness in the reports is noteworthy.

ii. Financial Businesses

Consumer financial data is both highly sensitive and highly valuable. The Gramm-Leach-Bliley Act (GLB) and the associated FTC regulations govern the security and privacy of consumers' financial data in the hands of a wide range of businesses that are "significantly engaged" in providing financial products and

231. 45 C.F.R. § 164.502(a)(1)(ii) (2021).

232. *Id.* § 164.501(6)(iv).

233. *See, e.g.*, Report of the Consumer Privacy Ombudsman at 6, *In re* Hooper Holmes, Inc., No. 18-23302 (Bankr. S.D.N.Y. Oct. 3, 2018), ECF No. 171; Consumer Privacy Ombudsman Report to the Court at 11-12, *In re* Novasom, Inc., No. 19-11734 (Bankr. D. Del. Sept. 24, 2019), ECF No. 140.

234. Report of Consumer Privacy Ombudsman at ¶¶ 36-38, *In re* St. Vincent's Catholic Med. Ctrs. of N.Y., No. 10-11963 (Bankr. S.D.N.Y. July 12, 2010), ECF No. 593 [hereinafter *St Vincent's* Report].

235. Consumer Privacy Ombudsman Report to the Court at 9-11, *In re* Turkey Lake, No. 15-12091 (Bankr. N.D.N.Y. Dec. 23, 2015) [hereinafter *Turkey Lake* Report].

services and that are therefore considered "financial institutions."[236] These rules can govern businesses such as car dealerships that wouldn't ordinarily be thought of as "financial institutions."[237] Eleven reports (7.86%) deal with businesses subject to the GLB rules.

The GLB rules generally require covered businesses to provide regular notices to consumers regarding how their information is used and explain their rights to opt out of any sharing of the information with unaffiliated third parties. But there are exceptions to these notice and opt-out rights, and one of those exceptions is for transfers of information "[i]n connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit."[238] FTC guidance has interpreted this to mean that so long as the purchaser of "all or a portion of a business or operating unit" agrees to abide by the seller's privacy policies, no notice of the transfer need be provided.[239] The reasoning appears to be that, with such a transfer, the consumer information is only incidental to the transaction. Thus, consumers will be protected because the regulations that applied to the seller will usually apply to the buyer. But this reasoning is not airtight. The rules fall short of requiring that the purchaser be a covered entity or be in the same line of business as the seller. Also, even if the intention of the provision is to require sale of an entire business or line of business, the text of the rule arguably permits the sale of customer information, standing alone, to qualify as "a portion of . . . an operating unit."

Despite these potential concerns, of the ten cases to which GLB rules apply, six of the reports (4.26%) recommend neither notice nor a right to opt out. In the remaining four cases, the report recommends notice and an opportunity to opt out due to the sensitivity of the data. Again, as with the healthcare information, there is strong evidence of privacy law's near-total reliance on the sectoral privacy regulation of GLB for consumer financial information.

iii. Children's Information

The Children's Online Privacy Protection Act of 1996 (COPPA)[240] and its associated regulations[241] restrict the ability of online actors that direct their services to, or collect information from, children under thirteen years old. COPPA imposes sharp restrictions on the collection and use of children's data by these covered actors. Recall that part of the initial outrage over the *Toysmart* case arose because information about children was involved; the marketing of

236. Privacy of Consumer Financial Information Rule, 16 C.F.R. § 313.3(k) (2021) (implementing 15 U.S.C. § 6801(b) (2018)).

237. *See* MULLIGAN & LINEBAUGH, *supra* note 41, at 8-10.

238. 16 C.F.R. § 313.15(a)(6) (2021).

239. *Id.*

240. 15 U.S.C. §§ 6501-6506 (2018).

241. 16 C.F.R. § 312 (2021); *see also* MULLIGAN & LINEBAUGH, *supra* note 41, at 24-25 (providing background on COPPA).

this information contrary to the privacy policy was thought to be particularly egregious.[242]

Only four cases (2.84%) implicate information subject to COPPA. In each case, the reports recommend destruction of the information. This outcome is more stringent than FTC guidance might require, but it appears to be based on the particular facts of these cases.[243] For instance, one debtor gathered information from children for a "kid's club" at one of its restaurants. The report noted that the debtor failed to comply with COPPA's parental consent requirements when gathering the information and accordingly recommended that it be destroyed.[244]

The majority of reports briefly mention COPPA. But while the ombuds police egregious and known violations of COPPA reasonably aggressively, they evince little concern with its potential application in run-of-the-mill cases. Many of them find it inapplicable because the debtor did not knowingly collect data from children under the age of thirteen.[245] But COPPA also requires a fact-specific determination of whether a website, service, "or a portion thereof" is "directed to children."[246] If so, the company must then refrain from collecting any consumer information prior to requiring the consumer to self-verify an age older than thirteen or obtain parental consent. Few reports engage in a complete analysis of whether the company's web presence or services might in fact implicate COPPA.

One report, for instance, states that the debtor's "products and services are generally directed to adults," and without further analysis concludes that "[t]herefore, COPPA does not apply to this proceeding."[247] Of course, a company could "generally" direct its services to adults but also devote "a portion of" the service to children and thus be subject to COPPA. In most cases this distinction is likely not meaningful, but it raises questions concerning how strictly ombuds apply COPPA across the full range of cases.

In an outlier case, one ombud applied a much stricter approach, arguably more faithful to the statutory text, placing the onus firmly on the data collector and custodian to demonstrate compliance with COPPA: "[Debtors] do not appear to have employed any means for preventing the collection of personal information from consumers who were under the age of 13 at the time of

242. *See supra* note 119 and accompanying text.

243. The FTC's Statement of Basis and Purpose accompanying COPPA provides that if the seller and buyer are in the same line of business, the transfer may not be "material," and thus there is no need for the information to be transferred only an opt-in basis. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59897 (Nov. 3, 1999).

244. Consumer Privacy Ombudsman's Preliminary Report at ¶¶ 23, 72, *In re* VI Acquisition Corp., No. 08-10623 (Bankr. D. Del. Mar. 12, 2009), Dkt. No. 1141. Although this report is styled as "preliminary," there does not appear to be any later report on the docket.

245. 16 C.F.R. § 312.2 (2021). The relevant portions are reproduced in the definition of "Web site or online service directed to children."

246. *Id*.

247. Report of Consumer Privacy Ombudsman at 10, *In re* Plum TV, Inc., No. 12-10017 (Bankr. S.D.N.Y. Feb. 29, 2012), ECF No. 113 [hereinafter *Plum TV* Report].

collection . . . . Because it was obtained improperly, this information should not be maintained by the Debtors, or transferred to the Buyer." [248] Accordingly, the ombud recommended a stringent standard: "destroy or delete" any information that the debtors can confirm came from children, and as to other data, "[t]o the extent that the Debtors are unable to determine the age of a consumer at the time that a consumer's Customer Information was collected, the Debtors should presume that the consumer was under 13, and agree to destroy or delete the data, unless the Debtors have a reasonable belief that the consumer was 13 or over at the time the information was provided."[249]

Some critics contend that because COPPA's standards are so rigid and demanding, it encourages companies to facially prohibit gathering information from children, even if companies know that children may well be submitting information contrary to the policy.[250] The fact that so few businesses out of those discussed in the reports admit to having any COPPA-governed information is suspicious at best and provides some support for this criticism. The fact that even independent experts engage in this sort of cursory, "check the box" analysis of COPPA's application also supports the even more broad-reaching critique, urged by Waldman and others, that modern privacy law most often involves superficial compliance intended to shield normal business practices rather than to act prophylactically for consumers.[251]

5. Impact on Consumers

Ombuds frequently discuss whether and to what extent consumers will be harmed by the proposed transaction. They do so partially because of bankruptcy law: it is part of their statutory mandate to assess the costs and benefits of the sale on consumers and whether any "potential alternatives . . . would mitigate privacy losses or potential costs."[252] But they also note that without harm to consumers, there is likely no violation of consumer protection regulations under either state or federal law.[253]

Especially in the absence of sensitive information, reports generally characterize the damage to consumers as minimal or nonexistent. The reports reason that because of the protections provided above, consumers are not any

248. *Steve & Barry's* Report, *supra* note 165, at 19-20.

249. *Id*. at 20.

250. *See* HOOFNAGLE, *supra* note 16, at 193-215.

251. *See, e.g.*, Waldman, *supra* note 5, at 777 (arguing that "privacy standards are being co-opted into corporate compliance structures that provide little to no protection"); Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CAL. L. REV. 1221, 1280 (2022) (critiquing privacy law's emphasis on individual rights and internal compliance and advocating a reorientation of privacy law and practice around "principles of power, equality, and democracy").

252. 11 U.S.C. § 332 (2018).

253. *See, e.g., Turkey Lake* Report, *supra* note 235, at 12 ("Nearly all states that have enacted 'little FTC' statutes that appear to predicate standing to maintain a private action on actual injury resulting from the alleged offending business practice. In general, harm is a core requirement of these statutes. Since the sale of consumer records to the Buyer will not result in harm to consumers, these laws cannot act as a bar to this sale.").

worse off than they were before the sale, and that the right to opt out ensures that consumers who disagree can mitigate any damage themselves. For example, the report in the *Circuit City* case states that "[i]n this sale, it is unclear if there is any injury at all . . . . No credit card numbers are involved; no social security numbers—only name, address, and e-mail address . . . . Thus, the worst that can happen to consumers whose data is sold . . . is that they will receive some unwanted mail, which they are free to place in the trash."[254] The report also emphasizes the ease of opting out[255] and concludes that "any 'violation' of the privacy policy statement is 'minimal' or 'technical' in nature."[256] These are typical characterizations and conclusions.

Reports also generally emphasize the value to consumers of continuity in receiving service or marketing communications from the successor to the seller. This is sometimes convincing, as with a bankrupt rural heating oil company in New Hampshire, when the transfer ensures continuity of an essential service.[257] In other cases, the assertions strain credulity. The report in the bankruptcy case of a group of Mexican restaurants states that the "proposed sale of PII would greatly benefit consumers in this case. That transfer would permit . . . customers to receive uninterrupted products and services they expect from this establishment."[258] One might respond that in the age of the internet, it seems unlikely that customers would suffer too much from having to locate and obtain food from the restaurants even if the buyer doesn't obtain old customer information. In any case, this too is a typical characterization and conclusion regarding the benefits to consumers of the transfer.

As far as considering more protective alternatives, the reports generally concede that a pure opt-in framework would be more protective, but they conclude that it is unnecessary, whether because the information to be transferred is not classified as particularly sensitive or that it is not worth the additional costs or burdens on the seller.[259] As I have explained elsewhere, it is possible that the urgency of the bankruptcy sale process and the general inclination to focus on

254. *Circuit City* Report, *supra* note 181, at 23.

255. *See id*.

256. *Id*.

257. *See* Report of the Consumer Privacy Ombudsman at 7, *In re* Viking Oil Co., No. 09-10165 (Bankr. D.N.H. Oct. 28, 2009), ECF No. 73 ("Over the last several years, the State has experienced more than one precipitous failure of an oil delivery company and the resultant dislocation and insecurity to customers should not be underestimated.").

258. Consumer Privacy Ombudsman's Report at 19, *In re* Real Mex Rests., Inc., No. 11-13122 (Bankr. D. Del. Feb. 8, 2012), ECF No. 877; *see also Jo-Jo Holdings* Report, *supra* note 178, at 22 ("Prohibiting a transfer of PII in connection with a transfer of other business assets can harm consumers, particularly if the buyer plans to continue to operate the existing businesses.").

259. *Cf. Life Uniform* Report, *supra* note 226, at 8 (explaining the burdens of opt-in requirements on commerce); Randi Singer & Olivia Greer, *Transferring Personally Identifiable Information in Bankruptcy M&A–Part 3*, WEIL RESTRUCTURING (June 22, 2021), https://restructuring.weil.com/pre-filing-considerations/transferring-personally-identifiable-information-in-bankruptcy-ma-part-3/ [https://perma.cc/7PFW-GD8Q] (quoting one frequently serving ombud stating during an interview that "I view strict application of an opt-in procedure as the death of a company. You know, I've always adored Loehmann's . . . and they were completely destroyed because they were forced to do an opt-in. They didn't have a chance. If you're going to do opt-in, you might as well not sell the data").

bringing value into the bankruptcy estate drive some of these recommendations.[260] But ombuds are not generally bankruptcy experts; they are privacy experts. More likely, they are influenced by privacy law's bias toward appreciating the commercial value of data over the value of privacy—that is, the value to consumers (and potentially society more broadly) of having data protected, destroyed, and not used in commerce.

6. Reputation as Protection

There is reason to think that companies are constrained by concerns over the reputational damage that they can suffer if misuse of consumer data comes to light.[261] Relatedly, the sale of consumer data to a "qualified buyer" that intends to continue or take over the seller's line of business is thought to be more consumer protective than a stand-alone sale of the data because these same reputational concerns constrain the qualified buyer. This line of reasoning surfaces several times in reports: "A going-concern purchaser has plenty of incentive to protect the transferred PII, including FTC action . . . as well as customer backlash."[262] Similarly, another report reasons that the buyer "has significant incentive—including but not limited to the strong incentive of maintaining the value of Debtor's customer friendly brand—to protect the transferred PII and abide by the Debtor's most restrictive privacy policy."[263] The same reasoning may play a role in numerous other reports under the surface.

7. Anonymization

As mentioned above, an important and unsettled issue in privacy law is the degree to which "anonymization" can protect consumers while permitting companies to use data commercially.[264] If parties could strip identifying details from data, then data could be freely transferred and used for purposes such as "Big Data" analysis without damaging individual consumers.[265] Experts have objected that anonymized data can usually be deanonymized easily; others have noted that consumers as a whole can be harmed even by anonymized data.[266] Thus, while anonymization may hold some promise as a tool of privacy protection, it is no panacea.

260. *See* Bradley, *supra* note 29, at Section II.B.3.b (discussing "pro-transactional mindset" of bankruptcy proceedings).

261. *See supra* notes 71-74, 113, and accompanying text.

262. Consumer Privacy Ombudsman's Preliminary Report at 20, *In re* Tweeter Home Ent. Grp., Inc., No. 07-10787 (Bankr. D. Del. July 12, 2007), ECF No. 437.

263. *Eddie Bauer* Report, *supra* note 166, at 24. *See also* Report of Consumer Privacy Ombudsman at 18, *In re* Urban Brands, Inc., No. 10-13005 (Bankr. D. Del. Oct. 27, 2010) (using nearly identical language).

264. *See supra* note 84 (collecting sources).

265. *See* Rubinstein & Hartzog, *supra* note 84, at 728-55.

266. *See supra* note 84.

Most ombuds' reports do not mention anonymization. They prescribe the requirements above and simply provide that data not transferred pursuant to those recommendations should be destroyed. However, some reports permit data to be retained in "anonymized" form, or they exempt anonymized data from their recommendations altogether.[267] Ombuds used anonymization to partly or entirely "cleanse" a transfer in eight cases (5.67%). The reports seem to have accepted the effectiveness of anonymization at face value and did not provide any details concerning the anonymization methodology. This may suggest a lack of recognition, in at least some corners of privacy law, of the critiques of anonymization and may indicate a need for increased regulatory attention to this area. On the other hand, the problem seems fairly narrow, and several of the reports that relied on anonymization did so on a narrow basis, such as de-identifying only as necessary to comply with the requirements of the Video Privacy Protection Act.[268]

8. Information Security Practices

In addition to considering the privacy implications of the proposed transfer of information, most reports discuss the protection of information—the technical means by which information is secured from theft by malicious actors—before and after transfer. This comports with trends in privacy law toward recognizing security as an important aspect of privacy. After all, no matter how strong the privacy protections provided by a data custodian, if that custodian's security practices inadequately protect data from third-party intrusions, consumers' privacy interests are profoundly harmed.

Eighty-one reports (57.45%) include some recommendation about security, usually a generic recommendation that the buyer be obligated to take reasonable steps to secure consumer information. The details are usually left unspecified. When particular statutory schemes such as HIPAA apply,[269] reports typically reference the security requirements of those schemes in approving sales to buyers obligated to uphold them. The remaining sixty cases (42.55%) make no recommendation concerning security.

In addition, most reports state or imply that there has been at least some investigation of the security practices of the seller and/or buyer, but details are generally limited. Several reports note that the ombud discovered violations of data protection law by the seller and argue that consumers' information is likely to be better off with the buyer that has undertaken to remedy those defects.[270] One report calls out a serious security problem with how the website of the

267. *Wet Seal* Report, *supra* note 204, at 2 (permitting anonymized transfer as an alternative for otherwise nontransferable information).

268. *See Great Atlantic & Pacific* Report, *supra* note 153, at 25-26.

269. *See supra* notes 229-230.

270. *See, e.g.*, Consumer Privacy Ombudsman Report to the Court at 7, *In re* JS Mktg. & Commc'ns, Inc., No. 05-65426 (Bankr. D. Mont. Dec. 20, 2006), ECF No. 137; Consumer Privacy Ombudsman Report to the Court at 8, *In re* W. Med., Inc., No. 06-01784 (Bankr. D. Ariz. Aug. 1, 2006), ECF No. 169.

bankrupt car company Chrysler was collecting highly sensitive consumer data and states, "[t]he Ombudsman strongly suggests that Chrysler address this issue immediately . . . ."[271]

But substantive engagement with security is the exception and not the rule. On the whole, security was a less prominent issue in the reports than privacy—in other words, reports were more concerned with the use of data by the buyer than by the potential leak of data to malicious third parties. Security recommendations are generally formulaic and rudimentary; they often amount to little more than requiring a representation that the buyer will "maintain at least the same level of information security currently maintained by the Debtors, and comply with applicable privacy laws and regulations governing the transfer, storage, maintenance, and access to Customer PII."[272] In terms of consumer well-being, security may be the more important issue, as it protects consumers from malicious and often criminal actors acting entirely outside of the law. Reflecting this reality, the FTC has devoted considerable attention to data-security practices.[273] Reports' failure to treat this issue in detail is surprising and again supports the notion that the privacy law applied by ombuds remains thin and underdeveloped.

There are several possible reasons that reports focus on privacy more than security. One is that the privacy implications of sales have been more controversial and high profile. After all, outrage over Toysmart's data sales led to the creation of the consumer privacy ombudsman position in the first place. Alternatively, reports may focus on privacy because ombuds are lawyers and, despite their expertise in privacy law, may not feel comfortable in the more technical area of security practices. Finally, ombuds may simply explore and resolve any concerns about security directly with the seller and buyer and deem the matters too technical to include in a report filed with the court.

This issue deserves further exploration. Perhaps ombuds should be selected with security training in mind, or regulators should produce more technical guidance to ensure that security gets the attention it deserves.

9. Recordkeeping and Organization

Reports generally state that the privacy policy that applies to a particular consumer is the one in effect at the time information was gathered, unless the consumer consented to a later modification.[274] Several reports indicate

271. Report of Consumer Privacy Ombudsman at 18, *In re* Chrysler LLC, No. 09-50002 (Bankr. S.D.N.Y. May 26, 2009), ECF No. 2654.

272. Consumer Privacy Ombudsman's Report at 22, *In re* Real Mex Restaurants, Inc., No. 11-13122 (Feb. 8, 2012), ECF No. 877.

273. *See* Solove & Hartzog, *supra* note 19, at 650-55 (noting that "when viewed collectively, the FTC's data security jurisprudence forms a rather detailed list of inadequate security practices," and listing those practices with case descriptions).

274. There is potentially some tension between this principle of privacy law and the Bankruptcy Code provisions concerning the appointment of ombuds, which provide that there should be an

uncertainty over debtors' privacy policies and practices due to a lack of sufficient records; even if a current privacy policy is available, researching past policies with sufficient precision is impossible. Some reports note that debtors failed to observe proper security precautions for customer data or to preserve documentation of these practices. This lack of records obviously hinders ombuds' efforts to issue recommendations.

Faced with this challenge, reports seek to reconstruct what the policies and practices were, based on the debtors' records, the memories of any available personnel, and their own internet research, but this is an imprecise task. Nonetheless, the recommendations of the ombuds in these situations generally resemble those of transactions where records do exist, although ombuds sometimes add recommendations that security and documentation practices should be better guaranteed going forward. Still, ombuds' recommendations appear less dependent on the privacy policy at issue than on general privacy principles, supporting the notion that ombuds depart significantly from a contractarian approach.

10. State and International Laws

The transfer of consumer data can also implicate state and foreign laws. These laws can be within the scope of the "applicable nonbankruptcy law" that ombuds are statutorily ordered to apply. Every transfer of U.S. consumers' data implicates at least one state—often many of them—and in an increasingly digital commercial world, cross-border consumer interactions are more common as well.

Many ombuds recognize the applicability of other laws, but their effects so far are very muted in the cases included in this dataset. Ninety-four reports (66.67%) analyze state law. In each of those cases, ombuds conclude (usually explicitly, sometimes only implicitly) that, if the report's recommendations are followed, the transfer will comply with state law. In the vast majority of incidents, the analysis is cursory, and merely states either (1) that if FTC standards are met, then the state laws that generally parallel them can be deemed met as well, or (2) that the state laws require harm to consumers in order to establish a violation, and because of the nature of the transfer to a qualified buyer with the other varied protections, there would be no such harm. For instance, one report provides, as the entirety of its state law analysis, the following: "Most states have consumer protection laws that are consistent with the FTC Act. If the proposed PII transfer satisfies the FTC transfer requirements, state laws should likewise be satisfied."[275]

appointment when the transfer would violate "a policy prohibiting the transfer . . . if such policy is in effect on the date of the commencement of the case." 11 U.S.C. § 363(b)(1) (2018). The Code section could be read to focus not on whatever policy effectively covers the relevant data but only the policy in effect on the petition date (even perhaps if that policy was only recently put into place). *See* Bradley, *supra* note 29, at Section II.B.3.a.ii (discussing this tension).

275. *See, e.g.*, *Plum TV* Report, *supra* note 247, at ¶ 34.

Some reports mention laws such as data-breach notification or data-disposition laws but dispense with them speedily and summarily by stating the buyer has agreed to comply with them.[276] Only one report—"out of an abundance of caution"—excludes data from Californians because of the new California Consumer Privacy Act.[277]

In a couple of cases, usually involving compliance with state laws in particular areas such as healthcare, finance, or education, reports note that state laws impose higher protections and craft recommendations accordingly.[278] But these are outliers. In another small set of cases, reports note that state laws concerning the posting of privacy policies may have been violated, but they merely recommend forward-looking remediation and do not consider this a basis for scuttling a sale.[279]

Non-U.S. privacy laws, usually from Canada or the EU are discussed in a few reports. They are simply not mentioned in 111 (78.72%) of the reports. Perhaps ombuds simply assume that there was no data from citizens of other countries, or perhaps the applicability of other standards does not occur to them. Eight reports (5.67%) consider and analyze international standards, finding them satisfied. This compliance usually takes a very cursory form, however: "The Buyers have advised the Ombudsman that they will abide by the privacy laws applicable to customers residing outside the United States."[280]

In sixteen reports (11.35%), the report states that no non-U.S. customer information exists or that any such information will not be transferred. One report recommends against the transfer of the information of EU or Canadian customers altogether,[281] and one requires that any such customers opt into a transfer.[282] In several other reports, the likely presence of non-U.S. data was recognized but any non-U.S. legal impediments were, surprisingly, disregarded.[283]

---

276. *See Turkey Lake* Report, *supra* note 235, at 13 ("Many states have passed laws that require persons or entities to destroy, dispose of, or otherwise make personal information unreadable or undecipherable, in order to protect the privacy of . . . customers. At least 29 states have laws that govern the disposal of personal data held by businesses . . . . The Buyers have agreed to follow applicable state laws in this case.").

277. Report of the Consumer Privacy Ombudsman at 3 n.7, *In re* Fred's Inc., No. 19-11984 (Bankr. D. Del. Jan. 24, 2020), ECF No. 775.

278. *See, e.g.*, *St Vincent's* Report, *supra* note 234, at 14-15, and accompanying text.

279. *See, e.g.*, *Eddie Bauer* Report, *supra* note 166, at 22.

280. *Loot Crate* Report, *supra* note **Error! Bookmark not defined.**, at 15.

281. *See* Report of Consumer Privacy Ombudsman at 8-12, *In re* Sharper Image Corp., No. 08-10322 (Bankr. Del. May 27, 2008), ECF No. 725.

282. *See* Consumer Privacy Ombudsman's Interim Report to the Court at 12-18, *In re* Refco Inc., No. 05-60006 (Bankr. S.D.N.Y. Nov. 14, 2016), ECF No. 3384.

283. *See, e.g.*, Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman at 22 n.68, *In re* BPS US Holdings., Inc., No. 16-12373 (Bankr. D. Del. Jan. 19, 2017), ECF No. 593 (stating in a footnote in the conclusion of the report that the debtor does not segregate Canadian from U.S. customer data and "[a]s such, this report does not consider the extent to which applicable U.S. nonbankruptcy laws would compel a similar conclusion for data that pertained solely to Canadian consumers"); Consumer Privacy Ombudsman Report to the Court at 7, *In re* Snow Lion Corp., No. 08-28414 (Bankr. D. Utah Feb. 17, 2019), ECF No. 32 (noting data was collected from consumers in over sixty countries but then stating that "[d]ue to the condensed investigation period, data protection laws in the above countries were not

Altogether, the treatment of state and non-U.S. laws suggests that privacy law remains profoundly dependent on U.S. federal law even in the eyes of independent experts. As more stringent state laws are passed and awareness of them grows, this may change, but the lack of real influence in this dataset is striking.

III. Assessing the Law in the Reports

This Part provides additional background on ombuds and their work, and explains why the reports can be described as establishing a sort of "common law" governing the sale of private consumer data. It then suggests some further implications of the reports for the future of privacy law and commerce in consumer data.

A. Reports as "Privacy Common Law"

> RadioShack collected personal information from millions of consumers, including name, physical mailing address (billing and shipping), telephone number, email address, credit or debit card number, and purchase history for over 117 million customers.
> – Jessica L. Rich, Director of the FTC's Bureau of Consumer Protection[284]

This Section discusses the reports and the institutional context from which they emerge. It describes the reports as functionally forming a body of "privacy common law." The term "common law" has a number of different meanings.[285] As used here, the primary relevant meanings are the common law as "the set of rules that lawyers use to settle any dispute or problem to which no constitution or statute applies"[286] and the common law as "modern judge-made law."[287] The argument advanced here takes its inspiration from that of Hartzog and Solove, who have argued that the FTC's work over time has produced a substantial body of privacy law that is analogous to the common law, which they describe as "characterized by incremental development through judicial decisions in a series of concrete cases."[288]

As with the FTC work analyzed by Hartzog and Solove, the ombuds' reports lack some hallmarks of common law. They are not produced by courts in

---

reviewed for applicability in order to provide guidance in this area"); Report of the Consumer Privacy Ombudsman at 9 n.5, *In re* Kid Brands, Inc., No. 14-22582 (Bankr. D.N.J. Aug. 19, 2014), ECF No. 280 ("Debtors indicate that they conduct business in the United States and Australia. This Report does not address any privacy laws that may apply to a company doing business in Australia.").

284. Rich, *supra* note 129, at 1-2.

285. *See Common law*, BRYAN A. GARNER, A DICTIONARY OF MODEL LEGAL USAGE 177-78 (2d ed. 1995) (listing seven senses in which the phrase is used by legal sources).

286. *Id*. at 178 (quoting FRED RODELL, WOE UNTO YOU, LAWYERS! 20 (1939)).

287. *Id*.

288. Solove & Hartzog, *supra* note 19, at 619. *See also* Cass R. Sunstein, *Is Tobacco a Drug? Administrative Agencies as Common Law Courts*, 47 DUKE L.J. 1013, 1019 (1998) (discussing how agencies often "[o]perat[e] as common law courts").

a hierarchical structure applying formally stated rules of precedent. But in other respects, they exemplify numerous features of common law. Both the content and the institutional context of the reports support the notion that they are well-grounded and legitimate nonstatutory expressions of privacy law.

First, as Section III.A.1 explains, the reports provide reasoned applications of broad legal principles to particular cases, and they show an awareness of a growing body of other contributions to privacy jurisprudence. In this sense, the reports compare favorably to other sources of privacy jurisprudence, including FTC enforcement and guidance materials. While the reports all arise in bankruptcy proceedings, and while most of them share general contours, they are not just a set of identical "rubber stamps," nor do they merely convey whether one expert approved or disapproved of the particular course of action proposed in each case. To the contrary, they are customized and reasoned recommendations that can give guidance beyond the narrow circumstances in which they arose, much in the way of traditional common-law decisions. They also reference and rely on a shared and growing body of privacy jurisprudence, including that developed by ombuds working in earlier cases.

Second, as explored in Section II.A.2, despite the unusual means by which it has been developed, the law in the reports has been shaped by a range of authoritative and expert actors who have a role in producing reports and an interest in their accuracy: judges, private lawyers, and ombuds as well as federal and state regulators. In that sense, reports as a whole represent the product of a politically accountable and expert consensus of the law at the intersection of commerce and privacy. Whether or not one believes that the reports represent the law we *should* have, there are reasons to believe that they present the law we *do* have and that their contributions to understanding that law should be studied more closely.

1. The Reports' Content

In their trailblazing work, Solove and Hartzog noted that while the FTC does not issue traditional judicial opinions, its written products—complaints, settlements, reports, and so on—in the realm of privacy bear marked resemblance to, and serve much the same function as, traditional common-law decisions.[289]

Ombuds' reports bear a similar resemblance to common-law decisions and serve similar functions. Ombuds differ in their thoroughness, but reports are generally lengthy, detailed, and thorough discussions of privacy law as it bears on particular cases. Ombuds' reports generally evidence serious engagement with a wide variety of sources: case law, regulations, FTC statements and policies, and secondary sources, including some written by ombuds themselves. An overwhelming majority of the reports relied upon various FTC materials and

289. Solove & Hartzog, *supra* note 19, at 619-27.

settlements.[290] To give an example, 120 (85.11%) of the reports specifically referenced Section 5 of the FTC Act, and nearly as many, 109 (77.3%), referenced the *Toysmart* case in particular. This practice accords with the statutory guidance provided to ombuds, which requires them to analyze both the applicable privacy policies and the governing nonbankruptcy law.

While there are of course no formal rules of precedence governing the effect that reports from earlier cases should have on any ombuds' recommendations, in practice, the reports draw on and rely on one another. There is variation among reports and ombuds, but in broad strokes, the reports are consistent in their style and content, both over time and across various individuals serving as ombuds. Thirty-two reports (22.70%) directly cited to other reports. Even those that lacked specific citations were clearly indebted to other ombuds' reports, sharing analysis, recommendations, citations, and so on.[291] The reports' convergence on the "qualified buyer" framework bears this out.[292] If anything, the reports have become exercises in conformity, precisely because the law they apply is so consistent.

In each of these ways, the reports compare favorably with other sources of privacy common law, such as the materials produced by the FTC. The FTC's privacy jurisprudence is founded upon the settlements and consent decrees it enters into with companies. Experts parse these documents as soon as they are released. As one former FTC leader stated, industry experts "seem to analyze literally every word of the complaint and [settlement] order in search of hidden messages."[293] These are certainly valid and important sources of privacy law, but it must be said that FTC settlements leave something to be desired as *jurisprudence*. Because they are intended to memorialize binding legal obligations, they are drafted in careful, formal language—usually a series of "whereas" clauses, providing background, followed by operative clauses laying out the parties' agreements.[294] There is little or no room for the sort of citations and discursive explanations that are expected in judicial opinions.[295]

The ombuds' reports compare favorably with FTC consent decrees in that they generally include not just a concrete set of recommendations but also explanations of reasoning, citations of authority, and acknowledgements of

290. *See, e.g.*, *Vanity Shop of Grand Forks* Report, *supra* note 163, at 18-24 (citing cases, FTC materials, and other sources).

291. In private conversation, an ombud who has served in more than one case confirmed this reality, noting that he and other ombuds were often aware of the work of several other ombuds. *See also* Bradley, *supra* note 29, at Section II.B.3.a.ii (discussing characteristics of reports and noting instances of unacknowledged borrowing among reports).

292. *See supra* Section II.B.2.

293. Solove & Hartzog, *supra* note 19, at 624; *see also id*. at 585 ("Those involved with helping businesses comply with privacy law—from chief privacy officers to inside counsel to outside counsel—parse and analyze the FTC's settlement agreements, reports, and activities as if they were pronouncements by the Chairman of the Federal Reserve.").

294. *See, e.g.*, *Toysmart* Stipulation, *supra* note 115.

295. *Cf.* Solove & Hartzog, *supra* note 19, at 607-08 (summarizing critiques of FTC enforcement materials as sources of law).

contrary arguments—the familiar hallmarks of common-law decision making.[296] The length of reports is difficult to compare precisely because some reports include extensive block quotations of materials such as privacy policies or statements of law. To allow an approximate comparison, in our count we disregarded title pages, signature pages, and attachments, but included block quotations.[297] Using this methodology, the median length of the reports was fifteen pages, and the mean was 16.49 pages. Notably, the standard deviation was 9.35, indicating considerable variation.

In addition to drawing from a wide variety of credible sources, the reasoning employed by ombuds stretches beyond the immediate circumstances of a sale within a bankruptcy proceeding. Although not every report cites to other reports, the reports do tend to bear striking resemblances to one another—these are not fresh creative acts or writings on a blank slate, but rather expressions of particularized judgment based on a relatively stable core set of principles. These facets of the reports permit the law they establish to be applied to a broader range of situations than the context of their initial creation.

To be sure, the FTC produces an array of materials to help place its decisions in context, ranging from formal reports to guidelines to press releases to commissioner statements or speeches or testimony. These documents are valid and useful tools to unpack the FTC's perspective on privacy law, and they are cited in many ombuds' reports. They provide helpful clarifications on the FTC's reasoning in particular cases and can help synthesize its guidance across many examples. Still, these other materials are often removed from the particular legal proceedings at issue, and it is often unclear whether they are intended as general recommendations, aspirational best practices, or statements of binding law.[298] They leave a significant role to be played by fact-bound, common-law analysis such as that presented by ombuds' reports.

Finally, the reports form a more representative sample of businesses engaging in privacy-related practices. FTC enforcement actions tend to be focused on massive companies or egregious consumer abuses, whereas ombud reports range from mundane small businesses to some of the largest—such as RadioShack, which as the quotation above reflects, transferred data concerning a significant portion of the American population. In addition, the businesses that are the subjects of ombuds' reports have financial distress in common but do not necessarily share a propensity to violate consumer protection law. Thus, while

296. John Ferejohn, *Judicializing Politics, Politicizing Law*, 65 LAW & CONTEMP. PROBS. 41, 53-54 (2002) (emphasizing the need for judges to provide well-reasoned decisions and noting that "[p]oorly justified decisions tend not to have extensive impact"). This is of course contemplated by the Bankruptcy Code provisions that require the ombud to weigh the "losses or gains" of privacy, other "costs or benefits" of the transfer to consumers, and any consumer protective alternatives. 11 U.S.C. § 332(b) (2018).

297. Also, if more than one report was filed—consistently with how the reports were generally treated in this study—the pages from all reports were counted as one report. *See supra* Section II.A.

298. *See* Solove & Hartzog, *supra* note 19, at 626 ("These materials are purportedly offered by the FTC as guides, yet the FTC has never clearly articulated which parts of its recommendations are mandatory and which parts are simply best practices.").

by no means a perfect sample, they are more typical than the "dataset" of targets of FTC enforcement. This is not to deny that the FTC and other regulators play a crucial role in the development of privacy policy—indeed, I argue below that the reports underscore the importance of regulatory leadership.[299] But the reports help flesh out the law through both their content and the context of their creation.

2. The Reports' Context and Process

The means by which ombuds have developed the law of the sale of consumers' private data bears little resemblance to the traditional legislative or regulatory process. But the ombudsman regime is not completely removed from the political process, either. Judges as well as several different politically accountable actors have roles to play in the process and have the authority to intervene if they wish. All of this helps to transform the reports from expert opinions to something like legitimate and authoritative statements of the law.

The major players in developing the law of consumer privacy sales are the bankruptcy judge, the U.S. Trustee, the ombuds, and regulators. These actors must all work together, and, in essence, each has a veto power if the law strays too far from their own preferences or views. The U.S. Trustee has near-complete authority to designate the ombud[300] and can decline to provide any future appointments to an ombud that goes too far in either antagonizing the parties to the transaction or the court.[301] Each court could, of course, decline to accept the ombud's recommendation, in whole or in part, or request further research into any issue. Finally, regulators have the power to intervene in cases as they wish, and when they have chosen to do so, their intervention appears to have been very effective. And of course, the reports are produced in the context of a bankruptcy, where, unlike most commercial transactions, there is a remarkably high degree of transparency. As one court has put it, "[d]uring a chapter 11 reorganization, a debtor's affairs are an open book and the debtor operates in a fish bowl."[302]

Ombuds themselves are for the most part well-qualified and attentive to the broader legal landscape of privacy. In terms of qualifications and background, ombuds are selected by the U.S. Trustee and generally have a significant experience and expertise in technology and privacy law.[303] In addition, most ombuds are repeat players in the system and have developed expertise in the course of dealing with numerous courts and debtors in bankruptcy; these ombuds will have built up experience over a range of cases that informs their future

299. *See infra* Section III.B.

300. *See* 11 U.S.C. § 332(a) (2018).

301. For instance, representatives of the trustee could appear in court to object to the sale or to an ombud's fees. 11 U.S.C. § 307 (2018).

302. *In re* Alterra Healthcare Corp., 353 B.R. 66, 73 (Bankr. D. Del. 2006). *See also* Alan S. Trust, *Bankruptcy as a Fish Bowl of Disclosure*, 29 AM. BANKR. INST. J. 48, 48 (2010) ("A debtor, corporate or breathing, is subject to having creditors and others peer in and see what is going on in their lives. They are swimming in a fish bowl of disclosure.").

303. *See* Bradley, *supra* note 29, at Section II.B.1.

decisions.[304] An ombud has the power of writing the recommendation in a particular case, knowing that the recommendation is likely to carry considerable sway.

The U.S. Trustee Program is a unit of the Department of Justice. Most of its employees and managers are career public servants but they answer to political appointees and ultimately to the Attorney General.[305] The program has a broad mandate and considerable policymaking discretion in bankruptcy proceedings. Its supervision is exercised through an Executive Office in Washington. Its policy views and practices are managed on the ground by U.S. Trustees appointed in the twenty-one regions (with ninety field offices) in which the program divides the country.[306]

U.S. Trustees have considerable power to intervene in court proceedings, to exercise supervisory authority over debtors, and to appoint neutral professionals such as case trustees and consumer privacy ombudsmen.[307] The Trustees' right to exercise control over ombuds' appointments gives them significant influence over the law of consumer privacy as it has been established in bankruptcy proceedings. Trustees have not provided any formal explanation for their appointment practices.[308] But U.S. Trustees repeatedly appoint certain ombuds, giving strong reason to believe that they approve of how ombuds have gone about their duties.[309] This presumably includes not only the substance of ombuds' decisions but the thoroughness with which they perform their tasks and write their reports.

Another mechanism of political accountability lies with the FTC.[310] The FTC is governed by five commissioners, each appointed to a seven-year term.[311] No party can control more than three of the commissioners; usually, the chair,

304. In specific, four ombuds—Alan Chapell, Lucy L. Thompson, Luis Salazar, and Elise S. Frejka—account for nearly half of the 141 total cases. *See id*. at Figures 1 and 2.

305. *See* 28 U.S.C. § 586(c) (2018) ("Each United States trustee shall be under the general supervision of the Attorney General . . . .").

306. 28 U.S.C. § 581 (2018). There are two exceptions, Alabama and North Carolina, which have "Bankruptcy Administrators," who perform largely the same duties as U.S. Trustees including the appointment of consumer privacy ombudsman, but who are appointed and ultimately supervised by the circuit judges of the U.S. Courts of Appeal for each state. *Siegel v. Fitzgerald*, 596 U.S. 1, 2-3 (2022). Although it is conceivable that their distance from political supervision affects how Bankruptcy Administrators exercise their power, the study did not reveal any distinctions. *See, e.g.*, Notice of Appointment of Consumer Privacy Ombudsman, *In re* Advanced Sports Enters., No. 18-80856 (M.D.N.C. Jan. 14, 2019), ECF No. 361 (appointing Luis Salazar, one of the most frequently appointed ombuds across numerous districts). Because U.S. Trustees control appointments in forty-eight of the fifty states, and because the Bankruptcy Administrator districts appear to follow their lead, this study focuses on them.

307. *See, e.g.*, 11 U.S.C. §§ 307, 330(a)(2), 341, 701, 704(a)(8) (2018).

308. *See, e.g.*, Coordes, *supra* note 28, at 35-39 (arguing for greater transparency); *see also* Singer & Greer, *supra* note 259 (quoting a frequently appointed ombud stating that "[i]t depends a bit on the jurisdiction but essentially when a bankruptcy sale is teed up, the U.S. Trustee's Office will request recommendations for a consumer privacy ombudsman from the debtor or, much less frequently, from the buyer. The U.S. Trustee will then review the recommendations and make an appointment").

309. *See supra* note 304 and accompanying text (noting that four ombuds have received nearly half of the total appointments in cases in this study).

310. *See* HOOFNAGLE, *supra* note 16, at 3-81 (providing capsule history of the FTC, including the role of politics in shaping its structure, practices, and priorities).

311. 15 U.S.C. § 41 (2018).

who is also a commissioner, resigns when a new administration takes over the White House so that the President's party commands a majority of the FTC.[312] The FTC has a large professional staff of lawyers and economists; its public positions are deeply informed and tend to remain consistent over time. But in controversial and unsettled areas, its views also respond to political factors. The commissioners exert significant control over the priorities and positions of the FTC.[313] In addition, industry actors, public interest organizations, and others in the "privacy advocacy community" can and have exercised significant influence on its policymaking.[314] "When these organizations call on regulators to act, they can also mobilize press coverage, questions from sympathetic members of Congress, and grassroots pressure from their members."[315] Certainly, in the contested and evolving area of privacy regulation, the FTC has been and remains responsive to political leadership, to advocacy groups, and to regulated businesses and industry groups.

The FTC has had a powerful influence on the law developed in the ombuds' reports. Least directly but perhaps most powerfully, its settlements and other statements of guidance are the primary documents upon which the law of private data sales is based. These reflect not only the analysis of career employees within the FTC but also of its politically appointed leadership. More directly, the FTC has intervened in particular cases. In *Toysmart*, it brought suit to enjoin the sale.[316] In other cases, it has written letters: to courts, articulating concerns over sales that potentially violate consumer protection law; to ombuds, seeking to help shape their recommendations; and to parties, seeking to warn them over potential violations that could be caused by their proposed courses of action.[317] In *Radio Shack*, the director of its Bureau of Consumer Protection (BCP), Jessica L. Rich, wrote a lengthy memo to the ombud, "express[ing] BCP's concerns about the possible sale of certain consumer personal information currently in the possession of RadioShack Corporation . . . as part of the bankruptcy proceeding."[318] The letter discusses Radio Shack's expansive privacy policies in considerable detail, surveys the relevant law, and encourages the ombud to recommend adherence to the *Toysmart* framework.[319] In another case, in which there was a potential sale of the information that had been gathered about consumers of "a gay male youth-oriented magazine," the FTC wrote a stern letter warning the proposed buyer that given the privacy policy and the nature of the

312. *See, e.g.*, *U.S. FTC Chair Says He Will Resign Along with Senior Staff*, REUTERS (Jan. 19, 2021), https://www.reuters.com/article/us-ftc-simons/u-s-ftc-chair-says-he-will-resign-along-with-senior-staff-idUSKBN29O1XB [https://perma.cc/QL8Y-Z5VS] (noting usual practice).

313. *See* HOOFNAGLE, *supra* note 16, at 3-81.

314. McGeveran, *Friending*, *supra* note 12, at 1022-23. McGeveran does note, however, that the FTC "is not required to act on complaints, and citizens cannot challenge regulatory inaction." *Id.*

315. *Id.*

316. *See supra* note 126 and accompanying text.

317. *See* Elvy, *supra* note 28, at 479-80 (discussing involvement of FTC in various cases, including in Borders bookstores case); Rich, *supra* note 129, at 4 n.12.

318. Rich, *supra* note 129, at 1.

319. *Id.* at 1-5.

information, acquiring such information might open it to liability for unfair or deceptive trade practices.[320] In addition to these relatively public actions, the FTC may have taken other informal actions to affect particular cases, for instance by making phone calls or sending emails, which are not reflected in the public record.

In many ways, ombuds' actions can be seen as lenses through which the views of two major agencies headed by executive branch appointees, the Office of the U.S. Trustee and the Federal Trade Commission, are reflected and refracted. Both agencies have influence on ombuds and their reports. They also have political incentives to remain attentive to the process, if only to avoid potential blowback over the next *Toysmart*. Ombuds must by necessity be responsive to the views and preferences of these regulators, while bringing their own education and analysis to bear on the particular case.

States have a say in proceedings as well.[321] State attorneys general may appear in bankruptcy court "on behalf of consumer creditors if the court determines the appearance is in the public interest,"[322] and they have done so publicly in a number of privacy cases.[323] Some state investigations or lawsuits may be stayed during bankruptcy or preempted by federal law, but states have considerable ability to chill sales of consumer data, for instance by threatening to bring actions under state law against buyers of assets in violation of consumer protection laws. These threats and interventions have force both with bankruptcy judges and with parties. State attorneys general have curtailed or completely scuttled transactions in several cases including *Radio Shack*, a case involving a dating website called True.com, and of course, *Toysmart*.[324] Even where they do not submit filings in a case, they may be involved in negotiations. The ombud in *Circuit City* reported that she "received input from the Debtors, the Buyers, and representatives of the National Association of Attorneys General (NAAG), and the State Attorneys General, and has endeavored to reflect the substance of their views in this Report."[325] Other reports may have drawn from similar input without acknowledgement.

Bankruptcy courts themselves have a role to play in the process, and again their involvement bolsters the legitimacy of the law developed by the ombuds.

320. *See* Office of Director, Bureau of Consumer Protection, letter to Peter Larson & Martin E. Shmagin, attached as Ex. A to Dkt. No. 76, *In re* Cummings, No. 10-14433 (Bankr. D.N.J. July 22, 2010).

321. *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016) [hereinafter *Privacy Policymaking*] (discussing potential roles of states in privacy-related proceedings).

322. FED. R. BANKR. P. 2018(b).

323. *See* Citron, *Privacy Policymaking*, *supra* note 321, at 782-83, 789-90 (describing the involvement of state attorneys general in bankruptcy cases).

324. *See* Citron, *Privacy Policymaking*, *supra* note 321, at 783; *supra* notes 132-137 and accompanying text; *see also* Motion by the Office of the Texas Attorney General to Have Trustee Destroy Consumer Personally Identifiable Information Upon Conclusion of Bankruptcy Case, *In re* Mulligan Mint, Inc., No. 13-34728 (Bankr. N.D. Tex. May 16, 2014), ECF No. 300 (noting that the intervention of the Texas Attorney General led to an agreement that the asset sale would not include private consumer information).

325. *Circuit City* Report, *supra* note 181, at 3.

Bankruptcy judges are non-Article III federal judges and are appointed by the circuits to fourteen-year terms, during which they can be removed only for cause.[326] While in some instances they might be motivated to make a particularly popular decision by the desire for reappointment, this is not true for judges who don't intend to seek reappointment. Some experts have argued that bankruptcy judges in some districts "compete" for cases, in order to gain prestige or simply to take part in more interesting or important matters.[327] Other judges may simply be invested, by virtue of their professional background, in promoting the bankruptcy system as a whole and making it as attractive as possible. These factors might lead them to support sales whenever possible. On the other hand, judges may wish to avoid the negative publicity or stress of presiding over a case like *Toysmart*. This might lead them to take a more cautious approach. Other judges may not respond to any of these external factors or considerations.

The dockets in the cases that we studied reflected little explicit engagement between judges and the ombuds. Nearly every sale appears ultimately to have either fallen through or been approved consensually because the ombuds' recommendations were followed. Given that judges seem generally to acquiesce in the reports' proposed actions, their role may be minimal compared with the other actors described above. Still, the involvement of an insulated judicial officer provides a backstop for an involved party who believes the other parties are straying too far from established law. It is another reason to believe that the reports form legitimate sources of law in an unsettled field.

The ombuds' reports' general inaccessibility is the most significant limiting factor to their functioning as effective common law. They are by no means as accessible as the FTC's orders, all of which are easily available with an internet search and which are often publicized.[328] Thus, their impact to those not already familiar with the ombud regime is likely minimal. This Article is intended to help publicize them, but publication of the actual reports would be valuable. The FTC or the U.S. Trustee could, for instance, provide such a service to aid future ombuds and the privacy-law community more generally.

The observations above support the conclusion that the ombuds' reports reflect and describe what has become a common law of transactions in customer data. This body of law is the product of the joint work of the courts, who ultimately approve sales; ombuds, who inform themselves concerning prior law and make recommendations applying that law to the present case; the Office of the United States Trustee, which exercises considerable power in choosing which ombud to appoint in each case and has the right to participate directly in cases when it desires; the FTC, which not only directly intervenes in bankruptcy cases as necessary but also enters into settlements, makes policy statements, and takes other actions to establish the contours of privacy law; counsel and business

326. *See* 28 U.S.C. § 152 (2018).

327. *See, e.g.*, Lynn M. LoPucki, *Chapter 11's Descent into Lawlessness*, 96 AM. BANKR. L.J. 250 (2022).

328. Solove & Hartzog, *supra* note 19, at 621.

decision makers for sellers and buyers, who propose the transactions that are then scrutinized by the ombuds; and the experts and observers who create secondary literature and who advocate in the public arena (and sometimes in the regulatory or judicial one) for their policy viewpoints.

This lawmaking process does not take the superficial form of common-law cases. Rather than being a product of an adversarial proceeding, the transactions are often approved by the court without objection. Still, the underlying process by which the law has formed bears deep similarities to common-law decision making. It is accretive and incremental, developing with a significant amount of input from a wide range of expert actors with differing goals and roles. It has been refined over time, iteratively, as the product of ongoing tensions in public opinion and commercial realities in this important policy arena, and as a result, it remains inevitably unsettled and continually evolving.

B. Implications for Privacy Law

1. Protection Beyond Privacy Policies, and the Value of Process

Consumer advocates could be forgiven for fearing the worst of the consumer privacy ombudsman regime. They might have guessed that ombuds would merely rubber stamp the auction of consumer data to the highest bidder. And some of the reports conduct a cursory analysis in some respects, for instance considering COPPA materials or data security. In addition, ombuds often weigh the imperatives of commerce more heavily than the values of consumer protection.

Still, the body of law as developed by ombuds provides real, albeit limited, protection to consumers. The reports generally recommend that courts include consumer protections even where privacy policies arguably justify a sale without any protections. This Section will first explore some protections provided by the law given in the reports, note some of its limitations, and then indicate some of its implications for the future development of privacy law.

With relatively minor deviations, ombuds nearly always recommend that courts permit the proposed sale, using the rough framework adopted by the FTC in the *Toysmart* case.[329] The reports require that (1) the buyer be a "qualified buyer," meaning one that is in the same industry as the seller, (2) that the buyer use the information for the same purpose as the seller, (3) that the buyer agree to be obligated to follow the seller's privacy policy, and (4) that some form of notice and opportunity to "opt out" of the transaction be provided.[330] These guardrails form part of ombuds' recommendations even when the language in the governing privacy policies arguably permits transfers with fewer protections. The reports tend to impose restrictions on sellers based on broad principles given in broad terms, or merely implied, elsewhere in the privacy policies; some ombuds look

329. *Toysmart* Stipulation, *supra* note 115.

330. *See supra* Section II.B.2.i.

to consumers' expectations based on business practices and communications as a whole. Recommendations include consideration of the measures that sellers and buyers have taken to maintain the security of information from unauthorized actors, although the consideration of this issue is rather cursory in many reports. Reports take account of the sensitivity of the data involved and recommend the destruction of data where the transfer falls afoul of the law or does not serve the purpose for which the data was gathered. In sectors such as healthcare or finance, they rely heavily on the more substantive, sectoral regulations for the storage and use of data. Generally, then, the reports support an account of privacy law as looking beyond the strictly contractarian notice-and-choice framework and toward more substantive, context-based approaches to privacy protection.

None of the sales appear to have been made to mere data brokers, even though some of the privacy policies arguably permit such a sale. A negative implication that could be drawn from the reports is that they disfavor such a sale of consumer data, and particularly so if the privacy policy provides anything less than clear and conspicuous notice that such sales are permissible.

In addition, there may be some gains to those involved with the data sales in the form of privacy "culture."[331] Both on an individual and a corporate level, spending significant time and resources dealing with an ombud and the court might heighten longer-term awareness of, and engagement with, privacy norms and practices. It raises the likelihood that actors will account for privacy the next time their transactions involve consumer information and may help support better privacy and security practices within the involved organizations.

In light of these successes, a potential implication of this study is that advocates and policymakers should consider forcing more transactions to be open to evaluation or preclearance in a transparent—ideally, fully public—setting. A major critique of current privacy law is that it provides few constraints, largely giving companies the discretion to interpret a body of vague parameters however they like as they make decisions about the use of consumer data and take actions unlikely to be detected or punished.[332] The consumer privacy ombudsman regime could be seen as a sort of pilot study for the protections that could be imposed on a broader range of transactions,[333] serving as a partial answer to this critique.

As mentioned, because ombuds are sometimes appointed before a buyer is identified and sometimes after, it is impossible to tell from this data how much direct influence the reports had in ensuring that such a high percentage of transfers would be to qualified buyers. Assuming that the ombuds process affects the transactions, it would require more study to reveal whether the involvement

331. *See* Bamberger & Mulligan, *supra* note 9, at 277-78.

332. *See supra* note 110.

333. *See, e.g.*, Bradley, *supra* note 29, at Section III.B.2.d (proposing to expand scope of transactions to be scrutinized); Elvy, *supra* note 28, at 518-19 (proposing appointment in foreclosure sales under U.C.C. Article 9).

of the experts or the transparency required by the process (or both) brings these benefits.

Still, it is striking that there were so few deviations from the basic protections discussed above. It seems likely that the involvement of neutral privacy experts has provided some constraints on some transactions. This suggests that even relatively weak laws, such as we have now, can have significant effect if they are actually applied in some sort of public setting. The law applied by ombuds appears to work to deter the most egregious abuses, such as sales to data brokers. But this can only work when there is a regime in place that requires transparency and disclosure. The ombuds' work supports more policy consideration of the degree to which sunlight, in Justice Louis Brandeis's metaphor,[334] could be the best disinfectant of transactions in consumers' private information.

2. The Limits of the Ombuds' Common Law of Privacy

The reports also reveal the profound limits of privacy law as currently constituted. The protections generally fall short of what many consumer advocates—such as the attorneys general in the *Toysmart* case—might want.[335] Reports generally require a very low degree of consumer consent to data protection practices; they rely on provision of notice, sometimes by website only, and an opportunity to opt out, which consumers rarely use.[336] In addition, many of the reports permit businesses to modify their policies later on to loosen data protection practices, so the protections enjoyed by consumers at the time of the transfer may be mostly illusory.

More fundamentally, as experts have pointed out, an ongoing challenge of existing privacy law is that it relies heavily on trusting the custodian of consumers' data but lacks sufficient penalties to deter abuse of that trust. The law imposes various requirements on custodians to protect consumer data, but the right to have one's data protected largely lacks a remedy. No doubt, the risk of reputational harm or FTC investigations have some *in terrorem* effect, at least for consumer-facing companies that rely on good public image to attract business. But there is little reason to believe these risks are adequate to deter abusive conduct given how much questionable conduct falls within a legal gray area and the difficulty of detecting even clear abuses.

The law developed in the ombuds reports suffers from this problem. But arguably these critiques are outside the scope of what could be addressed by ombuds given the current state of the law. Common-law reasoning is generally suited for exploring the application of broad legal principles as they apply to concrete circumstances. The reports bear this out, looking to existing sources of law as they provide guidance in their particular cases. Reports consolidate their

334. *See* Louis D. Brandeis, *What Publicity Can Do*, HARPER'S WEEKLY, Dec. 20, 1913, at 10.
335. *See supra* note 132 and accompanying text.
336. *See supra* Section II.B.2.iii.

recommendations around the *Toysmart* settlement and the notice-and-choice model. Some reports, such as the *Gateway* report, go on to apply stricter rules,[337] and some look toward a consumer-expectations model as they weigh transactions in private data. But even the best ombuds are profoundly limited in the materials they have before them and in the lawmaking they can do. Ombuds have applied and developed a law that provides real protections, but they also have bumped up against the limits of their power. At times, the reports become routine exercises in compliance, applying their framework to each fresh set of facts, with diligence, perhaps, but with little energy for regulatory innovation.[338] Reports make law, in other words, but do so timidly.

Many experts believe that the law or privacy cannot or should not be reduced to bright-line rules due to the speed of technological change and the modern threats to privacy interests. Thus, they have endorsed reliance on broad principles of data protection that can guide data protections as business, society, and technology continue to evolve.[339] This approach benefits from the work of elaboration and application done by ombuds' reports.

But significant shifts in the legal framework depend on "policy entrepreneurs" such as legislators and regulators, who can chart new courses and set larger scale changes in motion. Such policy entrepreneurs have superior capacity to gather information concerning current practices, study consumer preferences, evaluate the economic impact of current and proposed laws, and work with and mobilize public support for policy changes.[340] Embedding privacy officers within companies, or requiring approval of independent experts such as ombuds, can help develop privacy law and ensure that data is protected in particular circumstances. But ultimately, the effectiveness of these practices remains dependent on broader agenda-setting by legislators and regulators.

Conclusion

This Article uncovers and describes the previously unknown body of privacy law contained in ombuds' reports, contextualizes these empirical

337. *See supra* notes 218-223.

338. *See generally* Waldman, *supra* note 5.

339. *See, e.g.*, Bamberger & Mulligan, *supra* note 9, at 302 (discussing some of the challenges in establishing the "optimal specificity of regulatory mandates regarding privacy and regarding the institutional structures of privacy governance"); *id*. at 311 (noting that "a dynamic model of regulation that brings to bear both the uncertain enforcement threats and evolving social and market forces complicates the certainty of the threat and creates a continuous external stimulus that must be translated into meaningful internal practice"); Janger, *supra* note 28 (advocating for "muddy" standards rather than "crystalline" rules in the privacy-law context). *But see* Ari Ezra Waldman, *Privacy's Law of Design*, 9 U.C. IRVINE L. REV. 1239, 1243 (2019) ("Vague statutes . . . give corporate bureaucrats the chance [to] define the law in ways that benefit their bottom line rather than consumers, putting a thumb on the scale by the time the first court has its say . . . .").

340. *Cf*. HOOFNAGLE, *supra* note 16, at 113 ("Intervention, public interest funding for participation in rule-makings, and public comment on settlement agreements all were supposed to heighten engagement with the FTC. But all of these mechanisms have been short-circuited by modern FTC procedures in privacy cases, because these cases almost always settle before public participation could be meaningful.").

findings within current debates about privacy, and suggests some potential future trajectories for the law of consumer privacy. By significantly expanding our knowledge of privacy jurisprudence, the Article provides a sounder legal and factual basis for the many ongoing normative discussions in this crucial policy area.

The reports suggest that the law of transactions in consumers' private data increasingly relies upon more substantive frameworks, focused on consumer expectations and the complete commercial context, and decreasingly relies on a contractarian approach of hewing strictly to the terms of boilerplate privacy policies. The reports also provide some evidence that institutional structures, such as the consumer privacy ombudsman regime, can play an effective role in data protection in the commercial context. The guardrails set up around the transactions in the reports provide meaningful constraints on commerce in consumer data. At the same time, the reports' heavy reliance on guidance from the FTC shows that centrally positioned and politically accountable legislative and regulatory policy entrepreneurs will likely play the primary role in establishing the core tenets of privacy law going forward. In other words, the continued evolution of consumer privacy law will likely need not only decentralized efforts and specificity, but also centralized consideration and guidance.