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

THE OVERTON WINDOW AND PRIVACY ENFORCEMENT

*Alicia Solow-Niederman**

ABSTRACT

On paper, the Federal Trade Commission's ("FTC's") consumer protection authority seems straightforward: the agency is empowered to investigate and prevent unfair or deceptive acts or practices. This flexible and capacious authority, coupled with the agency's jurisdiction over the entire economy, has allowed the FTC to respond to privacy challenges both online and offline. The contemporary question is whether the FTC can draw on this same authority to curtail the data-driven harms presented by commercial surveillance.

This Essay contends that the legal answer is yes and argues that the key determinants of whether an agency like the FTC will be able to confront emerging digital technologies are social, institutional, and political. Specifically, it proposes that the FTC's privacy enforcement occurs within an "Overton Window of Enforcement Possibility." Picture the FTC Act's legal standards as setting forth a range of lawful enforcement behavior for the agency — a range within which further choices must be made. Within this lawful space, just as a politician's "Overton Window of Political Possibility" will not include every possible policy option, the agency's Window will not include every possible enforcement option. Rather, the Window for privacy enforcement — the space within which the agency might operate — will be sharply informed by four critical forces: social norms; institutional norms within the agency; the courts; and Congress.

This approach highlights how the agency's enforcement actions do not occur in a rigidly fixed domain; rather, they unfold within a dynamic space that can change over time, subject to forces both inside the agency and external to it. What's more, understanding enforcement as

---

* Associate Professor, George Washington University Law School; Advisory Board Member, Electronic Privacy Information Center; Affiliated Fellow, Yale Law School Information Society Project; Faculty Associate, Berkman Klein Center for Internet & Society at Harvard University. Thank you to the participants in the *Harvard JOLT*-UIowa IBL Symposium: Beyond the FTC, particularly Paul Ohm and Olivier Sylvain, for helpful feedback on a prior version of this project; to Emily Benfer, Jeremy Bearer-Friend, Danielle Keats Citron, Heidi Liu, Chris Morten, Portia Pedro, Andrew Selbst, Dan Solove, Tania Valdez, and Kate Weisburd for incisive comments; and to Woody Hartzog for generative early conversations. Thank you to Amy Koopmann in the University of Iowa College of Law Library for expert research assistance. I am grateful to the *Harvard Journal of Law and Technology* student editors, especially Dina Rabinovitz, for their feedback and assistance in preparing this piece for publication. This Essay reflects developments through October 2023, when it was substantively finalized for publication. Any remaining errors or omissions are my own.

a process in this way surfaces an often-overlooked point for federal legislation that seeks to endow new or existing agencies with additional regulatory authority: without a sufficiently large Window within which the agency can operate, all the theoretical grants of power in the world will have little impact on the ground. That's a sobering lesson. But it's empowering, too. For one, it suggests strategies for administrative officials who seek to exercise their enforcement authority, such as attempting to ground more progressive or novel actions in topics with thick social consensus. For another, it pushes policymakers seeking to empower agencies to consider institutional design; to account for the practical realities that an agency must confront over time; and to think creatively about where there might be play in the joints.

TABLE OF CONTENTS

I. INTRODUCTION

When Congress created the Federal Trade Commission ("FTC" or "Commission") in 1914, it probably did not have informational capitalism or generative AI in mind. What Congress did envision was an independent agency[1] tasked with "prevent[ing] unfair methods of competition in commerce as part of the battle to 'bust the trusts.'"[2] To empower the new agency, Congress endowed it with broad jurisdictional reach — the entire economy — and flexible authority.[3] Over time, the FTC's remit expanded, including through a statutory amendment that granted the agency formal consumer protection authority to investigate and prevent "unfair or deceptive acts or practices" ("UDAP").[4] These terms were not statutorily stipulated; rather, Congress left them undefined to avoid a restrictive understanding of the

1. William E. Kovacic & Marc Winerman, *The Federal Trade Commission as an Independent Agency: Autonomy, Legitimacy, and Effectiveness*, 100 IOWA L. REV. 2085, 2087 (2015).

2. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/SYM8-5TH8].

3. Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 ANTITRUST L.J. 1, 5–6 (2003); CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY xvi (citing GERALD BERK, LOUIS D. BRANDEIS AND THE MAKING OF REGULATED COMPETITION 1900–32 (2009)).

4. *What the FTC Does*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/what-ftc-does [https://perma.cc/UAB7-XXND]; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598 (2014) [hereinafter Solove & Hartzog, *New Common Law of Privacy*]; *see also* J. Howard Beales III, Bureau of Consumer Prot., *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection,* (May 30, 2003) (quoting Act of Mar. 21, 1938, Pub. L. No. 75-447, § 5(a), 52 Stat. 111, 111 (2012) (codified as amended at 15 U.S.C. § 45(a)(1))), http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection [https://perma.cc/A66W-G2ST].

categories or types of conduct that fell within the agency's jurisdiction.[5] In particular, because "there were too many unfair practices to define" and because attempts to specify them would soon become outdated, the FTC was to exercise its administrative expertise and enforcement authority to police the bounds of unfair commercial practices.[6] This flexible and capacious UDAP authority has allowed the FTC to respond to emerging challenges. Notably, with the rise of the commercial Internet in the late 1990s, the Commission moved to protect consumer privacy both online and offline,[7] and the agency has become the leading privacy regulator in the United States.[8]

The contemporary question is whether the FTC's capacious authority can be used to curtail the data-driven harms of commercial surveillance. This Essay argues that the answer is yes and contends that the key determinants of whether the FTC will be able to do so are social, institutional, and political.[9] It proposes that the lawful range of the FTC's privacy enforcement[10] occurs within an "Overton Window of

---

5. *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection,* 83 GEO. WASH. L. REV. 2230, 2236 (2015) [hereinafter Hartzog & Solove, *FTC Data Protection*]; *see also* H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.) (concluding that, for the original definition of "unfairness" under the FTC's competition authority, "[i]f Congress were to adopt the method of definition, it would undertake an endless task").

6. Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U. L. REV. 431, 471–72 (2021) (quoting S. REP. NO. 1705, at 2 (1936), *reprinted in* 6 ANTITRUST LEGIS. HIST. 4845).

7. HOOFNAGLE, *supra* note 3, at 146.

8. Solove & Hartzog, *New Common Law of Privacy*, *supra* note 4, at 588–89.

9. I am hardly the first to underscore the importance of social norms for the law, nor am I the first to observe the ideological dimensions of the FTC's past actions. For instance, on social norms, constitutional law scholars have long recognized the importance of social movements in pushing arguments from the realm of impossibility to the realm of plausibility — from "off the wall" to "on the wall," in Jack Balkin's memorable coinage. Jack M. Balkin, *From Off the Wall to On the Wall: How the Mandate Challenge Went Mainstream*, ATLANTIC (June 4, 2012), https://www.theatlantic.com/national/archive/2012/06/from-off-the-wall-to-on-the-wall-how-the-mandate-challenge-went-mainstream/258040 [https://perma.cc/M92V-2BYT]. On ideological commitments as shaping the FTC's historic decisions, see, for example, Herrine, *supra* note 6, at 433 (emphasizing the role of neoliberal ideology and not legal restrictions in shaping the FTC's past choices); Kurt Walters, *Reassessing the Mythology of Magnuson-Moss: A Call to Revive Section 18 Rulemaking at the FTC,* 16 HARV. L. & POL'Y. REV. 519, 533–37 (2022) (arguing that agency culture and a commitment to free markets, not binding legal restrictions, drove an ideologically conservative agenda in the FTC's past). As discussed below, see text accompanying notes 11–19 and *infra* Part II, this Essay adapts the Overton Window model's understanding of social norms and augments it by considering how internal institutional norms, including ideological commitments, as well as other external forces act as important determinants of the enforcement space available to the FTC at a given moment.

10. The major questions doctrine ("MQD") is the legal elephant in the room. As of this writing, there is ambiguity concerning the scope of the doctrine. To date, courts have not applied the MQD to cases involving agency enforcement. *See* Todd Phillips & Beau Baumann, *The Major Question Doctrine's Domain*, 89 BROOK. L. REV. (forthcoming 2024) (manuscript at 5–6), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4504304 [https://perma.cc/8VTK-ZMQB] (discussing application only to legislative rules). It is unclear whether that will continue. *See* Chris Brummer, Yesha Yadav & David Zaring,

Enforcement Possibility," which can be expanded, contracted, or shifted by social norms; internal institutional norms; courts; and Congress.[11]

This "Overton Window of Enforcement Possibility" imports and expands the social science concept of an "Overton Window of Political Possibility." The original Overton Window model focuses exclusively on social forces and contends that most politicians will only pursue policies "that are widely accepted throughout society as legitimate policy options."[12] This "model for understanding how ideas in society change over time and influence politics"[13] hypothesizes that policy ideas that

---

Regulation by Enforcement, S. CAL. L. REV. (forthcoming) (manuscript at 33), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4405036 [https://perma.cc/AX7X-NK76] ("So far, the major questions doctrine has only been deployed by the Supreme Court to reverse rules . . . . Nonetheless, to the extent that regulation by enforcement is turf expansive, there is some risk that the courts could get frustrated and sanction regulators who move beyond their usual remits however they do so, including by enforcement."); Chamber of Commerce v. CFPB, No. 6:22-cv-00381, slip op. at 17–18 (E.D. Tex. Sept. 8, 2023) (applying MQD to Consumer Finance and Protection Bureau's interpretation of its unfairness authority, in its internal handbook, to include discrimination). Recognizing vital open questions about whether courts will construe the doctrine as applying to judicial enforcement through Article III courts, to administrative enforcement of the sort that the FTC has often relied on, both, or neither, this Essay assumes *arguendo* that the MQD does not apply to the FTC's enforcement actions. A court's application of the MQD to enforcement actions like those at the FTC would heighten the judiciary's ability to constrain the agency's enforcement space and amplify the salience of the framework presented in this Essay.

11. For a more detailed discussion of these four forces and their interactions, *see infra* Part II.

12. *The Overton Window*, MACKINAC CTR. FOR PUB. POL'Y, https://www.mackinac.org/OvertonWindow [https://perma.cc/WMA3-M4BA]. As discussed below, previous legal scholarship in diverse domains has mentioned the Overton Window and suggested that it might affect the range of policy responses available to public officials. This Essay is the first, to my knowledge, to place the Overton Window and its relevance for administrative law front and center; to argue that the act of agency enforcement itself occurs within an Overton Window; or, as discussed *infra* Part II, to propose a distinct "Overton Window of Enforcement Possibility," articulate specific forces that can act on this Window, and distill them into a framework to understand how these forces can act singly or in combination to contract or expand the size of the enforcement space.

For brief invocations of the Overton Window in earlier legal scholarship, see, e.g., Zephyr Teachout & Lina Khan, *Market Structure and Political Law: A Taxonomy of Power*, 9 DUKE J. CONST. L. & PUB. POL'Y 37, 46 (2014); Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CAL. L. REV. 1221, 1253 (2022); Katharine G. Young, *Human Rights Originalism*, 110 GEO. L.J. 1097, 1124 n.155 (2022) (connecting the Overton Window to Professor Balkin's constitutional law scholarship concerning "off-the-wall" propositions, *see supra* note 9). For more in-depth discussion, see, e.g., John Inazu, *Beyond Unreasonable*, 99 NEB. L. REV. 375, 384 n.36 (2020) (citing concept to argue that "reasonableness lines are usually more fluid in politics than they are in law"); Michael Abramowicz & Andrew Blair-Stanek, *Contractual Tax Reform*, 61 WM. & MARY L. REV. 1537, 1576–77 (2020) (assessing what private intermediaries might do to "[o]pen[] the Overton Window" for tax reforms). One scholar, David Spence, has focused on climate policy and connected the Overton Window to other social science scholarship as well as assessed the interactions among the Supreme Court, Congress, political dynamics, and agency discretion. *See* David B. Spence, *Naïve Administrative Law: Complexity, Delegation and Climate Policy*, 39 YALE J. ON REG. 964, 994–98 (2022).

13. *The Overton Window*, *supra* note 12.

are not widely accepted throughout society lie outside of the Overton Window, and that a politician who pursues an out-of-bounds idea "risk[s] losing popular support."[14] Critically, the Overton Window can "shift and expand," moving some policy ideas in range and excluding others.[15] An individual can try to move the Overton Window by embracing a particular policy; indeed, some popular invocations of the term suggest that an individual can shift it by proposing an extreme stance that makes other, moderately less extreme stances seem more palatable.[16] The original model, however, is descriptive, not prescriptive.[17] Movement is more often due to the "slow evolution of societal values and norms,"[18] with social forces like civil society groups, think tanks, and grass roots organizations mediating what lies inside and outside of the Overton Window.[19]

Assessing the FTC's actions in terms of an "Overton Window of Enforcement Possibility" has both analytic and practical payoffs. Analytically, this framework underscores how the FTC's enforcement actions do not occur in a rigidly fixed domain. To the contrary, they unfold within a dynamic space that can change over time, subject to forces both inside the agency and external to it. These insights highlight an often-overlooked, yet vital, practical point for federal legislation that proposes endowing the FTC with additional regulatory authority: without a sufficiently large Overton Window within which the agency can operate, all the theoretical grants of power in the world will have little impact on the ground. This lesson is especially important given proposed federal privacy and AI bills that would expand FTC authority;[20] so, too, are these lessons germane for the design and implementation of other proposed federal agencies to address the myriad challenges raised by emerging technologies.[21]

This Essay proceeds in four parts. Part II contends that the FTC's Overton Window ("Window") is shaped especially powerfully by four

---

14. *Id.*

15. *Id.*

16. Maggie Astor, *How the Politically Unthinkable Can Become Mainstream*, N.Y. TIMES (Feb. 26, 2019), https://www.nytimes.com/2019/02/26/us/politics/overton-window-democrats.html [https://perma.cc/S7PV-U9UC].

17. *Id.*

18. *The Overton Window*, *supra* note 12.

19. Astor, *supra* note 16.

20. *See, e.g.*, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 401 (2022) (providing for privacy enforcement by the FTC); Algorithmic Accountability Act of 2022, S. 3572, 117th Cong. (2022) (directing the FTC to conduct impact assessments and lodging enforcement authority in the FTC).

21. *See, e.g.*, Lindsey Graham & Elizabeth Warren, Opinion, *Lindsey Graham and Elizabeth Warren: When It Comes to Big Tech, Enough Is Enough*, N.Y. TIMES (July 27, 2023), https://www.nytimes.com/2023/07/27/opinion/lindsey-graham-elizabeth-warren-big-tech-regulation.html [https://perma.cc/ML8B-342W] ("Our Digital Consumer Protection Commission Act would create an independent, bipartisan regulator charged with licensing and policing the nation's biggest tech companies . . . .").

forces: social norms; internal institutional norms; courts; and Congress. Part III looks to the past as proof of concept. It draws from original research to analyze ten years of the FTC's privacy enforcement precedents, assessing how historic patterns reflect a particular understanding of where the agency can and should enforce, based on the social and institutional consensus of the moment. Part IV illustrates how this precedent is not inevitable and articulates how the Window can evolve over time, using location data as an example of how the Window has expanded in response to shifting social norms as well as shifting internal institutional norms and ideologies. It then contends that actions by the courts and by Congress, and not by the FTC itself, will determine whether these expansions are sustainable in the middle and long-term. Part V concludes, emphasizing the need to situate FTC enforcement in dynamic social, political, institutional, and legal context.

II. THE CONTOURS OF PRIVACY ENFORCEMENT'S OVERTON WINDOW

This Part develops the concept of an Overton Window of Enforcement Possibility as a framework to understand the FTC's evolving privacy enforcement activities.

Although minted in the realm of political actors and think tanks, the Overton Window provides a useful way to think about administrative agencies, too. To be sure, the enforcement decisions of a public official at an administrative agency like the FTC are not quite like the choices of a politician. FTC determinations are bound by the terms of the relevant organic statute and informed by associated policy guidance. An "unfair or deceptive act or practice" is understood as "a material 'representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment'" (deceptive) or "a practice that 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition'" (unfair).[22] The FTC Act's statutory mandate is not keyed to a particular sector or a narrow range of conduct. Rather, UDAP authority is capacious and flexible, affording the agency a great deal of discretion about where and how to pursue investigation and enforcement.

---

22. Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Com. (Oct. 14, 1983) [hereinafter Policy Statement on Deception], *reprinted in In re* Cliffdale Assocs., Inc., 103 F.T.C. 110 app. at 174–84 (1984) (decision and order); *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, Fed. Trade Comm'n (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/STH3-ML3K] (quoting 15 U.S.C. § 45(n)).

Thus, one can envision the FTC Act's legal standards as setting forth a range of lawful enforcement behavior for the agency — a range within which further choices must be made. Within this lawful space, just as a politician's "Overton Window of Political Possibility" will not include every possible policy option, the FTC's "Overton Window of Enforcement Possibility" will not include every possible enforcement option. Rather, the Window for privacy enforcement — the space within which the agency might operate — will be sharply informed by four critical forces: social norms; institutional norms within the agency; the courts; and Congress.

Before further delineating this model, several caveats are in order. First, for the sake of clarity, this Essay focuses on these four forces as the most important ones shaping the FTC's Window, without claiming that they exhaust the factors and influences that bear on the FTC's decisions.[23] Relatedly, this Essay recognizes that other influences or motivations can and do act on the forces that are discussed here. As one example, well-resourced business interests, the media, or civil society organizations might affect social norms especially powerfully. The framework does not deny such channels of influence; to the contrary, the model proposed in this Essay is meant to serve as a generative foundation from which to trace out precisely such vectors of influence. Second, the idea that administrative agencies have an Overton Window of Enforcement Possibility is not unique to the FTC; rather, because the FTC's organic statute endows the agency with a great deal of discretion that it can exercise within the boundaries of the law, it sits as a particularly crisp example of dynamics that may be more subtle elsewhere. Third, the Window described here is objective. It is possible to imagine a subjective Window that is mediated by the agency's sense of what the Window is — perhaps colored by negative past experiences that led Congress to temporarily defund the FTC and restrict its authority, for

23. For instance, this Essay focuses on Congress and not the Executive Branch because the FTC is an independent agency that was designed to be more insulated from Executive Branch influence, while remaining more susceptible to congressional influence. *See* Kovacic & Winerman, *supra* note 1, at 2095–96. Nonetheless, a particular presidential administration might have a regulatory or deregulatory agenda that affects political support or otherwise shapes the agency's choices. In addition, a president's public statements might signal support for the steps an agency is taking. *See, e.g.*, Press Release, White House, Statement from President Biden on FTC Vote to Protect Children's Privacy (May 19, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/19/statement-from-president-biden-on-ftc-vote-to-protect-childrens-privacy [https://perma.cc/QUC4-P2MH]; Press Release, White House, Fact Sheet: Biden-Harris Administration Highlights Commitment to Defending Reproductive Rights and Actions to Protect Access to Reproductive Health Care One Year After Overturning of Roe v. Wade (June 23, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/06/23/fact-sheet-biden-harris-administration-highlights-commitment-to-defending-reproductive-rights-and-actions-to-protect-access-to-reproductive-health-care-one-year-after-overturning-of-roe-v-wade [https://perma.cc/ZT2J-ZVBC].

instance.[24] But the framing offered in this Essay refers to an objective, albeit intangible, enforcement space. As discussed below, within this objective Window, the agency's subjective understanding most directly affects one of the four forces, institutional norms.

The Overton Window of Enforcement Possibility provides a way of thinking about privacy enforcement as dynamic. To make this framing more concrete, consider the FTC's internal institutional norms, meaning the agency's own perception of which actions are (not) in range for practical reasons, ideological reasons, or both. These internal norms are affected by factors such as the agency's institutional design and available resources. Specifically, the FTC consists of five commissioners with staggered seven-year terms and no more than three commissioners from any political party.[25] It thus balances an inherently partisan tilt, because one party will always be in the numerical majority, and the need for bipartisanship, because a fully staffed Commission cannot represent just one side. The FTC is, moreover, notoriously underresourced.[26] The agency must exercise discretion in selecting which cases to pursue in the first instance, with an eye to scarce staff and funding.

Such institutional dynamics might limit the range of options that the agency sees as viable and thereby constrain the overall enforcement space. For instance, commissioners might hesitate to issue dissents lest the FTC come across as overly partisan. Or the Commission might pursue certain kinds of actions that seem less politically risky, such as relying on deception and not unfairness,[27] or hew to more moderate stances, overall, in its actions or in its remedies. "Might," not must, because there is no legal limit here: the FTC's authority does not require it to proceed in a bipartisan or uncontroversial fashion. This is an

---

24. *See* Luke Herrine, *Consumer Protection After Consumer Sovereignty* 14–16 (Univ. of Ala. Legal Stud. Rsch. Paper No. 4530307 2023) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4530307 [https://perma.cc/MD52-GPP2] (discussing Congress's negative reaction to the FTC's infamous "KidVid" rulemaking in the late 1970s, including the decision not to fund the agency for some time and to change the controlling rulemaking procedures); Herrine, *supra* note 6, at 440–41 (same).

25. *See* 15 U.S.C. § 41 (2018).

26. *See Developments in the Law — Consumer Protection for Gig Work?*, 136 HARV. L. REV. 1628, 1648 (2023) (citing testimony from former FTC Bureau of Consumer Protection Director David C. Vladeck: "[E]ven though the FTC now enforces eighty statutes in addition to the FTC Act, the FTC is significantly smaller today — in both funding and staffing — than it was in 1980").

27. The FTC's unfairness authority has been understood since the 1980s as politically risky, at best. The standard account, questioned in emerging law and political economy scholarship, is that the FTC overreached in its attempts to regulate unfairness in the 1970s and, subsequently chastened by Congress, retreated into a much narrower understanding of the concept. For a recounting of the classically accepted narrative, see Beales, *supra* note 4. For a summary of the classic account and rebuttal of it that emphasizes the role of neoliberal ideology and not legal restrictions in shaping the FTC's choices, see Herrine, *supra* note 6, and Walters, *supra* note 9.

internally imposed constraint that is informed by agency norms and, perhaps, by institutional design and/or political pressures.

The Window reveals these issues. Specifically, this framework underscores how the FTC could shift its internal norms and lawfully expand enforcement, which in turn raises questions about how such a choice might affect the overall enforcement space. Notably, in a world where the FTC is concerned with funding streams provided by a partisan body (Congress), there may be institutional incentives to avoid political controversy, lest Congress react to expanded institutional norms by pushing back and contracting space for enforcement. Indeed, the FTC's vivid memory of how Congress stripped authority and funding from the agency in the 1980s after the Commission's attempted "KidVid" rulemaking to regulate the advertising of sugary cereals to children has long shaped the agency's actions.[28]

Furthermore, extrapolating from this point about concern with political pushback suggests a more generalizable lesson about the dynamics of enforcement. When the agency operates in a way that is more obviously within the space of an established Window, its actions are perceived as less contentious, as Part III takes up in more detail. But because the agency is not legally bound to proceed in this less contentious manner, the Window can and does change over time, as Part IV exposes. Especially if an expansion unsettles a longstanding equilibrium, however, even a lawful expansion may provoke a reaction. Significantly, the reaction may come from the other forces, with courts and/or Congress pushing back and squeezing the agency in response to perceived overreach.

Such a squeeze may limit the FTC's viable options and thereby constrain where the FTC can move — including in ways that might undercut its effectiveness as a regulatory body. For instance, suppose that the Supreme Court eliminates a remedial pathway that the agency has long relied on, making it more difficult to obtain certain kinds of relief. Or suppose that Congress believes the Commission is overreaching and denies a requested budget increase, such that the FTC cannot obtain the technological expertise it needs for cutting-edge enforcement. Such outcomes might functionally narrow the Overton Window of enforcement actions that the agency can pursue.

Critically, these forces can respond to one another, as above; operate in isolation; and/or interact in more complex and nuanced ways. By way of illustration, building from the above examples, consider the potential impact of a highly partisan Republican faction in the House of Representatives. Even without any shift in the FTC's internal

28. For further discussion of the KidVid controversy and the "ghosts" that have long haunted the FTC, see Herrine, *supra* note 24, at 14–16 (citing interview with former Director of the FTC's Bureau of Consumer Protection, David C. Vladeck).

institutional norms, such a political bloc could push to defund aspects of the FTC's competition law enforcement in ways that threaten to provide fewer resources for its consumer privacy efforts.[29] Subject to the ability to gain enough support in the Senate, such a move by Congress would, in isolation, narrow the available enforcement space. Even if such a motion did not succeed, moreover, confronting and rebutting the sound and fury of contestation in the House could eat up valuable agency resources.

Congress and/or the courts could also widen the Window through a change in political attitudes or jurisprudence. Begin with political attitudes. Picture, for instance, a Democratically controlled Senate and House of Representatives, both of which are supportive of the FTC's enforcement activities to protect consumers in the face of "big tech." If Congress acts quickly to approve a budget increase, including funding for additional full-time staff in the FTC's Bureau of Consumer Protection to address "quickly evolving technological issues,"[30] then it would alleviate longstanding strains on the agency's limited resources and expand the Overton Window of Enforcement Possibility.

Such a shift in Congress's posture towards the FTC might also interact with other forces. For instance, in a world where concerns with funding become less salient for the agency, a less resource-constrained operating environment might also lessen the force of internal institutional norms that emphasize the political prudence of bipartisan, uncontroversial actions. Internal norms would likely still mediate how far the FTC would go, given the lingering scars of KidVid and the subsequent loss of congressional funding.[31] Nonetheless, this example illustrates how Congress might act as a force that expands the available enforcement space, as well as how this force might then afford a further opportunity for expansion through shifted institutional norms.

Other forces might enter the picture, too. Turning to jurisprudence, and returning to the above example featuring an expanded enforcement space, suppose that a conservative Supreme Court is, in general, wary of an expanding administrative state and invokes doctrines that cabin agency discretion.[32] Suppose, further, that a case involving the FTC's consumer protection enforcement authority comes before the Court. If the Court invokes doctrines that curtail the exercise of agency

---

29. *See, e.g.*, Darly Hobbs & William MacLeod, *Angry House Members Vent at FTC and Vote to Cut Its Budget*, JD SUPRA (July 17, 2023), https://www.jdsupra.com/legalnews/angry-house-members-vent-at-ftc-and-7327764 [https://perma.cc/NPK9-DCAQ].

30. *See* FED. TRADE COMM'N, CONGRESSIONAL BUDGET JUSTIFICATION: FISCAL YEAR 2024, at 9, 12 (2024), https://www.ftc.gov/system/files/ftc.gov/pdf/p859900fy24cbj.pdf [https://perma.cc/VUJ2-WNPV] (making and justifying such a request for fiscal year 2024).

31. *See* discussion *supra* text accompanying note 27.

32. I offer this point as an illustrative hypothetical to explain the contours of this Essay's Overton Window framework. As explained *supra* note 10, this Essay reserves further discussion of the major questions doctrine or other specific doctrines, like non-delegation.

discretion as applied to the facts of the case, then the Court's actions might functionally limit the future space of enforcement possibility, too. Significantly, such a contraction could occur in tandem with expansions due to shifts in Congress and internal norms, thereby altering the overall space within which the agency operates in dynamic, interactive ways.

Before assessing these dynamics and appraising the potential risks and tradeoffs of different moves, it is helpful to step back and see how actual enforcement actions illustrate the operation of this model on the ground. The next Part takes up that task.

III. THE WINDOW AS A FRAME: ASSESSING THE PRIVACY ENFORCEMENT SPACE OF THE PAST

This Part analyzes a decade of privacy enforcement actions and situates them within this Essay's Overton Window model.[33] Read cumulatively, these actions define the Window's frame, with historic enforcement patterns revealing the contours of the agency's enforcement space based on prevailing social norms, institutional norms, and judicial and legislative actions during this period. This Part's analysis of the past also sets the stage for Part IV's evaluation of where there may be opportunities to expand or shift the Window in the present and future, and why or why not.

---

33. This research starts approximately where Professors Solove and Hartzog's study in *The FTC and the New Common Law of Privacy*, *supra* note 4, left off, picking up with enforcement actions in March 2013 and including all actions through March 5, 2023. The 147 actions analyzed in this Essay consist of all complaints listed within the "Privacy and Security" category on the FTC's "Cases and Proceedings" website, and which were filed between March 5, 2013, and March 5, 2023. *See Legal Library: Cases and Proceedings*, Fed. Trade Comm'n, https://www.ftc.gov/legal-library/browse/cases-proceedings [https://perma.cc/KK4D-9KW3]. It includes both administrative proceedings and actions pursued in federal court. It does not include cases for which the FTC's complaint was initially filed before March 5, 2013. *See, e.g.*, Complaint for Injunctive and Other Equitable Relief, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-1365 (D. Ariz. June 26, 2012). The analysis excludes one matter, *LifeLock*, for which a 2015 action alleging violations of a 2010 order was filed under seal. *See FTC Takes Action Against LifeLock for Alleged Violations of 2010 Order*, Fed. Trade Comm'n (July 21, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/07/ftc-takes-action-against-lifelock-alleged-violations-2010-order [https://perma.cc/56KM-QMZT]. Note that the numbers diverge from those reported in a 2019 Government Accountability Office analysis that did not include data security complaints. *See* GOV'T ACCOUNTABILITY OFFICE, GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY 43–50 (2019). Here, I include data security actions because they have been essential building blocks of the FTC's "common law" of privacy and to avoid difficult line-drawing in claims that feature both data security issues and privacy concerns. *See, e.g.*, Complaint ¶¶ 32, 34, 36, Retina-X Studios, LLC, FTC Matter No. 172 3118 (Oct. 22, 2019) (alleging an unfairness claim that Retina-X "sold monitoring products and services that required circumventing certain security protections" alongside deception claims based on "false and misleading" data security representations).

First, a bit of history helps to contextualize the FTC's actions. The Commission is an accidental privacy regulator. Relying on case-by-case enforcement, and without an overarching "omnibus" federal privacy law to set a protective baseline, the FTC has extended its "decades-long experience and precedent in enforcing false advertising cases" and often "borrow[ed] norms" from industry self-regulation as well as from statutory information privacy regimes that control particular sectors,[34] such as the Children's Online Privacy Protection Act[35] ("COPPA") (for children's privacy) or the Fair Credit Reporting Act[36] ("FCRA") (for consumer credit reporting). In a foundational article, Professors Daniel Solove and Woodrow Hartzog argue that the Commission's enforcement actions represent a common law-like approach that permits development of the law over time in response to dynamic conditions.[37] This pattern of legal evolution features "incremental development"[38] and privileges "adherence to precedent" and "consistency in decisions," thereby allowing the FTC to avoid charges that it is "acting inconsistently, ignoring previous actions, or reaching too far beyond particular cases."[39] Aggregated over time, these discrete actions constitute a body of privacy law.[40]

The Commission's enforcement of Section 5 of the FTC Act, the source of much of its legal authority to regulate privacy,[41] can sound in deception or in unfairness. An agency seeking to proceed cautiously might pursue claims that are easier to establish, in the sense of demanding fewer resources to investigate and less evidence to make a strong case. So, too, might it prioritize claims that appear less normative, in

34. HOOFNAGLE, *supra* note 3, at 146.

35. 15 U.S.C. §§ 6501–6506 (2021).

36. 15 U.S.C. §§ 1981–1981x (2021).

37. Solove & Hartzog, *New Common Law of Privacy*, *supra* note 4, at 589–90; *see also* Julie Brill, Former Commissioner, Fed. Trade Comm'n, *Privacy, Consumer Protection, and Competition*, Keynote Speech at the 12th Annual Loyola Antitrust Colloquium (Apr. 27, 2012), at 1 & n.1, https://www.ftc.gov/news-events/news/speeches/privacy-consumer-protection-competition [https://perma.cc/KT5S-VGJZ] (citing Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States*, BNA PRIV. & SEC. L. REP. (Dec. 13, 2010), and Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 273 (2011)).

38. Solove & Hartzog, *New Common Law of Privacy*, *supra* note 4, at 619; *see also* Shyamkrishna Balganesh & Gideon Parchomovsky, *Structure and Value in the Common Law*, 163 U. PA. L. REV. 1241, 1267 (2015) (citing P.S. ATIYAH, PRAGMATISM AND THEORY IN ENGLISH LAW (1987); BENJAMIN N. CARDOZO, THE GROWTH OF THE LAW (1924); BENJAMIN N. CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 150–51 (1921); OLIVER WENDELL HOLMES, JR., THE COMMON LAW 1–2 (Little, Brown & Co. 1923) (1881)); Oliver Wendell Holmes, Jr., *The Path of the Law*, 10 HARV. L. REV. 457, 469 (1897).

39. Hartzog & Solove, *FTC Data Protection*, *supra* note 5, at 2233. *But see, e.g.*, Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 958–61 (2016) (questioning the legitimacy of the FTC as a "common law-like" body).

40. *See* sources cited *supra* note 37.

41. *See Privacy and Security Enforcement*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement [https://perma.cc/ZUY4-75B4].

the sense of demanding less of a subjective, qualitative theory of harm — especially if the Commission is also concerned with institutional norms that push it to avoid partisan controversy or internal division.[42]

Most deception claims will fit the bill. An especially crisp example is what Professors Solove and Hartzog term "broken promises of privacy," the theory supporting many of the FTC's very earliest actions.[43] The proof of the violation is inherent in the very fact that a company broke its promises. That makes the allegation easy to establish. In addition, little to no substantive judgment is required to conclude that the company was deceptive: the company's own representations concerning its privacy or data security provide an external benchmark. Such allegations thus seem to demand less of a substantive understanding of harm grounded in social values or theories of the market.[44]

Deception claims have dominated the Commission's activity since its early days enforcing consumer privacy online.[45] In the last decade, these actions have made up over half of the FTC's enforcement activity.[46] Such allegations tend to be quite straightforward. To take one example from a 2017 complaint, if a company tells its consumers that they can "opt out of tracking by instructing their browser to 'stop accepting cookies,'" yet "continue[s] to track consumers by using the Verizon X-UIDH header," then the company has deceived consumers.[47]

And even accepting that not every deception claim is quite so simple,[48] many are. Indeed, out of all complaints in the decade studied, around one-third of the FTC's actions were based on a straightforward

---

42. *See* discussion *supra* text accompanying notes 26–27.

43. *See* Solove & Hartzog, *New Common Law of Privacy, supra* note 4, at 667.

44. This sort of claim is more likely to be what Professors Daniel Solove and Danielle Keats Citron term "visceral and vested," making them more conventionally cognizable. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 754 (2018) [hereinafter Solove & Citron, *Risk and Anxiety*]. For further analysis of courts' struggles with privacy harms, see generally Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022) [hereinafter Citron & Solove, *Privacy Harms*].

45. *See* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 4, at 628 n.211 ("Of the 154 privacy-related complaints analyzed for this Article, eighty-seven unambiguously relied upon a theory of deception in alleging a violation of Section 5, whereas there were only forty-six complaints that unambiguously relied upon a theory of unfairness . . . .").

46. Out of 147 enforcement actions filed between 2013 and 2023, eighty-six claims (59%) featured stand-alone deception allegations. I coded a claim as sounding solely in deception if it explicitly invoked only Section 5 deception authority, stated that the alleged acts and practices were "misleading," or both. This figure excludes complaints containing both unfairness and deception allegations. Including such complaints increases the figure to 107 cases (74%).

47. Complaint ¶ 13, Turn Inc., FTC Docket No. C-4612 (Apr. 21, 2017), https://www.ftc.gov/system/files/documents/cases/152_3099_c4612_turn_complaint.pdf [https://perma.cc/6RJF-LTQ9].

48. For instance, Solove and Hartzog suggest a gradual shift from a "broken promises" approach to a "broken expectations" theory of deception. *See* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 4, at 667–68.

misrepresentation of participation in an international privacy program.[49]

These deception actions, particularly the simpler variety, represent the most small-c conservative option for the FTC. Such actions permit the agency to conserve scarce resources by racking up wins in comparatively easy cases, often bundling similar allegations concerning a number of companies.[50] They also allow the FTC to steer clearer of ideological controversies, because there is a black and white violation (the broken promise) and a self-evident external standard (the international privacy framework) to which to point. Deception actions such as these thus accord with entrenched institutional norms that privilege stability, efficiency, and consensus. While correlation is not causation, the FTC's pursuit of these kinds of claims is consonant with the actions of an agency that is mindful of these internal norms and institutional resource constraints, and which prefers to avoid more normative controversies that might trigger partisan or ideological dissensus.

Indeed, on the rare occasions that deception complaints have proven more contentious, the dispute has tended to center on underlying ideological beliefs about the relationship between a consumer and a business. One illustrative example is a 2015 settlement in *In the Matter of Nomi Technologies*.[51] *Nomi*, an action involving an allegedly misleading opt-out provision in mobile device tracking technology, split along partisan lines. One dissent by a Republican commissioner contested the premise that a lack of opportunity to opt out of the tracking technology in retail stores, despite contrary representations in Nomi's

---

49. Out of 147 total enforcement actions and eighty-six stand-alone deception actions, fifty claims are for stand-alone violations of an international privacy program. This figure excludes claims, such as *In re Cambridge Analytica*, that both explicitly alleged violations of the FTC Act and also separately alleged violations of an international privacy framework; thus, if anything, it undercounts this category. Complaint, Cambridge Analytica, LLC, FTC Docket No. 9383 (July 24, 2019). For a sampling of such complaints filed in 2020 alone, see Complaint, Ortho-Clinical Diagnostics, Inc., FTC Docket No. C-4723 (July 8, 2020); Complaint, T&M Protection Resources, LLC, FTC Docket No. C-4709 (Jan. 28, 2020); Complaint, Click Labs, Inc., FTC Docket No. C-4705 (Jan. 29, 2020); Complaint, Global Data Vault, LLC, FTC Docket No. C-4706 (Jan. 29, 2020); Complaint, EmpiriStat, Inc., FTC Docket No. C-4701 (Jan. 16, 2020); Complaint, Trueface.ai, FTC Docket No. C-4699 (Jan. 16, 2020); Complaint, Thru, Inc., FTC Docket No. C-4702 (Jan. 16, 2020); Complaint, DCR Workforce, Inc., FTC Docket No. C-4698 (Jan. 16, 2020); Complaint, LotaData, Inc., FTC Docket No. C-4700 (Jan. 16, 2020); Complaint, Medable, Inc., FTC Docket No. C-4697 (Jan. 9, 2020).

50. *See, e.g.*, Press Release, Fed. Trade Comm'n, Thirteen Companies Agree to Settle FTC Charges They Falsely Claimed To Comply With International Safe Harbor Framework (Aug. 17, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/08/thirteen-companies-agree-settle-ftc-charges-they-falsely-claimed-comply-international-safe-harbor [https://perma.cc/6H75-Q57T]; Press Release, Fed. Trade Comm'n, FTC Approves Final Orders Settling Charges of U.S.-EU Safe Harbor Violations Against 14 Companies (June 25, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/06/ftc-approves-final-orders-settling-charges-us-eu-safe-harbor-violations-against-14-companies [https://perma.cc/9YVA-T77X].

51. Decision and Order, Nomi Technologies, Inc., FTC Docket No. C-4538 (Sept. 3, 2015).

privacy policy, would be material to consumers.[52] He suggested that "aggressive prosecution of this sort" would "deter" companies from self-regulation that could "promote consumer choice and transparency."[53] The other dissent echoed concerns about how the action would interfere with the "Commission's own goals of increased consumer choice and transparency of privacy practices" and argued that it imposed a disproportionate penalty.[54]

Nomi thus involves substantive debates about what consumer protection requires. Indeed, actions of this sort implicate deeper questions such as proper ambit of the FTC in mediating consumer-business relationships. When an enforcement action raises such questions, it can expose ideological fault lines. Doing so may conflict with internal norms: especially when dissents fall along partisan lines in a 3–2 configuration, as in *Nomi*, the very act of airing ideological differences is in tension with institutional norms that privilege bipartisan consensus. Notably, this conflict does not emerge if there is ideological agreement within the agency — if, for instance, all the FTC commissioners agree that maximizing consumer choice and transparency are sufficient to protect consumers. Whether commissioners are willing to dissent thus turns on not only how much agency officials are concerned with institutional norms that might disfavor partisan controversy, but also how much ideological homogeneity or heterogeneity exists within the agency. Internal dissent, especially along partisan lines, may be an early signal that institutional norms are shifting or that the Window is otherwise evolving. Part IV returns to this possibility.

In addition, while deception claims have dominated the FTC's enforcement activity over the past decade, they are only part of the story. Recall that the Commission's UDAP authority also empowers it to pursue claims that sound in unfairness.[55] Tracing the agency's unfairness precedents helps to clarify the contours of the Window afforded by the historic configuration of social and institutional norms and sustained by Congress and the courts. Begin, as the agency must, with the controlling legal test for unfairness: as codified in Section 45(n) of the FTC Act, the FTC must assess whether "benefits to consumers or to competition" outweigh the alleged injury.[56] In this analysis, the FTC is

52. JOSHUA D. WRIGHT, DISSENTING STATEMENT OF COMMISSIONER JOSHUA D. WRIGHT IN THE MATTER OF NOMI TECHNOLOGIES, INC. 2 (2015) https://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwright statement.pdf [https://perma.cc/M56S-T8DK].

53. *Id.* at 4.

54. MAUREEN K. OHLHAUSEN, DISSENTING STATEMENT OF COMMISSIONER MAUREEN K. OHLHAUSEN IN THE MATTER OF NOMI TECHNOLOGIES, INC. 1 (2015) https://www.ftc.gov/system/files/documents/public_statements/799571/150828nomitech mkostatement.pdf [https://perma.cc/JX66-M835].

55. See discussion *supra* text accompanying note 41.

56. 15 U.S.C. § 45(n) (2021).

permitted to consider "established public policies . . . with all other evidence," yet "such public policy considerations may not serve as the primary basis for such determinations."[57]

How has the FTC applied this test? In the past, perhaps reflecting a cautious interpretation and reluctance to invoke the unfairness standard, the FTC has most frequently invoked its unfairness authority in situations that could be pegged to external metrics, rather than relying too much on an underlying substantive understanding of harm or social values at stake. This small-c conservative tack has allowed the agency to proceed without specifying an underlying normative theory, surfacing latent ideological commitments, or needing to expend resources to fend off allegations that public policy is the primary basis for the determination in a way that exceeds the agency's statutory authority.[58]

Data security-based unfairness actions are illustrative. Such enforcement actions may be understood as an attempt to exercise unfairness authority by tapping into industry guidelines and established best practices, thereby avoiding the appearance of de novo, normative policy choices.[59] In contrast to a privacy action, which implicitly or explicitly embraces a substantive understanding of which consumer privacy interests are worth protecting, data security is in principle easier to peg to specific, seemingly objective shortcomings.[60]

To make these points more concrete, consider the FTC's first data security action that included an unfairness claim, *In the Matter of BJ's Wholesale Club*.[61] Here, the agency pointed to specific issues concerning "personal information collected at [BJ's] stores," such as the company's failure to "encrypt the information while in transit or when stored on the in-store computer networks"; failure to "use readily available security measures to limit access to its computer networks through wireless access points on the networks"; failure to "conduct security investigations"; and failure to delete stored information after "it no

57. *Id.*

58. *Cf.* Andrew D. Selbst & Solon Barocas, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law*, 171 U. PA. L. REV. 1023, 1056 (2023) (arguing that the public policy language in Section 45(n) "sounds like a stronger prohibition than it is" and lamenting how courts have at times construed it as a further constraint on FTC authority).

59. This Essay reserves the related but distinct question of whether the FTC has provided adequate notice of its data security standards. For scholarship on point, see, e.g., Hurwitz, *supra* note 39 at 959; Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 130–31 (2008).

60. *See* Solove & Hartzog, *New Common Law of Privacy*, *supra* note 4, at 627 (discussing data security as an area in which it is easier to assess "the company's conduct and see[] to what extent it measures up to industry standards writ large" (quoting email from David Vladeck, Dir., Bureau of Consumer Prot., to authors (Oct. 3, 2013, 1:12 PM))); *id.* at 651–56 (canvassing FTC actions in data security and identifying specific metrics).

61. Complaint, BJ's Wholesale Club, Inc., FTC Docket No. C-4148 (Sept. 23, 2005).

longer had a business need to keep the information, and in violation of bank rules."[62]

Data security allegations of this sort feature prominently in more recent unfairness actions, too. The FTC's data security actions have continued to reference extrinsic, seemingly more objective baselines. As just one example, in *D-Link Systems*, the FTC highlighted the company's failure to protect against security flaws that had been "ranked among the most critical and widespread vulnerabilities" for nearly a decade.[63]

This kind of data security claim dominates the FTC's unfairness allegations. Across all complaints that included both a deception and unfairness allegation, the unfairness component of nearly two-thirds sounded in whole or in large part on data security issues.[64] To be sure, the FTC may need to be judicious to ensure that there is enough of an external benchmark against which to enforce, especially in the wake of the Eleventh Circuit's 2018 decision vacating the Commission's order in *In the Matter of LabMD*.[65] But that phenomenon is itself the mark of a desire not to disturb the status quo: the FTC is apt to seek out enforcement opportunities that allow for the imposition of rule-like factors and seem to require less independent judgment. Data security remains such

---

62. *Id.* at 2.

63. Complaint for Permanent Injunction and Other Equitable Relief ¶ 15, FTC v. D-Link Sys., Inc., No. 3:17-cv-00039-JD (N.D. Cal. Jan. 5, 2017).

64. Out of twenty-three total such complaints, fifteen (65%) fall in this category. *See, e.g.*, Complaint, Chegg, Inc., FTC Docket No. C-4782 (Jan. 26, 2023); Complaint, Drizly, LLC, FTC Docket No. C-4780 (Oct. 24, 2022); Complaint, Cafepress, FTC Docket Nos. C-4768 & C-4769 (June 24, 2022); Complaint, Skymed Int'l, Inc., FTC Docket No. C-4732 (Feb. 5, 2021); Complaint, Zoom Video Commc'ns, Inc., FTC Docket No. C-4731 (Feb. 1, 2021); Complaint for Permanent Injunction and Other Relief, FTC v. Equifax, No. 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019); Proposed Stipulated Order for Injunction and Judgment, FTC. v. D-Link Sys., Inc., No. 3:17-CV-39-JD (N. D. Cal. July 2, 2019); Complaint, ClixSense.com, FTC Docket No. C-4678 (July 2, 2019); Complaint for Permanent Injunction and Other Equitable Relief, FTC v. AshleyMadison.com, No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016); Complaint, Lenovo, Inc., FTC Docket No. C-4636 (Jan. 2, 2018); Complaint, ASUSTeK Comput., Inc., FTC Docket No. C-4587 (July 28, 2016); Complaint, GMR Transcription Servs., Inc., FTC Docket No. C-4482 (Aug. 21, 2014); Complaint, GeneLink, Inc., FTC Docket No. C-4456 (May 12, 2014); Complaint, foru Int'l Corp., FTC Docket No. C-4457 (May 12, 2014); Complaint, TRENDnet, Inc., FTC Docket No. C-4426 (Feb. 7, 2014). In addition, three stand-alone unfairness claims, *InfoTrax Systems*, *LabMD*, and *Accretive Health*, focus solely on data security; one other, *In the Matter of LightYear Dealer Technologies*, alleges an unfairness count based solely in data security along with alleged violations of the Gramm-Leach-Bliley Act Safeguards Rule. Complaint, Infotrax Sys. L.C., FTC Docket No. C-4696 (Jan. 6, 2020); LabMD, Inc. v. FTC, 894 F.3d 1221, 1225 (11th Cir. 2018); Complaint, Accretive Health, Inc., FTC Docket No. C-4432 (Feb. 24, 2014); Complaint, Lightyear Dealer Techs., LLC, FTC Docket No. C-4687 (Sept. 6, 2019). If these four complaints are included, then nineteen out of a total of thirty-eight complaints (50%) that involve either deception and unfairness or stand-alone unfairness claims focus on data security allegations.

65. *LabMD*, 894 F.3d at 1224. *But see* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247, 256 (3d Cir. 2015) (confirming FTC authority to issue data security order and finding that the Commission had provided adequate notice of which actions could be considered "unfair").

an option; indeed, nearly half of the data-security based unfairness complaints analyzed for this Essay were filed after the resolution of *LabMD*.[66] When it pursues an action of this type, the FTC can enforce in a way that appears more clearly within the bounds of its Window at a particular point in time, without any expansion or shift in the enforcement space.

That said, even within this fixed space of enforcement possibility, there is room for the agency to proceed in a number of directions. Another unfairness option available to an FTC that seeks to enforce without disturbing institutional norms is to connect its actions to a different external source of legal authority.[67] Such allegations can draw on another substantive area that is covered by other statutes, such as children's privacy or health information. The FTC may explicitly "double dip[]" by including counts under both the FTC Act and another statute or regulation that it enforces,[68] like COPPA or the Health Breach Notification Rule.[69] Or it may implicitly draw on concepts, such as health privacy or financial privacy, that already have traction within the sectoral approach to privacy protection. These actions involve more of a substantive question, but they do not require the Commission to signal a distinct normative commitment of its own.

Consider, as one illustrative example of both tactics, matters that center on the privacy of financial information. The entrenched and accepted understanding of financial information as a category of consumer data that must be protected permits the FTC to assert unfairness arguments without significantly shifting the Window or generating a reactionary squeeze by courts or by Congress. In the 2021 complaint for *United States v. Vivint Smart Home*,[70] for instance, the FTC included both a stand-alone unfairness count and a count for alleged violations of the FCRA that "constitute unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act."[71] The Commission's unfairness argument hinged on alleged "unfair sale of false debt to debt

66. Seven of the fifteen unfairness-only complaints fall in this category. *See* Complaint, Chegg, FTC File No. 2023151; Complaint, Drizly, LLC, FTC Docket No. C-4780; Complaint, Cafepress, FTC Docket Nos. C-4768 & C-4769; Complaint, Skymed Int'l, Inc., FTC Docket No. C-4732; Complaint, Zoom Video Commc'ns, Inc., FTC Docket No. C-4731; Complaint for Permanent Injunction and Other Relief, FTC v. Equifax, No. 1:19-mi-99999-UNA; Complaint, ClixSense.com, FTC Docket No. C-4678.

67. Incidentally, if a court is assessing whether to apply the major questions doctrine to an FTC enforcement action, this move might also insulate the agency against charges that its enforcement is "novel" in ways that make the question "major." *See* Daniel Deacon & Leah Litman, *The New Major Questions Doctrine*, 109 VA. L. REV. 1009, 1070 (2023) ("The Court's major questions cases have increasingly relied on an anti-novelty principle[.]"); Philips & Baumann, *supra* note 10 (manuscript at 10) (citing Deacon & Litman).

68. Solove & Hartzog, *New Common Law of Privacy*, *supra* note 4, at 663.

69. 16 C.F.R. pt. 318 (2022).

70. No. 2:21-cv-0026-TS (D. Utah 2021).

71. *Id.* ¶¶ 41–45.

buyers or collectors."[72] These consumer privacy interests are closely related to financial interests addressed by other statutes, such as the Fair Credit Reporting Act or the Gramm-Leach-Bliley Act ("GLBA").[73] Here, and in other similar cases, the actions entail a substantive understanding of privacy harms based on a normative assessment of which interests are worth protecting. But the close nexus to a noncontested category (financial information) has allowed the FTC to expand its enforcement without generating internal disagreement,[74] challenging internal norms, or creating external conflict.

The FTC has, moreover, pursued unfairness actions that similarly feature financial information, yet which sound only in the FTC Act. A striking example comes from a trio of actions undertaken in 2014: *FTC v. Bayview Solutions, LLC*,[75] *FTC v. Cornerstone and Company*,[76] and *FTC v. Sitesearch Corporation*,[77] each of which involved a firm's collection of and improper attempts to monetize sensitive consumer data. In *Bayview* and *Cornerstone*, the FTC alleged that the debt brokers "exposed highly sensitive information about tens of thousands of consumers while trying to sell portfolios of consumer debt on a public website."[78] In *Sitesearch*, the FTC alleged that the data broker "purchased sensitive information, including Social Security and bank account numbers, from pay-day-loan websites, and then sold that information to entities it knew had no legitimate need for it."[79] In these instances, there was no asserted violation of a statute, yet the close connection to established categories of sensitive financial information permitted the FTC to rely on unfairness, while still seeming to avoid more

72. *Id.* ¶¶ 46–50.

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

74. This appearance may to some extent be an artifact: the four actions discussed in this section were each brought in federal court, rather than pursued as administrative proceedings, and so there were no dissenting statements filed. That said, in three of the four, the Commission voted 5-0 to file a complaint; in *Vivint Smart Homes*, the vote was 4-0, with Commissioner Rohit Chopra issuing a separate statement that advocated for more aggressive remedial intervention on behalf of injured consumers. *See* ROHIT CHOPRA, STATEMENT OF COMMISSIONER ROHIT CHOPRA IN THE MATTER OF VIVANT SMART HOME (2021), https://www.ftc.gov/system/files/documents/public_statements/1589544/final_chopra_statement_on_vivint.pdf [https://perma.cc/295Y-EA2Z].

75. No. 1:13-cv-01830, 2015 U.S. Dist. LEXIS 193839 (D.D.C. Apr. 20, 2015).

76. No. 1:14-cv-01479 (D.D.C. Apr. 21, 2015).

77. No. 2:14-cv-02750 (D. Ariz. Dec. 11, 2015).

78. Press Release, Fed. Trade Comm'n, Debt Brokers Settle FTC Charges They Exposed Consumers' Information Online (Apr. 13, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/04/debt-brokers-settle-ftc-charges-they-exposed-consumers-information-online [https://perma.cc/K2SH-DXXQ].

79. Press Release, Fed. Trade Comm'n, Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers (Feb. 18, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive-personal-information-scammers [https://perma.cc/HD9P-6XPZ]; *see also* Complaint for Permanent Injunction and Other Equitable Relief ¶ 45, FTC v. Sitesearch Corp., No. 1:14-cv-01479 (D.D.C. Apr. 21, 2015).

explicit normative calls of its own. Where, as here, the Commission can proceed with a nexus to a sufficiently entrenched privacy interest, it can lessen the burden of establishing that there is a cognizable violation and make its case easier to establish — without any other change in the enforcement space itself.

Extrapolating from these matters suggests that a Commission that wishes to operate squarely within the Window can act strategically by demonstrating how any FTC Act argument that demands a more normative judgment is in fact connected to another substantive body of law. That is just what the Commission has done in the past: out of all stand-alone unfairness allegations filed between March 2013 and March 2023, two-thirds involve topics commonly understood to be sensitive, such as health information, financial information, or children's information;[80] intrusions in the consumer's home, a domain traditionally understood to be private;[81] or both.[82] To this extent, enforcement that falls squarely within an entrenched Window does not necessarily thwart the ability to redress new harms. But if there does not happen to be a preexisting body of law, then enforcing within an entrenched Window may still limit the ways that the FTC can proceed. The next Part considers how a distinct source of external authority, social norms, in tandem with a willingness to alter internal institutional norms, may

80. These actions are Complaint, Lightyear Dealer Techs., LLC, FTC Docket No. C-4687 (Sept. 6, 2019) (financial information, with counts for alleged violations of both FTC Act and GLBA Safeguards Rule); Complaint for Civil Penalties, Permanent Injunction and Other Relief, United States v. Vivint Smart Homes, Inc., No. 2:21-cv-00267-TS (D. Utah Apr. 29, 2021) (financial information, with counts for alleged violations of both FTC Act and FCRA; see discussion *supra* text accompanying notes 70–74); Complaint for Permanent Injunction, Civil Penalties, and Other Relief, United States v. Epic Games, Inc., No. 5:22-CV-00518 (E.D.N.C. Dec. 19, 2022) (children's information, with counts for alleged violations of both FTC Act and COPPA Rule); Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Katrina Moore, No. 5:18-cv-01960 (C.D. Cal. Sept. 13, 2018); Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Integrated Flight Solutions LLC, No. 3:18-cv-1658 (D. Or. Sept. 13, 2018) (financial information, such as fake paystubs and fake tax returns, with counts solely under FTC Act); Complaint for Permanent Injunction and Other Equitable Relief, FTC v. MyEx.com, No. 2:18-cv-00035 (D. Nev. Jan. 9, 2018) (financial information and non-consensual intimate imagery, with counts for alleged violations of FCRA, Telemarketing Sales Rule, and FTC Act); Complaint for Permanent Injunction and Other Equitable Relief, *FTC v. Bayview Solutions, LLC*, No. 1:14-cv-01830 (Oct. 31, 2014) (financial information, with counts for alleged violations of FTC Act; see discussion *supra* text accompanying notes 75–79); Stipulated Final Order for Permanent Injunction, *Cornerstone*, No. 1:14-cv-0147 (Apr. 21, 2015) (same); Complaint for Permanent Injunction and Other Equitable Relief, *Sitesearch*, No. 2:14-cv-02750 (Dec. 23, 2014) (same).

81. *See In the Matter of Aaron's* (permitting access to webcams inside consumers' homes and exposing intimate behavior as well as allowing collection of sensitive personal information, such as financial information, medical information and geolocation). Complaint at 2, Aaron's, Inc., FTC Docket No. C-4442 (Mar. 11, 2014). For scholarship on the importance of intimate privacy, see, e.g., DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE (2022); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019).

82. Ten out of fifteen total unfairness actions involve one or more of the identified categories of sensitive information.

support outright shifts in or expansion of the FTC's Overton Window of Enforcement Possibility.

IV. THE DYNAMIC WINDOW: EVALUATING PRIVACY ENFORCEMENT'S PRESENT AND FUTURE

This Part analyzes some of the FTC's more recent enforcement moves and contends that past enforcement precedents do not dictate the present and future, yet external forces as well as internal norms do mediate what is possible for privacy enforcement. It argues that shifts in privacy enforcement's Overton Window have occurred predominantly where there is a thick social consensus that supports the FTC's activities, especially when coupled with an internal willingness to alter institutional norms. It then builds from the framing presented in Part II and contends that it is not possible to assess whether such an evolution marks an expansion of enforcement space over the medium and long-term without also considering the other forces that bear on the Window: actions by the courts and by Congress.

As Part III suggests, privacy enforcement may fall less crisply within the Window when there is both no direct connection to existing sectoral protections and no clear measuring stick against which to assess violations. Claims involving location data illustrate these challenges.[83] Such actions involve a substantive judgment because there is no legal authority, external benchmark, or industry standard to invoke when it comes to the collection or use of location data. Although Fourth Amendment jurisprudence has long emphasized protection of the home, and the Supreme Court has recognized the significance of location tracking with respect to government surveillance,[84] there are no federal sectoral information privacy protections for this category of data.[85]

Assuming there's no simple, less controversial deception allegation available, a lack of firm legal baselines means that making the case for an unfairness-based location data allegation is harder in at least two ways. For one, it is harder because more evidence and more resources are necessary to conduct a compelling cost-benefit analysis of the injury versus the benefits to the consumer or to competition in the way

83. Thank you to Danielle Keats Citron for especially helpful discussions concerning location data.

84. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (recognizing how timestamped cell phone location "data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'" (quoting United States v. Jones, 565 U.S. 400, 415 (2012))).

85. *See* Stacey Gray & Pollyanna Sanderson, *Policy Brief: Location Data Under Existing Privacy Laws*, FUTURE PRIV. F., at 2–7 (Dec. 2020), https://fpf.org/wp-content/uploads/2020/12/FPF_Guide_Location_Data_v2.2.pdf [https://perma.cc/U68Q-X95D].

that the legal standard demands. For another, it is harder because it is difficult to appraise the extent of the injury itself without an underlying substantive theory. A fulsome evaluation of the privacy harm is critical for the unfairness analysis because it is otherwise impossible to weigh the costs to consumers, and whether they are "reasonably avoidable by consumers themselves," against the potential "benefits to consumers or to competition" from the business models that rely on this data.[86] Properly assessing the harm requires accounting for the range of interests affected by location data, including the ways in which inferences drawn from combinations of location data and other data may expand relevant privacy considerations.[87]

An unfairness-based enforcement action involving location data is thus inevitably normative. For instance, in assessing the injury, how much should one account for potential disparate effects on marginalized populations?[88] How much should one be concerned with incorrect inferences drawn from collected data?[89] Reasonable minds may differ on these matters, depending on ideological commitments about the nature of the market and the consumer's relationship to it. Yet the legal test for unfairness demands resolution of these issues.

Critically, although the need to answer such questions places such an action less squarely within the FTC's past enforcement space, that does not necessarily mean that it falls outside of the Window. Recall that the contours of the Window will depend in part on institutional norms. If the agency's leadership determines that it does not place a high priority on bipartisan consensus, and/or if commissioners decide that it makes sense to invest resources to espouse a different ideological vision of consumer protection, even if the agency ultimately loses in court,[90] then shifted internal norms can themselves expand the Window.

Recall, too, that social norms can work to expand, contract, or move the Window. When social norms about a particular topic evolve — as has been the case with thickening societal consensus that

---

86. 15 U.S.C. § 45(n).

87. *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361 (2022).

88. *See, e.g.*, Citron & Solove, *Privacy Harms*, *supra* note 44, at 856 (identifying how "misuse of personal data can be particularly costly" for historically marginalized populations and pinpointing how location data sharing can "expose [women and minorities] to physical danger").

89. *Cf.* Alice Xiang, *Being "Seen" Versus "Mis-Seen": Tensions Between Privacy and Fairness in Computer Vision*, 36 HARV. J.L. & TECH. 1, 34–45 (2022) (distinguishing, in the context of human-centric computer vision systems, between "harms of being seen" and "harms of being mis-seen," and discussing each category of harms).

90. *Cf.* David McCabe, *Why Losing to Meta in Court May Still Be a Win for Regulators*, N.Y. TIMES (Dec. 7, 2022), https://www.nytimes.com/2022/12/07/technology/meta-vr-antitrust-ftc.html [https://perma.cc/2ZL7-HTDG] (quoting FTC Chair Lina Khan's statements, in the antitrust context: "I'm certainly not somebody who thinks that success is marked by a 100 percent court record").

location data is sensitive — then an FTC action involving that topic may be more squarely within the realm of viable enforcement options. To be sure, a social norm may reflect the opinions of policy elites, the trade press, legal academics, or the bar, and not the population writ large. Furthermore, pursuing an enforcement action on this basis still requires difficult normative evaluations in ways that might run up against entrenched institutional norms or ideological commitments. Nonetheless, amply thick social consensus (even from an "undemocratic" sampling of the population) might provide support for distinct ideological stances within the agency, thereby expanding the enforcement space.

Location data seems like an example of a shift in the Overton Window of Enforcement Possibility in the face of evolving social norms. There has been a growing political and popular consensus about the sensitivity of this information. State attorneys general have recognized the sensitive nature of such information for nearly a decade,[91] and mainstream media outlets have published investigations drawing public attention to this topic.[92] Federal legislators have repeatedly introduced bills that would provide greater protection of location data,[93] and officials at the FTC itself have spoken about the importance of protecting location data in public testimony and in policy statements.[94] In addition,

---

91. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 782 (2016) (discussing New York Attorney General's investigation of Uber for its "internal location tracking system"); *id.* at 780 (discussing Texas Attorney General's actions against app providers that improperly collected location data from children); Danielle Citron, *BEWARE: The Dangers of Location Data*, FORBES (Dec. 24, 2014, 3:04 PM), https://www.forbes.com/sites/daniellecitron/2014/12/24/beware-the-dangers-of-location-data [https://perma.cc/73GC-EK5C] (discussing then-California Attorney General Kamala Harris's warning to constituents concerning location data).

92. *See, e.g.*, Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/UG74-DCT6].

93. *See* Davis Wright Tremaine, *Updated Location Privacy Protection Act Introduced*, PRIV. & SEC. L. BLOG (Apr. 3, 2014), https://www.dwt.com/blogs/privacy--security-law-blog/2014/04/updated-location-privacy-protection-act-introduced [https://perma.cc/J8UE-KZ5W] (discussing the Location Privacy Protection Act of 2014, an update to a bill initially proposed in 2011).

94. *See* Press Release, Fed. Trade Comm'n, FTC Testifies on Geolocation Privacy (June 4, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/06/ftc-testifies-geolocation-privacy [https://perma.cc/MJD4-UEY4] (summarizing FTC's enforcement, testimony, and policy activities in this space, as of 2014); *Prepared Statement of the Federal Trade Commission on S.2171 the Location Privacy Protection Act of 2014 Before the United States S. Comm. on the Judiciary, Subcommittee for Priv., Tech. and the L.*, 113th Cong. (2014), https://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf [https://perma.cc/V4SD-N7QY] (prepared statement accompanying 2014 congressional testimony by FTC Director of the Bureau of Consumer Protection). For a more recent statement emphasizing the sensitive nature of location data, see Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FTC BUS. BLOG (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-

legal scholars have long underscored how location tracking can engender a host of harms, facilitating abuses that include tracking, stalking, harassment, and physical harm, not to mention the revelation of sensitive information and the prospect of discriminatory profiling or other life-altering decisions based on such disclosures.[95] An FTC enforcement action involving location data can, in short, draw on social consensus that has accreted for years.

This thick social consensus helps to explain the FTC's 2022 action involving a data broker, Kochava. The initial complaint included a single count for "unfair sale of sensitive data," alleging that Kochava "sold, licensed, or otherwise transferred geolocation data" that, in combination with "unique persistent identifiers," revealed when consumers visited sensitive locations such as mental health providers, medical practitioners, places of religious worship, shelters for domestic violence survivors, and addiction recovery centers.[96] This approach sits in contrast to prior actions concerning location data. For instance, in *United States v. OpenX Technologies*,[97] the FTC relied on its deception authority and alleged that a company operating a "real-time bidding platform" for online and mobile advertising space made false and misleading statements about its collection of consumer location data.[98] That permitted the Commission to avoid political controversy and operate within the established Window.

In contrast, *Kochava*'s unfairness count goes to the heart of the firm's business model and seeks an injunction to bar the firm's allegedly invasive activities. The complaint highlights how the firm's ability

---

other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [https://perma.cc/A53K-FL63].

95. *See, e.g.*, Solove & Citron, *Risk and Anxiety*, *supra* note 44, at 754 (discussing visceral and vested harms); *see also* Michelle Boorstein & Heather Kelly, *Catholic Group Spent Millions on App Data that Tracked Gay Priests*, WASH. POST (Mar. 9, 2023, 8:52 AM), https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops [https://perma.cc/PT7U-4HRB] (reporting on use of commercially purchased mobile app tracking data, including location data, to out gay priests).

96. Complaint at ¶ 36, FTC v. Kochava, Inc., No. 2:22-cv-377 (D. Idaho Aug. 29, 2022) (FTC). The FTC has since filed an amended complaint. *See* discussion *infra* text accompanying note 101. This Essay focuses on the initial complaint, both for illustrative purposes and because the amended complaint was filed under seal. *See* Allison Grande, *Kochava Fights to Keep FTC's 'False' Privacy Claims Sealed*, LAW360 (June 15, 2023, 10:33 PM), https://www.law360.com/articles/1689403/kochava-fights-to-keep-ftc-s-false-privacy-claims-sealed [https://perma.cc/HU5F-29LW].

97. No. 2:21-cv-09693 (C.D. Cal. 2021).

98. *Id.* at ¶¶ 13, 34–45. Notably, the *OpenX* matter also included alleged violations of the COPPA Rule, thereby also connecting the violations at issue to a privacy interest (children's information) that is comparatively uncontroversial and already well-recognized by formal legal protections. For a similar action involving location data that sounds in deception, *see* Complaint ¶¶ 15, 18, Goldenshores Techs., LLC, FTC Docket No. C-4446 (Apr. 9, 2014) (alleging that makers of a flashlight application made deceptive representations concerning the transmission of location data); *see also* Hartzog & Solove, *FTC Data Protection*, *supra* note 5, at 2275–76.

to collect, aggregate, and share data that is capable of revealing extraordinarily intimate facts permits Kochava to intrude too far into consumers' private lives.[99] Notably, the FTC's original complaint did not include any specific allegations of concrete harm to an identified individual that resulted or could result from Kochava's conduct,[100] leading the district court to initially grant Kochava's motion to dismiss with leave to file an amended complaint.[101] No matter how *Kochava* is ultimately resolved, the initial decision to bring this matter and the subsequent response from the company and the court highlight three critical lessons.

First, because *Kochava* lays bare the ideological choices under the surface of unfairness claims, it exposes how shifting social and institutional norms can expand the Window. On social norms, a thickening consensus about the sensitivity of this data preceded enforcement.[102] Without such norms, it is not obvious that the FTC would have felt emboldened to pursue *Kochava*. Social norms thus promoted conditions for an expansion of the Window. On institutional norms, when the FTC is willing to risk more politically contentious stances, it can potentially expand the Window.[103] It does not seem possible to resolve *Kochava* without embracing a substantive theory about the FTC, the relationship between consumers and the market, what sort of injury is or is not enough to satisfy the unfairness test, and how to conduct cost-benefit analysis in a way that reflects a correct understanding of these concepts. In the past, the FTC's desire to avoid partisan controversy may have led the Commission to conceptualize an action like *Kochava*

---

99. *See* Kyle R. Dull, Kristin L. Bryan & Brianna Soltys, *Federal Trade Commission's Enforcement Action Against Data-Broker Kochava Heats Up With Motion To Dismiss Briefing And Upcoming Hearing*, NAT'L L. REV. (Feb. 20, 2023), https://www.natlawreview.com/article/federal-trade-commission-s-enforcement-action-against-data-broker-kochava-heats [https://perma.cc/UUR3-PKPM] ("[Kochava's] intrusion into a consumer's private life without the proper controls over access and use, the FTC claims, constitutes an illegal and unfair business practice.").

100. *See* Nancy L. Perkins, Kristina Iliopoulos & Jason T. Raylesberg, *FTC Files Complaint Against Data Broker Kochava Inc. for Sale of Sensitive Geolocation Data*, ARNOLD & PORTER ENF'T EDGE BLOG (Sept. 27, 2022), https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2022/09/ftc-files-complaint-against-data-broker [https://perma.cc/H2Y3-C2T5].

101. FTC v. Kochava, 671 F. Supp. 3d 1161, 1180 (D. Idaho 2023). After this Essay was substantively finalized, the district court denied Kochava's motion to dismiss the FTC's amended complaint. *See* FTC v. Kochava, No. 2:22-CV-00377, 2024 WL 449363, at *5 (D. Idaho Feb. 3, 2024).

102. *See* discussion *supra* text accompanying notes 91–95.

103. Again, dissents can be a clue that an action involves such a choice. Kochava featured a 4-1 vote, with one of two Republican commissioners on the FTC at the time voting not to authorize the FTC staff to file the complaint against the company. *See* Press Release, Fed. Trade Comm'n, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other [https://perma.cc/U2RK-C5F8].

as outside the bounds of the Window. The current FTC takes a different line. It seems likely, for instance, that the FTC's initial complaint did not include any specific allegations of concrete harm because, to borrow Professor Arvind Narayan's turn of phrase, the FTC sees "the business model . . . [as] the privacy violation."[104] This move reflects a willingness to espouse a potentially more controversial position in a way that internal norms previously foreclosed.

Second, *Kochava* suggests how more cutting-edge actions that implicate ideological tradeoffs can fall within an expanded Window, yet still provoke pushback — including in ways that may winnow privacy enforcement in the middle and long-term. Rather than settle in the manner that nearly all FTC enforcement actions do,[105] Kochava is fighting the FTC's allegations, hard, in federal court. This litigation requires an outlay of additional resources from an already resource-constrained agency; functionally, it may limit which actions the FTC can undertake in the future, especially if Congress does not authorize adequate funding to support more vigorous enforcement. This outcome underscores how Congress, and the agency's reliance on it, affects the evolution of the Window in dynamic fashion.[106]

Third, *Kochava* illustrates how courts can constrain the FTC's enforcement space. The district court's May 2023 memorandum opinion and order stated that the FTC has not adequately established that "Kochava's practices create a 'significant risk' of concrete harm" under its first theory of consumer injury.[107] The court was also "somewhat skeptical" that deficiencies in the alleged "substantial injury" prong for the FTC's second theory of consumer injury "can be cured through an amended complaint."[108] Because judicial enforcement requires a court to make its own substantive assessment of the nature of the harm, courts can curtail the agency's more expansive theory of enforcement — and

104. Arvind Narayanan, *When the Business Model *is* the Privacy Violation*, FREEDOM TINKER BLOG (Apr. 12, 2018), https://freedom-to-tinker.com/2018/04/12/when-the-business-model-is-the-privacy-violation [https://perma.cc/XCM9-5V68].

105. Solove & Hartzog, *New Common Law of Privacy*, *supra* note 4, at 585.

106. It also hints at underlying questions of political economy concerning which kinds of regulated entities can and cannot afford to litigate and fight FTC settlements. These questions are especially salient insofar as privacy law represents a "responsive regulation" model wherein public and private actors collaborate in the governance project. *See generally* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 960 (2016) ("This Article argues that we should understand most privacy regulation through the prism of responsive regulation."). For discussion of how powerful private actors figure into the Window as articulated in this Essay, see discussion *supra* text accompanying note 23.

107. FTC v. Kochava Inc., 671 F. Supp. 3d 1161, 1175 (D. Idaho 2023) (quoting FTC. v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 2010)).

108. *Id.* at 1176.

if the agency loses, the negative precedent might narrow its future Overton Window of Enforcement Possibility.[109]

As a strategic matter, then, the question for the FTC becomes whether even an action that ostensibly falls within the Window might, if pursued, produce a response that narrows the range of actions available over time. Privacy enforcement is not a static choice, made by the FTC alone. The space for enforcement occurs within a dynamic and multifaceted Window, and Congress and the courts affect its shape as much as the agency does. The next Part canvasses considerations for the FTC in the face of these strategic tradeoffs.

V. LESSONS FOR ENFORCEMENT AT THE FTC AND BEYOND

The Window teaches us that privacy enforcement is not static, yet simultaneously imparts the difficult lesson that any one actor cannot control the Window. Evolution of the Overton Window of Enforcement Possibility is a process, with one force — such as a shift in internal institutional norms, or a shift in social norms that might afford space for the FTC to expand its own enforcement scope — intersecting with another force — such as a reactive shift by Congress or by the courts. What, then, is a resource-constrained agency that seeks to increase privacy enforcement and embrace a distinct, progressive ideology to do?

This Part offers pragmatic ways for the FTC to approach the future of privacy enforcement. As acknowledged below, these proposals have limits. Nonetheless, they can both empower internal actors — indeed, the FTC has already quietly implemented many of them — and inform external policymakers and scholars who are interested in expanding the enforcement authority of the FTC or other proposed tech regulators.[110]

One tack is to focus less on innovative theories of harm, and more on innovative remedies. Consider *In re Everalbum, Inc.*,[111] a matter in which the FTC relied on two deception counts alleging, respectively, that the company made false or misleading statements about users'

109. This Essay reserves the distinct, critical question of how courts can narrow the Window by constraining the remedies available to the FTC. *See* AMG Cap. Mgmt., LLC v. FTC, 141 S. Ct. 1341, 1344 (2021) (holding that Section 13(b) of the FTC Act does not "authorize[] the Commission to seek, and a court to award, equitable monetary relief such as restitution or disgorgement"). So, too, does it reserve the question of how judicial determinations that make it comparatively easier for parties to challenge the FTC in federal court might lead to an increase in litigation costs, thereby straining agency resources even more. *See* Axon Enter., Inc. v. FTC, 143 S. Ct. 890, 897 (2023) (holding that parties that object to FTC proceedings can bring claims in federal district court, and that these "district courts have jurisdiction to hear those suits — and so to resolve the parties' constitutional challenges" to agency structure). These developments make it even more important to consider the interaction between forces in assessing the overall enforcement space afforded by the Overton Window, sharpening this Essay's claims.

110. *See* discussion *supra* text accompanying notes 20–21.

111. Complaint, Everalbum, Inc., FTC Docket No. C-4743 (May 6, 2021).

ability to turn facial recognition on or off and did not abide by its pledges to delete users' data after deactivation.[112] The FTC's action represents a conventional and straightforward legal theory; it contains no mention of other harms from the use of facial recognition, nor any unfairness count that engages with these likely harms, despite the fact that one commissioner filed a statement that mentioned the potential for "providers of facial recognition to make false accuracy claims and engage in unfair, discriminatory conduct."[113] What is novel is the remedy: the FTC required Everalbum to delete not only all improperly collected data, but also all "models or algorithms developed in whole or in part" from this improperly collected data.[114] Now, this tack sacrifices the chance to develop a legal theory that redresses harms like discrimination or bias. Yet such a conservative initial foray into an area might strategically avoid skirmishes over the Commission's legal authority while supporting distinctive remedies and, perhaps, enabling the FTC to pursue more far-reaching future actions sounding in unfairness.[115]

Another approach is for FTC leadership to pursue what this Essay terms "insulating" strategies that attempt to diffuse the political contentiousness of a particular enforcement action. For instance, actions that are supported by both a changing social norm and a sectoral hook may afford more space for a different ideological understanding of consumer harm, particularly if the agency is also willing to shift its own internal norms. One illustrative example is a May 2023 charge involving a fertility app, Premom, that tracks ovulation, periods, and other sensitive health information.[116] The FTC's complaint not only included five counts of deception and two counts of unfairness, but also alleged a violation of the Health Breach Notification Rule for the second time

---

112. *Id.* at *6; *see also* Solow-Niederman, *supra* note 87, at 376–77 (discussing *Everalbum*).

113. Complaint at 2, Everalbum, Inc., FTC Docket No. C-4743.

114. Agreement Containing Consent Order at 2, Everalbum, Inc., FTC Docket No. C-4743 (Jan. 11, 2021).

115. The FTC has discussed the prospect of unfairness claims involving AI providers in two blog posts. *See* Michael Atleson, *The Luring Test: AI and the Engineering of Consumer Trust*, FTC BUS. BLOG (May 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust [https://perma.cc/NHN5-CC8T]; Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC BUS. BLOG (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai [https://perma.cc/V285-TTSJ].

116. Press Release, Fed. Trade Comm'n, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc [https://perma.cc/DSB8-XGAX]. I discuss *Premom* to highlight a notable contrast with past enforcement actions and to provide a concrete example of one possible future strategy for the FTC, but otherwise do not analyze enforcement actions filed after March 5, 2023.

in the Commission's history.[117] The agency's discussion of consumer injury includes a paragraph alleging "unauthorized disclosure of facts about individuals' sexual and reproductive health, parental and pregnancy status, as well as other information about . . . individuals' physical health conditions and status" that "is likely to cause Premom users stigma, embarrassment, or emotional distress, and may also affect their ability to obtain or retain employment, housing, health insurance, disability insurance, or other services."[118]

To state the obvious, this theory of harm differs tremendously from past theories that focus on impediments to consumer choice or transparency.[119] Notably, it is supported both by existing legal protections for health data enshrined in the Health Insurance Portability and Accountability Act of 1996[120] and in the Health Breach Notification Rule itself, and also by an emerging social consensus that fertility data is especially sensitive in the wake of *Dobbs v. Jackson Women's Health Organization*[121] and the overturning of *Roe v. Wade*.[122] These developments may have moved the Overton Window of Enforcement Possibility, such that an action like *Premom* now falls within it — even though, just over two years earlier, before *Dobbs*, and before the leadership of Chairperson Khan, the FTC pursued only deception claims in a similar action against another fertility app, Flo.[123]

In future potential actions, if the FTC seeks to similarly expand its enforcement in ways that embrace a thicker, normative understanding of harm, then it might consider strategically pursuing counts that can similarly reference evolving social norms, an existing body of law, or, ideally, both. Now, there may be limits to how quickly, or how much, the Window can move — leadership may only be able to leverage these shifts so much, and a too-rapid attempt to shift institutional norms could still provoke a pushback. Still, areas with social and sectoral support may provide insulation for the agency in the face of other, potentially countervailing forces, and thus may be especially ripe for expanded enforcement action.

The further difficulty, however, is that these insulating tactics are reactive, relying on prior developments outside of the FTC to diffuse potential controversy concerning the Commission's own unfairness claims. In domains without time or occasion to cultivate social norms

---

117. Complaint for Permanent Injunction at 22–28, Civil Penalty Judgement, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-3107 (N.D. Ill. May 17, 2023).

118. *Id.* at 17–18.

119. *See* discussion of *Nomi supra* Part III.

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

121. 142 S. Ct. 2228 (2022).

122. 410 U.S. 113 (1973).

123. Complaint, Flo Health, Inc., FTC Docket No. C-4747 (Jan. 13, 2021); *see also* Solow-Niederman, *supra* note 87, at 375–76 (discussing *Flo*).

and/or where there is not a source of law from which to draw, the FTC cannot avail itself of such an approach.

* * * * *

That is sobering news. Yet confronting these limits can be an opportunity. Conceptualizing privacy enforcement as an Overton Window positions the FTC to think strategically at the same time that it empowers scholars and policymakers to understand enforcement as a dynamic space, informed by social norms, internal institutional norms, Congress, and the courts. Moreover, the Overton Window of Enforcement Possibility reveals a vital lesson for enforcement at the FTC and at agencies beyond it: if the Window is too small, then little is possible. This Essay helps to provide tools to act on that lesson by specifying where an agency like the FTC might feel constrained, and why, as well as by clarifying how a shift in one force might produce a response by another. So, too, might this framework prompt administrative officials who seek to exercise their enforcement authority and legislators who seek to endow an agency with authority — such as congressmembers who propose expanding FTC authority as part of a federal privacy statute[124] — to consider institutional design; to account for the practical realities that an agency must confront, over time; and to think creatively about where there might be play in the joints. The work of enforcement is an ongoing process that unfolds in social, political, and legal context. Where an agency can go is not open and shut.

124. *See* proposed bills *supra* note 20.