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

PLATFORMS, PRIVACY, AND THE HONEYPOT PROBLEM

*Kirsten Martin**

ABSTRACT

Platforms are increasingly important in how we listen to music, watch movies, read news, maintain friendships, work, bank, shop, and travel. Whether Amazon, eBay, Sabre, Tinder, or the New York Stock Exchange ("NYSE"), each platform's goal is to facilitate an efficient match for market actors. Importantly, the governance polices of the platform are how platforms create value and differentiate themselves from their competitors when in a competitive market. However, when not in competitive markets, platforms may abuse market power through those same governance policies. For digital platforms with market dominance, privacy and data governance polices can serve as vehicles to abuse power, where the collection, storage, sharing, and use of data benefit the platform owner but harm market actors on the platform.

However, recent rulings and antitrust scholarship have too often looked past privacy governance as a mechanism platforms use to abuse market power. These courts and academics have gone so far as to override user privacy interests and preferences in the name of platform efficiencies and competition — some claiming that users have no privacy interests in the data collected by a platform.

In this Essay, I argue that antitrust scholars and courts have taken privacy shortcuts to mistakenly frame users as having no privacy interests in data collected by platforms. These privacy shortcuts — characterizing privacy as concealment or as protection from intrusion — justify platforms creating an attractive customer-facing platform to lure in customers and later exploit user data in a secondary platform or business. I call this the Honeypot Problem. As such, these privacy shortcuts hide an important mechanism used by platforms to abuse market power and justify the growth of honeypot platforms that act like a lure for consumers to collect their data only to later exploit that data in a different business.

I offer a positive account of privacy on platforms to show how the problems introduced by the privacy shortcuts can be resolved by understanding the norms of data governance for a given platform. Privacy on platforms is defined by the norms of appropriate flow — what data is collected, the conditions under which information is collected, with whom the data is shared, and whether data is used in furtherance of the

* William P. and Hazel B. White Professor of Technology Ethics, Mendoza College of Business, University of Notre Dame.

context of the platform. Norms of privacy and data governance — what and how data is collected, shared, and used — will differ when on LinkedIn versus Tinder, since each platform performs different functions and has different contextual goals, purposes, values, and actors. However, privacy and data governance norms are a mechanism by which these platforms differentiate and compete in a competitive market and abuse market power in less competitive markets.

TABLE OF CONTENTS

I. INTRODUCTION

Within the overall struggle to understand privacy online, platforms stand out as a particularly sticky issue. Contrary to traditional firms, digital platforms are able to collect, store, and aggregate a mosaic of data about their users and across many facets of our lives.[1] Platforms have become increasingly important in how we listen to music, watch movies, read news, maintain friendships, work, bank, shop, and travel.[2] Digital platforms have become imaginative in how to collect and create

1. Beatriz Kira, Vikram Sinha & Sharmadha Srinivasan, *Regulating Digital Ecosystems: Bridging the Gap Between Competition Policy and Data Protection*, 30 INDUS. & CORP. CHANGE 1337, 1340 (2021) ("A traditional firm can only collect data on its own customers, but a digital platform can access a vast amount of data related to all sellers and buyers on multiple sides of its platform.").

2. *See* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 614–15 (2011).

new types of data, as well as how to use, share, and exploit consumer data in facilitating transactions.[3]

Not surprisingly, privacy scholars have noticed this free flow of consumer data and questioned the types of data collected,[4] data harms created,[5] and inferences developed,[6] as well as how the data can be used against us by these platforms.[7] For example, data can be used to make us addicted[8] or to target individuals with less power or with specific vulnerabilities[9] due to the ability to create and facilitate informational harms.[10]

---

3. Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 589 (2021) ("Advertising techniques developed to predict or to influence behavior are increasingly gaining purchase in other industries. The same capabilities that help digital companies know (or claim to know) what attributes make someone likely to buy an advertised product, or that are leveraged to increase a desired behavior, can be used for other tasks. For instance, these techniques may be used to identify potential voters likely to engage on an issue or with a candidate, to identify what activities are associated with risky or risk-averse financial or health behavior, or to predict how much different people are willing to pay for the same product. . . . Overall, the digital economy powered by these behavioral techniques represents roughly $2.1 trillion, making it the fourth-largest industry in the United States.").

4. *See, e.g.*, Kirsten Martin & Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables*, 18 COLUM. SCI. & TECH. L. REV. 176, 183 (2016); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1128–30 (2015).

5. *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1132–33 (2011); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 796 (2022); Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1042–43 (2018).

6. *See, e.g.*, Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 360–64 (2022); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 497–98 (2019); Sandra Wachter, *The Theory of Artificial Immutability: Protecting Algorithmic Groups Under Anti-Discrimination Law*, 97 TUL. L. REV. 149, 157 (2022); Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 453 (2020).

7. *See, e.g.*, Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 451–53 (2019); Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 2–4 (2019); Kirsten Martin, *Manipulation, Choice, and Privacy*, 23 N.C. J.L. & TECH. 452, 455–57 (2022); Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 158–59 (2019).

8. *See, e.g.*, Vikram R. Bhargava & Manuel Velasquez, *Ethics of the Attention Economy: The Problem of Social Media Addiction*, 31 BUS. ETHICS Q. 321, 333–34 (2021).

9. *See, e.g.*, SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS 17–24 (2020); RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE 46–48 (2019); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 12–13 (2018); CATHERINE D'IGNAZIO & LAUREN F. KLEIN, DATA FEMINISM 53–57 (2020); Anna Lauren Hoffmann, *Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse*, 22 INFO., COMMC'N & SOC'Y 900, 901–03 (2019); Luke Stark & Jesse Hoey, *The Ethics of Emotion in Artificial Intelligence Systems*, 2021 ACM CONF. ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY 782, 788–89.

10. *See, e.g.*, Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346–48 (2014); Ari Ezra Waldman, *Law, Privacy, and Online Dating: 'Revenge Porn' in Gay Online Communities*, 44 L. & SOC. INQUIRY 987, 987 (2019); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1874 (2019).

And firms, including platforms, with dominant market power have strong incentives to externalize the costs of protecting privacy onto society.[11] Rather than seeking to further burden users, scholars have moved from focusing on the ability of individuals to manage and "negotiate" privacy preferences with platforms[12] to focusing on the obligations or duties that platforms should have for their users based on obligations of trust,[13] fiduciary duties, and obligations of loyalty.[14]

In the United States, the response to this chorus of voices — that platform users have robust, specific privacy interests and that platforms have associated duties to respect privacy interests of users — has been to continually narrow both what privacy means as well as the role of platforms in protecting privacy. Users are framed as not caring about privacy or caring so little as to "trade" their privacy interests away when on platforms.[15] Privacy is also framed as a hindrance to innovation and market efficiencies.[16] The story emerging from industry and platform governance scholarship is that either consumers do not care,[17] or consumers may care a little but trade privacy for platform engagement,[18] and nevertheless privacy may hinder innovation and efficiencies.[19] Within this narrative, privacy is fighting a losing battle: it is devalued, non-existent, or seen as counter to innovation.

As platforms grow in dominance, scholarship and courts have struggled to understand how privacy is a quality users look for in their

---

11. Gregory Day & Abbey Stemler, *Infracompetitive Privacy*, 105 IOWA L. REV. 61, 66 (2019).

12. *See* Viljoen, *supra* note 3, at 646–48 (discussing the move away from a focus on the individual to negotiate their interests in data governance on a platform); *see also* Alessandro Acquisti, *Privacy, Economics, and Regulation: A Note*, 24TH FIN. MKTS. CONF. ATLANTA FED. RSRV. BANK, May 2019, at 20–21 (discussing the inappropriate responsibilization of individuals asked to take on the impossible burden of understanding data flows and ensuring their privacy interests are met with online firms and platforms); Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, SCIENCE, Jan. 30, 2015, at 509, 509.

13. *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 79 (2018).

14. *See* Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356, 359–60 (2022) (describing a proposal for a data loyalty standard); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1214 (2017) (reviewing FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015)) (proposing requirements for data stewards); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 964–67 (2021) (proposing a data loyalty law).

15. *See infra* Section III.A.1 and notes 87–89.

16. Martin, *supra* note 7, at 475 n.73; *see also* Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 406 (1981); Erika M. Douglas, *Data Privacy as a Procompetitive Justification: Antitrust Law and Economic Analysis*, 97 NOTRE DAME L. REV. REFLECTION, 430, 447 (2022).

17. *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 2–3 (2021).

18. *See infra* Section III.A.1 and notes 87–89.

19. *See* Posner, *supra* note 16, at 406; Douglas, *supra* note 16, at 447.

choice of a digital platform. Recent rulings and scholarship have gone so far as to override user privacy interests and preferences in the name of platform efficiencies and competition.[20]

This disconnect between privacy research and platform antitrust scholarship and rulings is due to a misunderstanding of both (1) the goals and obligations of digital platforms and (2) the definition of privacy online. When taking privacy shortcuts, such as privacy as concealment or as protection from intrusion,[21] scholars, courts, and firms mistakenly frame users as having no privacy interest in the data collected by platforms. These privacy shortcuts justify platforms creating an attractive customer-facing platform to lure in customers and later exploit user data in a secondary platform or business. I call this the Honeypot Problem.

This Essay aims to make two contributions. First, I explain the mechanisms that platforms use to abuse market power through privacy and data governance policies. Second, I argue that current definitions of privacy that diminish privacy interests of users not only obscure this abuse of market power but also justify the growth of honeypot platforms that act like a lure for consumers to collect their data only to later exploit that data in a different business.

In Part II, I recenter the discussion of platforms as unique in creating a market or exchange for other actors.[22] Whether Amazon, eBay, Sabre, Tinder, or the New York Stock Exchange ("NYSE"), the goal of each platform is to facilitate an efficient match for market actors. Importantly, platforms use their governance polices to differentiate themselves from their competitors in a competitive market. However, in non-competitive markets, platforms may abuse market power through those same governance policies. For digital platforms with market dominance, privacy and data governance polices can serve as vehicles to abuse power, where the collection, storage, sharing, and use of data benefit the platform owner but harm market actors on the platform. For example, consider a social network that collects and uses user data not for the benefit of the user on the platform but to monetize that user data in a secondary market.

In Part III, I examine common shortcuts to defining privacy that obscure the anticompetitive behavior of platforms and justify the

---

20. *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1193–94 (9th Cir. 2022); *see* Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J.F. 647, 663–64; *see also infra* Section III.A.1.

21. *See* discussion *infra* Section III.A.1–2. The privacy as concealment shortcut claims that privacy interests are only in people or information that is hidden, and any recycled information has no privacy expectations. The privacy as protection from intrusion shortcut claims that privacy is preserved by keeping unwanted third parties from accessing data.

22. *See* Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1015 (2013); Avi Goldfarb & Catherine Tucker, *Digital Economics*, 57 J. ECON. LIT. 3, 10 (2019).

exploitation of user data. Convenient definitions of privacy, such as privacy as concealment or privacy as a lack of intrusion, are designed to allow firms to use and share the data however they wish and exclude others from offering a service on their platforms.[23]

I identify the Honeypot Problem where simplistic definitions of privacy provide the justification for platforms to create a honeypot: an attractive front-end platform that lures people into sharing their data only to then exploit the consumer data in a secondary market or platform.[24] Two justifications undergird the Honeypot Problem. Privacy as concealment justifies the consumer-facing platform as a lure in order to collect user data;[25] privacy as protection from intrusion legitimizes the exploitation of the consumer data in a secondary market. In this way, these privacy shortcuts obscure the abuse of market power by platforms, while also legitimizing the honeypot problem.

In Part IV, I offer a positive account of privacy on platforms to show how the problems introduced by the privacy shortcuts can be resolved by understanding the norms of data governance for a given platform. Privacy on platforms is defined by the norms of appropriate flow — what data is collected, the conditions under which information is collected, with whom the data is shared, and whether data is used in furtherance of the platform's contextual goals and purpose.[26] Every platform declares the context or social domain in which the platform collects data,[27] and the collection, storage, sharing, and use of data in furtherance of that context is considered appropriate and within the privacy norms for that platform. This approach to privacy — validated with empirical work — explains why individuals share data with platforms and expect that data to be used, shared, and stored within the context of the platform. Further, privacy as contextual integrity undermines both justifications of the Honeypot Problem.

Privacy as contextual integrity should be attractive for practice not only because the theory has been used and validated in empirical work, but also because the theory provides a path by which firms can respect user privacy while offering functionality, efficient exchanges, and innovation. However, privacy as contextual integrity does not justify an argument that consumers give up or trade privacy when they engage

---

23. *See* Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 1, 4–9 (2022).

24. A honeypot is a lure, a profit-sacrificing platform that is intended to attract users, like a decoy. The honeypot platform mimics a legitimate business but uses the user's interaction to gain information in order to then use that information in another business line or secondary platform. *See infra* Section III.B.

25. The more attractive, i.e., low-cost or free, the platform is for consumers, the more scholars and firms can argue that users have traded away their privacy interests by engaging with that platform. *See infra* Section III.B.

26. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 129 (2010).

27. *See infra* Part IV.

with a platform. Nor does privacy as contextual integrity support the exploitation of data for the benefit of the firm beyond the purpose for which it was shared — but neither do surveys of consumers.[28] While privacy as contextual integrity provides a roadmap for practitioners for how to respect privacy and justifies the collection, sharing, and use of consumer data in furtherance of the platform's context, the theory does not justify creating a lure for consumers to share their data only to exploit that data in another context.

II. PLATFORMS

The goal of a platform is to create a market and facilitate matches between platform participants.[29] For example, eBay enables transactions between buyers and sellers,[30] Netflix enables transactions between content and viewers,[31] Bing and Google Search enable a match between users and useful content online,[32] and the NYSE matches buyers and sellers of securities.[33] Where firms provide goods and services, platforms provide an exchange.

Further, platforms enact policies to make the exchange more efficient by decreasing transaction costs, including decreasing search costs, facilitating the execution of a transaction, and increasing the legitimacy of the exchange.[34] For example, setting a price format lowers bargaining and negotiating costs for buyers on the NYSE by making it easier to compare securities; rank ordering based on interest and location lowers search costs for renters on Airbnb; enforcing rules about fraud and legitimate economic actors lowers safeguarding costs on eBay. In each case, the platform's goal is to make transacting on the platform easier for users; and platforms differentiate themselves through these governance policies.

---

28. *See, e.g.*, Martin et al., *supra* note 4, at 204–07.

29. Goldfarb et al., *supra* note 22, at 4, 10.

30. *Our Company*, EBAY, https://www.ebayinc.com/company [https://perma.cc/3D6Z-HY7A] ("[W]e create pathways to connect millions of sellers and buyers . . . .").

31. *About*, NETFLIX, https://about.netflix.com/en [https://perma.cc/7K3L-GC4E] ("[W]e give you access to best-in-class TV series, documentaries, feature films and mobile games.").

32. *How Bing Delivers Search Results*, MICROSOFT, https://support.microsoft.com/en-au/topic/how-bing-delivers-search-results-d18fc815-ac37-4723-bc67-9229ce3eb6a3 [https://perma.cc/GQ5V-5H3D]; *How Results Are Automatically Generated*, GOOGLE SEARCH, https://www.google.com/search/howsearchworks/how-search-works/ranking-results [https://perma.cc/5EBW-VAP7].

33. *NYSE's Focus for U.S. Equity Markets: Quality, Transparency, Simplicity*, NYSE, https://www.nyse.com/article/market-focus [https://perma.cc/F2UY-G9DA].

34. Kirsten Martin, Hong Guo & Rob Easley, *When Platforms Act Opportunistically: The Ethics of Platform Governance* 9 (Nov. 2023) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4202821 [https://perma.cc/J3BB-AQB2] (identifying "three types of transaction costs of the economic actors on the exchange that can be affected by the platform company's governance policy decisions: search and information costs, bargaining and decision costs, and policing and enforcement costs").

Increasingly, firms have created platforms where the flow and use of data are core components of the value proposition.[35] While digital platforms abide by the same economic theories as traditional platforms,[36] the amount of data collected by these digital platforms can create a distraction for theorizing about platform governance. For example, some (mistakenly) argue these digital platforms are just different from any analog context,[37] or digital platforms are free or low-cost and require new approaches,[38] or the amount of data collected (whether in furtherance of the platforms' context or not) is what defines a platform, which is different from offline platforms.[39] However, the purpose of the platform, the measurements of market power, and the mechanisms to abuse market power remain consistent whether or not a platform relies on or collects a "large" amount of user data.

A. Platforms as Unique

Platforms differ from traditional firms in creating a market for others to transact. As such, how we assess their competitive attributes shifts to a focus on their policies rather than on mere consumer price.

1. Platforms Compete on Policies Rather Than on Consumer Price.

For traditional firms, price is an important component of demand for the product being sold.[40] However, for platforms, the service being offered is the exchange, and the price and quality of goods sold on the exchange is an outcome of the exchange not set by the platform; eBay does not set prices for consumer goods on its platform, and the NYSE does not set prices for securities on its platform.[41] Where firms compete on price, platforms compete on policies. And for digital platforms, with

35. *See* Kira et al., *supra* note 1, at 1340–41.

36. *See* Catherine Tucker, *Digital Data, Platforms and the Usual [Antitrust] Suspects: Network Effects, Switching Costs, Essential Facility*, 54 REV. INDUS. ORG. 683, 683–84 (2019).

37. *See* Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECH. L.J. 1051, 1053–54 (2017).

38. John M. Newman, *Antitrust in Digital Markets*, 72 VAND. L. REV. 1497, 1502, 1545 (2019) (arguing that digital platforms demand unique treatment due to the problem of zero price and that we pay with "data and attention").

39. Contrary to the argument herein, Professors Pamela Harbour and Tara Koslove see digital platforms as being defined by their data rather than the exchange they offer to economic actors. Pamela Jones Harbour & Tara Isa Koslove, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769, 773 (2010) ("[W]e suggest the definition of markets for data, separate and apart from markets for the services fueled by these data. . . . Data market definition also would properly recognize the increased significance and value of the massive and growing data troves that constantly are generated by Internet activities.").

40. David S. Evans & Richard Schmalensee, *Multi-sided Platforms*, *in* THE NEW PALGRAVE DICTIONARY OF ECONOMICS 4 (3d ed. 2018).

41. *Id.*

their reliance on consumer data and opportunities for platform companies to leverage that data, privacy and data governance policies become important quality attributes.[42]

2. Platforms and Market Power

"Within the traditional analysis of firm market power, evidence of high market power is, at times, conflated with the abuse of market power and measured through price increases in excess of marginal cost for consumers."[43] I discuss market power and abuse of market power separately because firms can have strong market power and not abuse it.[44]

While the drivers of market power are similar for traditional firms and platforms, Professor Catherine Tucker argues against the sheer amount of data as being dispositive of market dominance and instead examines the impact of data on three sources of market power.[45] Network effects, switching costs, and status as an "essential facility" are all sources of market power for traditional firms and platforms that, importantly, may or may not have a direct relationship to the amount of data a company holds. In other words, a company with a large amount of data could still have low market dominance; data alone is not enough to show market dominance.

For platforms, switching costs — or the cost for an economic actor on the exchange to switch to an alternative market to complete a transaction — is an important measurement of market power.[46] Switching costs include search costs, learning costs, and uncertainty costs, among

42. *See* Erika M. Douglas, *Monopolization Remedies and Data Privacy*, 24 VA. J.L. & TECH. 1, 25–30 (2020) (articulating a broader approach to consumer welfare including data privacy as a quality consumers may care about, along with other quality factors, in assessing consumer welfare); *see also* Pasquale, *supra* note 22, at 1010; Kira et al., *supra* note 1, at 1342.

43. Martin et al., *supra* note 34, at 18 (emphasis omitted); *see also* Marshall Steinbaum, *Establishing Market and Monopoly Power in Tech Platform Antitrust Cases*, 67 ANTITRUST BULL. 130, 132–35 (2022).

44. *See* Daniel A. Crane, *Market Power Without Market Definition*, 90 NOTRE DAME L. REV. 31, 36–37 (2014) (arguing to identify the presence of market power as distinct from the abuse of that power). *But see* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 745 (2017) (identifying the weakness of completely disentangling the measurement of market power from the abuse of market power: firms and platforms with greater market power may make it difficult to measure abuse).

45. Tucker, *supra* note 36, at 683 ("This paper discusses from an economics perspective whether the notion of a 'Data-opoly' makes sense, using in-depth analysis of whether large swathes of digital data are related to the typical sources of market power.").

46. See Daniel A. Crane, *Market Power Without Market Definition*, 90 NOTRE DAME L. REV. 31 (2014) (making a strong case that greater emphasis should be placed on switching costs for platforms as compared to focusing on higher barriers to entry traditional firms).

others.[47] Under this theory, platform market power can be measured, in part, by how difficult or costly it would be for actors on the exchange to transact in an alternative market.[48] For the NYSE, how easily can consumers buy securities without that particular exchange; for Lyft or Uber, how easily can consumers reach their destination without suing a particular ride platform? Importantly, a platform's market power is measured from the perspective of the economic actor on the exchange and can include the supplier or the consumer on the exchange.[49]

3. Platforms and Abuse of Market Dominance

Platforms differ from traditional firms (i.e., firms that manufacture and sell their products and services directly to consumers) in that a platform's service is the creation of a market in which other economic actors transact. Because platforms create markets for economic actors, a platform is unique in its dual purpose as both a firm and a creator of a market.[50] This dual purpose also provides opportunities for the two purposes to conflict, where a platform governance policy could benefit the platform as a firm but harm the platform as an exchange.[51]

In fact, platforms with market dominance have long been known to enact policies to advantage the firm and more powerful economic actors on the exchange in a way that is beneficial to the platform owner but detrimental to those with less economic power on the exchange.[52] In other words, platforms with strong market power will have an incentive to enact policies that benefit the firm (i.e., the platform owner) but harm the actors on their exchange,[53] particularly actors with less power,

47. Shin-Ru Cheng, *Market Power and Switching Costs: An Empirical Study of Online Networking Market*, 90 U. CIN. L. REV. 122, 127–28 (2021) (describing how switching costs include "compatibility costs, uncertainty costs, and learning costs").

48. *See* Martin et al., *supra* note 34, at 17 ("For example, the market power of a ride-share platform in regards to riders would be partially explained by market share, but also by how difficult would it be for riders to find alternative transportation — e.g., a taxi or public transportation. The market power of Google in online advertising would be partially explained by how difficult it would be for a company to place online ads without using Google's Ad Exchange.").

49. *Id.* at 19 ("[M]aking the platform attractive for one party (e.g., consumers) can increase the platform's market power in regards to the counterparty (e.g., supplier). Amazon provides an excellent example of a platform that is attractive to consumers and even lowers prices for consumers but is able to have a very strong market position for suppliers. Steinbaum uses ride-share platforms as another example.") (internal citations omitted).

50. *See* Panos Constantinides, Ola Henfridsson & Geoffrey G. Parker, *Platforms and Infrastructures in the Digital Age*, 29 INFO. SYS. RSCH. 381, 381, 384 (2018); *cf.* J. Harold Mulherin, Jeffrey M. Netter & James A. Overdahl, *Prices Are Property: The Organization of Financial Exchanges from a Transaction Cost Perspective*, 34 J.L. & ECON. 591, 593 (1991) (arguing same for financial exchanges).

51. Martin et al., *supra* note 34, at 2–3.

52. *See* Craig Pirrong, *A Theory of Financial Exchange Organization*, 43 J.L. & ECON. 437, 438 (2000).

53. *See* Joost Rietveld, Joe N. Ploog & David B. Nieborg, *Coevolution of Platform Dominance and Governance Strategies: Effects on Complementor Performance Outcomes*, 6

when the interests of the platform owner diverge from the interests of the exchange.

Platforms abuse their market power through the control of their platform governance decisions rather than through consumer pricing.[54] Through this control — the governance decisions of the exchange — platforms can exert their market power, act in ways that undermine exchange actors, and benefit only themselves.[55] Specifically, "when governance policies to control platform exchange *increase* transaction costs rather than decrease transaction costs of the exchange actors, the platform is undermining the efficiency of the exchange."[56] According to Martin et al., opportunistic governance policies that benefit the firm owning the platform but increase the transaction costs of the exchange would be corrected in the market if the platform were in a competitive market.[57] Platforms create value and differentiation based on the exchange governance policies, but they can also use policies as a mechanism to abuse market power.

Importantly, for digital platforms, privacy and data governance practices have become an attractive lever for opportunistic tactics where platforms with greater market dominance enact policies to benefit themselves as a firm, rather than enact polices to benefit the efficiency of the exchange or platform.

4. Examples of Platforms and Abuse of Market Dominance.

Sabre is the classic example of a platform abusing their market power through the governance policies of the platform. Owned in 1976

ACAD. MGMT. DISCOVERIES 488, 490 (2020) (arguing that power is enacted through a change in governance "as a platform becomes increasingly dominant").

54. *See* Crane, *supra* note 44, at 57–58 (explaining that while abuse of market dominance is regularly measured by the Lerner index and the excess of price over marginal cost, the market power of a platform cannot be adequately measured by consumer pricing); ROBERT H. LANDE, MARKET POWER WITHOUT A LARGE MARKET SHARE: THE ROLE OF IMPERFECT INFORMATION AND OTHER "CONSUMER PROTECTION" MARKET FAILURES 6–7, https://www.justice.gov/sites/default/files/atr/legacy/2007/03/27/222102.pdf [https://perma.cc/3SWA-FJKZ]; Steinbaum, *supra* note 43, at 136.

55. Khan, *supra* note 44, at 746 n.189 (2002) (quoting MILTON FRIEDMAN, CAPITALISM AND FREEDOM 119–20 (2002)) ("'Monopoly exists when a specific individual or enterprise has sufficient control over a particular product or service to determine significantly the terms on which other individuals shall have access to it.' The Chicago School accepts this definition with regard to price and output, but ignores other metrics of control.").

56. Martin et al., *supra* note 34, at 19. This approach is consistent with Professors Khan and Pozen's argument that firms exercise power through price-based levers as well as metrics of control. *See* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 517–18 (2019); Lina M. Khan, *Sources of Tech Platform Power*, 2 GEO. L. TECH. REV. 325, 327 (2018).

57. Martin et al., *supra* note 34, at 21 ("While most firms would presumably act in ways that improve the transaction costs for the exchange actors — thereby increasing the popularity and volume of transactions of the exchange — platforms have been known to implement policies that *worsen* the transaction costs of the exchange actors and decrease the efficiency of the exchange.").

by American Airlines, Sabre held a monopoly position for travel agents to search for and make airline reservations for customers.[58] Sabre was sued for anticompetitive behavior because the platform prioritized American Airlines flights in flight searches.[59] This policy benefited American Airlines but decreased the quality of the match on the exchange and increased transaction search costs for users.[60]

In a similar move, Amazon was accused of prioritizing its private label items in users' search results, thereby increasing the search costs for consumers and decreasing the quality of the match.[61] Amazon supposedly prioritized the sale of its own products and benefited the firm while harming the efficiency of the platforms and its users.

Ticketmaster came under similar scrutiny when the platform failed to adequately enable Taylor Swift fans to search for and purchase tickets for her 2023 concert. While the price of the tickets sold on the platform never changed, many verified fans were unable to purchase tickets on the primary exchange. Instead, scalpers were able to purchase tickets and sell them in a secondary exchange, offered by Ticketmaster, where the prices were higher and the processing fees were larger for Ticketmaster.[62] The governance policies of the primary exchange for Taylor Swift tickets not only increased the search costs for legitimate fans buying tickets to attend the concert, but also facilitated scalpers buying more tickets and contributing to the secondary resale market, which was much more profitable for the firm (Ticketmaster).

B. In Sum

Platforms offer an exchange between other economic actors and differ from traditional firms in two important ways: (1) platforms differentiate through governance policies rather than price, and (2) platforms abuse market power through these same governance policies. Platforms can exert their market power, or act in ways that undermine

---

58. *Id.*

59. *Id.*

60. *Id.* at 34; *see also* Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*, 14 ACM TRANSACTIONS INFO. SYS. 330, 331 (1996).

61. Aditya Kalra & Steve Stecklow, *Amazon Copied Products and Rigged Search Results to Promote Its Own Brands, Documents Show*, REUTERS (Oct. 11, 2023, 11:00 AM), https://www.reuters.com/investigates/special-report/amazon-india-rigging [https://perma.cc/TLU6-QMQL].

62. Ben Sisario & Madison Malone Kircher, *Ticketmaster Cancels Sale of Taylor Swift Tickets After Snags*, N.Y. TIMES (Nov. 17, 2022), https://www.nytimes.com/2022/11/17/arts/music/taylor-swift-tickets-ticketmaster.html [https://perma.cc/9WN5-2Q9E]. Ticketmaster charges a fee for the seller for resale as well as a processing fee for those buying resale tickets (as much as 23%). Resale tickets therefore went for a higher than face value price and Ticketmaster received a higher percentage of that higher resale price. Meghan Bragg, *Fact Check: What Do Ticketmaster Service Fees Cover?*, WCNC CHARLOTTE (Feb. 16, 2023, 11:55 AM), https://www.wcnc.com/article/news/verify/ticketmaster-service-fees-charlotte-nc/275-b9234b03-a523-4d4c-932e-712649751a4c [https://perma.cc/Z7KL-TQB2].

exchange actors and benefit only themselves, through the control of their governance policies of the exchange. For digital platforms that collect a significant amount of consumer data, platforms can abuse market dominance through their privacy and data governance policies in particular.

III. PRIVACY AND DATA GOVERNANCE

Digital platforms collect and create a lot of data about users.[63] They use that data to not only facilitate transactions but also to later monetize through advertising, marketing, political campaigns, and online manipulation.[64] Scholars and advocates have steadfastly made the case that people on platforms care about privacy and data governance.[65] On platforms, the governance of data flows involves more than whether an individual can adequately consent to sharing data. Professor Salomé Viljoen correctly argues that data governance should focus on the flow of data to include how the data is used to draw inferences, to exert power and control, and to reinforce population-based relations.[66] Similarly, Professor Rory Van Loo argues users have interests in what a firm does with their data even if the firm has collected the data and never shares that data with third parties.[67] Users have privacy preferences about what and how data is collected, shared, and used.[68]

However, attempts to theorize about privacy and platforms within antitrust can fall victim not only to mistakes about platforms but also to simplistic and convenient views of privacy, such as privacy as

---

63. Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 131 (2015) ("The data collected by electronic platforms can take several forms, including 'volunteered data' shared intentionally by consumers, 'observed data' obtained by recording consumer actions online, and 'inferred data' derived from analyzing volunteered and observed data.").

64. Viljoen, *supra* note 3, at 589 ("Advertising techniques developed to predict or to influence behavior are increasingly gaining purchase in other industries. The same capabilities that help digital companies know (or claim to know) what attributes make someone likely to buy an advertised product, or that are leveraged to increase a desired behavior, can be used for other tasks. For instance, these techniques may be used to identify potential voters likely to engage on an issue or with a candidate, to identify what activities are associated with risky or risk-averse financial or health behavior, or to predict how much different people are willing to pay for the same product. Overall, the digital economy powered by these behavioral techniques represents roughly $2.1 trillion, making it the fourth-largest industry in the United States.").

65. *See supra* notes 4–10 and accompanying text.

66. *See* Viljoen, *supra* note 3, at 603, 607–08.

67. Van Loo, *supra* note 23, at 4–5 (describing how these interests include whether the data is used, for example, to manipulate, discriminate, or exploit users or others).

68. While both Professors Van Loo and Viljoen refer to such concerns as data management and data governance rather than privacy, for context-dependent definitions of privacy, such as privacy as contextual integrity, whether privacy has been preserved or violated depends on whether a flow of information conforms with privacy norms of a given context. *See also infra* Section IV.A.4.

concealment or privacy as protection from intrusion. These definitions of privacy may prove convenient in justifying corporate behavior but have led us astray in a quest to understand privacy and platform governance.

A. Convenient Privacy Shortcuts

1. Shortcut #1: Privacy as Concealment

Privacy as concealment defines information or people as "private" when concealed and not private when a person or information is seen or shared.[69] Importantly, disclosed information, since not private, has no rules, norms, or expectations as to how that data will be stored, used, or shared according to this definition.[70]

Defining privacy as concealment renders privacy inefficient to a functioning market since (in principle) relevant, concealed information could be helpful to improve transactions.[71] Economists can then (mistakenly) argue that privacy is harmful to efficiency because respecting privacy stops information flows.[72] As Professor Erika M. Douglas notes, this definition leads economists to see privacy as all about information asymmetries and assume that respecting privacy leads to a decline in efficiency and consumer welfare.[73] Privacy, simply defined, is anti-innovation, anti-functionality, and generally a bad idea. Professor Ryan Calo notes that "[e]conomists in general, [and] law and economics scholars in particular, tend to be heavily skeptical about privacy for its tendency to deny market participants information."[74] When privacy is defined as concealment, privacy loses in any economic fight.[75]

---

69. Thomas Nagel, *Concealment and Exposure*, 27 PHIL. & PUB. AFFS. 3, 22 (1998) ("[P]rivacy should impose a regime of public restraint and private protection . . . ."); Posner, *supra* note 16, at 405 ("[Privacy] is used to mean the concealment of information; indeed, this is its most common meaning today.").

70. Martin, *supra* note 7, at 496 ("In disclosing information, or even merely being in public or being online, consumers are seen from a legal perspective as relinquishing privacy. Firms are then permitted — even expected — to gather, aggregate, sell, and use the information to create value for themselves.").

71. *See* George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 625, 633 (1980).

72. Traditionally, concealment is considered inefficient: "[I]t reduces the amount of information in the market, and hence the efficiency with which the market — whether the market for labor, or spouses, or friends — allocates resources." Posner, *supra* note 16, at 406; *see also* Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249, 251 (2013) ("The roots of economic research on privacy (which can be found in seminal writings of scholars such as Richard Posner and George Stigler) focus on privacy as the concealment of (mainly negative) personal information.").

73. Douglas, *supra* note 16, at 447.

74. Ryan Calo, *Privacy Law's Indeterminacy*, 20 THEORETICAL INQUIRIES L. 33, 49 (2019).

75. Martin, *supra* note 7, at 495.

For platforms, defining privacy as concealment leads to a number of unfortunate implications. For example, since disclosed data has no privacy expectations or preferences, privacy as concealment leads to incorrect arguments that firms that own a platform are free to use that data in any way they choose.[76] Privacy as concealment leads to minimal guidance in how data can be shared or used post-disclosure.[77] In addition, if collecting any data means "giving up" privacy, then the amount of data collected by a firm is an important indicator of its respect for privacy. And taking into consideration privacy as an indicator of platform market power can mistakenly focus on the amount of data a platform collects as indicative of abuse of market power, since collecting data is defined as violating privacy by this definition.[78] Taken to its logical conclusion, since consumers are mistakenly framed as having no privacy interests in the data about them that is disclosed, collected, or inferred, a firm's ability to monetize that data (and the digital advertising industry in general) are elevated as the primary interests to consider with data governance.[79]

For example, in *hiQ Labs v. LinkedIn*,[80] the United States Court of Appeals for the Ninth Circuit did not believe LinkedIn's claims that their users had a privacy interest in the data that was shared and collected while on the platform.[81] LinkedIn's platform aims to connect professionals,[82] and LinkedIn's platform collects user data in order to facilitate those connections. hiQ Labs' business included scraping LinkedIn and identifying LinkedIn users whose activities suggested they were looking for employment.[83] hiQ could then sell that knowledge to the users' employers.[84] The mistaken conception of privacy as concealment, where privacy interests end once data is collected, leads not only to claims that platforms are not obligated to respect

76. Ohlhausen et al., *supra* note 63, at 132. ("Given the intrinsic value of this data, digital platforms can monetize it in several ways, including by using it internally to improve services or by selling it directly to advertisers or data brokers for repackaging.").

77. Martin, *supra* note 7, at 493.

78. For an example of such a definition, see Viktoria H.S.E. Robertson, *Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data*, 57 COMMON MKT. L. REV. 161, 171–72 (2020).

79. Douglas, *supra* note 20, at 660 n.50 ("Privacy regulation may reduce the collection and use [of] such data, which would reduce competition based on ad-targeting specificity.") (citing Catherine Tucker, *Online Advertising and Antitrust: Network Effects, Switching Costs, and Data as an Essential Facility*, CPI ANTITRUST CHRON., Apr. 2019, at 6).

80. 31 F.4th 1180 (9th Cir. 2022).

81. *Id.* at 1190; *see* Douglas, *supra* note 20, at 663 (noting that "the courts were skeptical of LinkedIn's claim of user privacy protection, finding little concrete evidence of the privacy harm LinkedIn claimed would occur to users from hiQ's continued access to their profile information").

82. *About LinkedIn*, LINKEDIN, https://about.linkedin.com [https://perma.cc/BZ92-PVBP] (noting that LinkedIn's mission is to "connect the world's professionals to make them more productive and successful").

83. *hiQ*, 31 F.4th at 1187.

84. *Id.*

privacy interests of their users after collecting their data, but also to arguments that other businesses (such as hiQ) have a "right" to this "public" information. Privacy as concealment provides the false basis to argue that hiQ should be allowed access to LinkedIn users' posts in order to develop their own business, since users (supposedly) have no interest in that data. However, even the originators of privacy as concealment did not envision the ability to collect, store, and transmit data to anyone the subject did not trust.[85]

In order to explain why individuals interact with firms, disclose data, and "give up" their privacy, privacy is said to be "traded" in exchange for a service. For platforms, this trade narrative resonates since some platforms are free to use for consumers; therefore privacy, by this incorrect definition, is the cost for being on a platform.[86] As Professor John M. Newman notes, the fact that many digital products are offered for free represents a clear, "obvious" benefit to consumers for scholars.[87] Further, since users are mistakenly argued as having no privacy interests in their data collected by platforms, firms are then expected to exploit user data.[88]

Gregory Day and Abbey Stemler summarize this narrative:

> Platform-based companies ("platforms") have mastered a business model whereby they offer users "free" and low-priced services in exchange for their personal information. With this data, platforms can design products, target advertising, and sell user

85. Martin, *supra* note 7, at 497 (arguing that scholars originally assumed firms would never gather more information than needed due to prohibitive costs to store and use information and that this cost would dissuade firms from idly surveilling people).

86. Michal S. Gal & Daniel L. Rubinfeld, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement*, 80 ANTITRUST L.J. 521, 522 (2016). ("The phenomenon of free goods is consistent with and perhaps even stimulated by the low weight given by many consumers to privacy and to the use of their revealed preferences by sellers.").

87. Newman, *supra* note 38, at 1544 ("Digital-product suppliers can use such data to feed the growing demand for targeted advertisements. This harvesting and reselling of data (the argument runs) 'results in obvious consumer benefit.'"); *see also* John M. Newman, *Antitrust in Zero-Price Markets: Foundations*, 164 U. PA. L. REV. 149, 152 (2015) (exploring the costs of free services and questioning the benefits by "correcting the rhetoric . . . by demonstrating that 'free' products are not free"). However, recent work has shown that the benefits of targeted advertising are not so "obvious": targeted ads based on behavioral data has been shown to include higher-priced products from lower-quality vendors than nonpersonalized or nontargeted alternatives. Eduardo Abraham Schnadower Mustri, Idris Adjerid & Alessandro Acquisti, Behavioral Advertising and Consumer Welfare: An Empirical Investigation 4 (Fed. Trade Comm'n PrivacyCon 2022, Working Paper, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4398428 [https://perma.cc/5PSK-Q42F].

88. Kira et al., *supra* note 1, at 1338–39 ("Crucially, the existence of zero-price platform-based ecosystems such as Facebook and Google is made possible by the means to monetize data. While the term 'free' describes the absence of a monetary price charged to the final consumer, the data harvested by the platform can represent nonmonetary costs charged to users in exchange for the free services and products (e.g. social networking or email) . . . .").

> information to third parties. The problem is that platforms can inflict greater costs on users and markets in the form of lost privacy than the efficiencies generated from their low prices.[89]

In sum, by defining privacy as concealment to assume that users have no privacy interests in collected data, scholars miss a mechanism that digital platforms have to abuse market power: enacting opportunistic privacy and data governance policies that violate user privacy but benefit platform owners. Privacy as concealment assumes, contrary to privacy research, that users have no privacy interest in disclosed data and therefore platforms cannot "harm" users through the storage, use, or sharing of their data. This shortcut definition of privacy does not reflect consumer preferences or expectations but does incorporate platform and firm interests in exploiting data.

2. Shortcut #2: Privacy as Protection from Intrusion

The second privacy shortcut is to frame privacy as preventing intrusion.[90] Privacy as protection from intrusion posits platforms as protectors of privacy if and only if third parties are precluded from having access to user data. Privacy is then used as justification for excluding possible complementary firms on an exchange.[91] Importantly, by this definition, platforms (or firms generally) cannot violate privacy if they store, use, or monetize user data themselves.

Van Loo provides Facebook as a case study of a platform that restricts access to user data by third parties such as LinkedIn, Pinterest, and MessageMe under the guise of protecting privacy.[92] These third parties provided competing complementary apps for Facebook and did not necessarily violate user privacy by virtue of being third parties with access to user data.[93] Sharing data with third parties may be a privacy violation if the actor does not help facilitate transactions on the exchange and is considered outside the context of the exchange. However, being a third party does not, by itself, constitute a privacy violation without knowing the context and purpose of the data sharing.

For example, Professor Van Loo's correct criticism of Amazon's approach to Sonos, a third-party manufacturer of speakers, exemplifies

---

89. Day et al., *supra* note 11, at 61.

90. Van Loo, *supra* note 23, at 4 ("Early conceptions of information privacy emphasized an anti-intrusion impulse as reflecting a desire 'to be let alone' by not being watched or having some information kept secret.").

91. Douglas, *supra* note 20, at 662 (using the example of hiQ to explain how "[d]ominant firms are invoking data privacy as a pro-competitive business justification for alleged exclusionary conduct").

92. Van Loo, *supra* note 23, at 22–24.

93. *Cf.* NISSENBAUM, *supra* note 26, at 156.

abusing privacy defined as unwanted intrusion.[94] Sonos "requested anonymized error rate data for when consumers used the company's speakers with Amazon's digital voice assistant, Alexa. Sonos wanted that data to improve the quality of its speakers' responses to voice commands."[95] Amazon refused, citing privacy concerns for users since Sonos was a third party.[96] However, users would have benefited from Sonos having access to the anonymized error rate data to improve their service — which consumers generally perceive to be trustworthy behavior for firms.[97] More likely, as noted by Professor Van Loo, Amazon withheld the data to give Amazon's own smart speaker devices a competitive advantage.[98]

Similarly, Apple implemented a policy in their app store to not allow third parties to track users across apps and contexts without explicit consent. However, Apple appeared to have exempted their own apps, such as the Find My app, which helps users locate their Apple devices.[99]

Framing privacy as protection from intrusion by third parties is particularly dangerous for platforms. When scholars conflate the firm with the platform, the interests of the platform are assumed to be congruent with the interests of the firm; information shared with a platform is assumed to be accessible to the firm as well.[100] However, platform owners often operate in many different markets, and firms own more than one platform.[101] Amazon runs a marketplace but also manufactures products; Meta runs multiple social networks as well as an ad

94. *See* Van Loo, *supra* note 23, at 24.

95. *Id.*

96. *Id.* at 24–25.

97. *See* Kirsten Martin, *Privacy Governance for Institutional Trust (or Are Privacy Violations Akin to Insider Trading?)*, 96 WASH. U. L. REV., 1367, 1387, 1403–04 (2019).

98. Van Loo, *supra* note 23, at 25 ("After all, Amazon itself recorded people's conversations in their homes without users' permission or even awareness. Moreover, Amazon shared actual recordings of consumers' in-home conversations with independent consultants it had hired — thereby handing over much more sensitive data to third parties than what Sonos requested. Amazon's broader behavior with respect to data thus suggests Amazon may have been using privacy as a pretext to keep anonymized voice data from Sonos.").

99. *Id.* at 23–24 ("Apple created access barriers to all third-party apps. It cited customers' privacy interests in not having third-party apps track them and collect excess data . . . . Apple's motives become murkier, however, when considering that Apple did not provide similar tracking and data collection protections with respect to its own apps. For instance, Apple's app Find My, like Tile, helps people to locate items. Yet Find My, unlike Tile, defaulted to location tracking 'on' even after Apple announced its universal new 'protections' against tracking.").

100. Kira et al., *supra* note 1, at 1338, 1340 (arguing that all platforms in a firm (e.g., social networks and ads) must be considered as necessarily intertwined).

101. Khan, *supra* note 44, at 713 ("In addition to being a retailer, it is a marketing platform, a delivery and logistics network, a payment service, a credit lender, an auction house, a major book publisher, a producer of television and films, a fashion designer, a hardware manufacturer, and a leading provider of cloud server space and computing power.").

platform.[102] In other words, by positioning privacy as protection from intrusion, platforms claim to be able to collect and use consumer data with impunity so long as third parties are kept at bay.[103]

Platforms use the fixation on third parties as "intruders" to excuse why they exclude third parties from a platform only to themselves exploit consumer data in ways that violate privacy norms. For example, Google's proposed "Privacy Sandbox" is offered as a privacy-preserving solution that prevents third party ad trackers from collecting users online browsing information and sharing that data for the purpose of hyper targeted advertising for users of Chrome.[104] However, Google would then be able to perform the same activities — including collecting users' online browsing activities to then place hyper-targeted ads — that are known to violate users' privacy.[105]

B. Privacy Shortcuts and The Honeypot Problem

These privacy shortcuts not only obscure privacy violations and anticompetitive behavior by claiming that users do not have a privacy interest in how collected data is used or shared, but also provide justification for the creation of platforms as a honeypot. A honeypot platform is a profit-sacrificing platform that is intended to lure users, like a decoy. The honeypot platform mimics a legitimate business with concerns about consumers but uses the user's interactions to gain information that can then be exploited in another business line or secondary platform.[106] While privacy shortcuts have been identified as offering a

---

102. Katie Tarasov, *How Amazon's Big Private-Label Business Is Growing and Leaving Small Brands to Protect Against Knockoffs*, CNBC (Oct. 12, 2022, 9:00 AM), https://www.cnbc.com/2022/10/12/amazons-growing-private-label-business-is-challenge-for-small-brands.html [https://perma.cc/JQC6-ETBL]; *Your Customers Are Here. Find Them with Meta Ads.*, META, https://www.facebook.com/business/ads [https://perma.cc/6M7H-G6J3].

103. Van Loo, *supra* note 23, at 23 ("Despite Facebook's external privacy justifications, the emails show that the company was selectively targeting access restrictions at the fastest-growing rival apps it viewed as posing a 'competitive threat.' Moreover, around the time that Facebook restricted data access to competitors, it expanded data access to heavy advertisers that were not competitors, like Amazon and Netflix.").

104. *See* Kirsten Martin, Helen Nissenbaum & Vitaly Shmatikov, No Cookies for You!: Evaluating the Promises of Big Tech's 'Privacy Enhancing' Techniques 25 (Dec. 9, 2023) (unpublished manuscript), https://kirstenmartin.net/wp-content/uploads/2023/12/Main-Article-FTC-No-Cookies-For-You-12-09-2023.pdf [https://perma.cc/F3PH-ZZTU].

105. *See* Martin et al., *supra* note 4, at 208–10; Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation Into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online*, 24 J. PUB. POL'Y & MKTG. 210, 210 (2015); *see also* Martin et al., *supra* note 104, at 53.

106. This is based on the common use of "honeypot" as a lure in espionage or in security. *See, e.g.*, *What is a honeypot?*, KASPERSKY, https://usa.kaspersky.com/resource-center/threats/what-is-a-honeypot [https://perma.cc/5E4U-37GQ] ("It's a sacrificial computer system that's intended to attract cyberattacks, like a decoy. It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals and the way they are operating or to distract them from other targets.").

pretext to block access by third parties for anticompetitive reasons,[107] this Essay argues that these two shortcuts go further to justify the creation and growth of platforms as honeypots and hide the abuse of market power by platforms.

First, privacy as concealment provides platforms with an incentive to produce a lure for consumers in order to collect information for use in a different context, in a different business, or on a different platform. For privacy as concealment, people trade away their privacy interests when engaging with online platforms. Platforms seen as free only reinforce that false narrative. The more attractive (i.e., low-cost or free) the platform is for consumers, the more scholars and firms can mistakenly argue that users have traded away their privacy interests by engaging with that platform.[108]

Second, privacy as protection from intrusion provides the justification for platform owners to then exploit user data themselves. Since the obligation of platforms is to keep third parties from gaining access to user data, platforms and platform owners are then justified in exploiting consumer data so long as third parties are not given access. Importantly, scholars then frame information collected on the platform as being shared with the firm in general.[109] However, a platform's goals, purposes, and context often diverge from those of the larger firm — which may own different businesses and platforms.[110] In fact, the longstanding issue with platforms is the implementation of governance policies on the platform that benefit the firm but harm actors on the exchange.[111]

And these problems interact: Professors Michal Gal and Daniel Rubinfeld argue that to understand the market for a low-price or free platform, one must bundle that platform with another exchange.[112] For example, social networks or search can only be understood as bundled with a company's ad network. This Essay disagrees. Their argument would be similar to a car dealer providing free or low-cost cars, but who is also in the more lucrative car repair business. Slowly, as the manufacturer gains market power, the cars are of lower quality with the requirement that most if not all the cars must be repaired through the sister repair business owned by the same company. According to Gal

---

107. Van Loo, *supra* note 23, at 24.

108. *See* Gal et al., *supra* note 86, at 522, 527; Day et al., *supra* note 11, at 63.

109. *See, e.g.*, Ohlhausen et al., *supra* note 63, at 121.

110. *Supra* Section II.A.3.

111. *See supra* Section III.A. Convenient Privacy Shortcuts

112. Gal et al., *supra* note 86, at 543 ("Internet search in isolation — i.e., as distinct from and not intertwined with the sale of search advertising — is not a relevant market for welfare analysis. Such a narrow focus . . . ignores the two-sided nature of the search-advertising platform and the feedback effects that link the provision of organic-search results to consumers with the sale to businesses of advertising accompanying those search results.").

and Rubinfeld's argument,[113] which is not unique,[114] the automobile company is really just a repair business since that is where all the profits are made. To make it similar to the situation online, the fact that the automobile company owns the repair shops would have to be hidden from the consumers.

Ironically, or strategically, the very policies that may be evidence of abuse of market power — opportunistic privacy and data governance polices — are explained away by impoverished, mistaken definitions of privacy in antitrust platform scholarship.

The logical conclusion of justifying the honeypot problem is to completely discount the front-end lure (e.g., email, search, social networking) as well as users' privacy interests in engaging with the platform-as-lure only to prioritize where the firm is able to exploit and monetize that data. Consider Professor Douglas's analysis of a hypothetical Gmail case where the government could force Google to grant third-party access to user email content.[115] Professor Douglas argues that considering privacy as an important attribute of the user's Gmail experience is not appropriate in such a remedy since Google does not compete on privacy in their lucrative advertising business.[116] Douglas notes that even the most charitable approach to privacy and antitrust scholarship calls for antitrust law to account for data privacy only where privacy is an attribute important to competition.[117] For Douglas, the important market to consider for email privacy is actually Google's ad exchange due to how profitable the ad platform is for Google rather than email, where the user engages and shares their data.[118] And Google's ad exchange is in a market that does not compete on privacy.[119] In fact, in the market for ad exchanges, platforms compete for users to give up their privacy preferences for the purposes of ad targeting.[120] In this framing, the market deemed relevant, and used to determine if privacy is important to consumers, is the market for profitable ad exchange, not the market for consumer-facing mail exchange. This

113. *See id.* at 562.

114. *See, e.g.*, Harbour et al., *supra* note 39, at 773 ("Internet-based firms often derive great value from user data, far beyond the initial purposes for which the data initially might have been shared or collected, and this value often has important competitive consequences."); Ohlhausen et al., *supra* note 63, at 131; Day et al., *supra* note 11, at 64; Newman, *supra* note 38, at 1544–45.

115. Douglas, *supra* note 42, at 32.

116. *Id.* ("The integrationist view would look for privacy-related quality competition between Google and the rival applications, but would find none. Google and the apps were competing to sell online advertising, not competing to offer users improved email data privacy.").

117. *Id.* at 32–33.

118. *Id.*

119. *Id.*

120. *Id.*

framing takes the existence of honeypot platforms is taken as a given.This Essay disagrees.

In our current digital market, honeypot platforms designed as a lure to feed users into hyper-targeted advertising platforms are more problematic since the secondary platforms are *more* profitable for the firm[121] but violate users' privacy and lower consumer welfare by serving ads for more expensive products from lower quality vendors to consumers.[122]

The answer to the honeypot problem is that users share information within norms of privacy for the platform with whom they are a user: email, search, rideshare, Twitter, Instagram, Airbnb, eBay, etc. That platform respects privacy by gathering, storing, using, and sharing data within the context of its exchange. I explore this positive account in Part IV.

IV. UNDERSTANDING PRIVACY ON PLATFORMS

A. Contextual Privacy Approaches

Rather than privacy as concealment or as protection from intrusion, more context-dependent definitions of privacy posit that an individual who shares information does so within a community, relationship of trust, or within a particular context.[123] Specifically, people engage with an organization or person for a specific purpose and within a social context, and privacy is respected when the norms of appropriate flow for that context are respected.[124] That context then drives what information should be collected (information type), how that information should be collected (transmission principle), who can have access to that information (actor), and how that information should be used (purpose or goal).[125] Importantly, people have privacy interests in how data is used, stored, and shared on a platform and expect flows of information to be in furtherance of the platform's context.

---

121. *See* Howard Beales Supplementary Comments at 1, https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00117/544506-00117.pdf [https://perma.cc/Z8JR-4NHL].

122. Mustri et al., *supra* note 88, at 4.

123. *See* NISSENBAUM, *supra* note 26, at 129; WALDMAN, *supra* note 13, at 79; Kirsten Martin, *Understanding Privacy Online: Development of a Social Contract Approach to Privacy*, 137 J. BUS. ETHICS 551, 553 (2016); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 435 (2016); Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 659 (2011).

124. *See* NISSENBAUM, *supra* note 26, at 140–47.

125. Kirsten Martin & Helen Nissenbaum, *What Is It About Location?*, 35 BERKELEY TECH. L.J. 251, 275 (2020) ("Fully specifying a privacy norm requires specifying five key parameters: information type (about what), subject (about whom), sender (by whom), recipient (to whom), and transmission principle (flow under what conditions).").

Research supports these approaches showing that people have nuanced privacy interests in public information,[126] that how firms use data is relevant to whether the firm meets the privacy expectations of individuals,[127] and that individuals approve of their data being used to benefit themselves and others while disapproving of the use of the same data for manipulation or marketing.[128]

In this Essay, privacy — defined as the norms of appropriate data flow including what data is collected, how data is collected, how that data is later shared and used within a given context — is a quality of the platform that consumers take into consideration when choosing a platform. Privacy, in this way, is yet another governance policy that platforms offer to remain competitive in a competitive market and a possible mechanism to abuse market power in less competitive markets.[129]

For each facet of privacy as contextual integrity — context, information type, actor, transmission principle, use/practice — I explain each concept, how each is important for privacy and data governance on platforms, and how platforms could violate norms of appropriate flow or privacy norms in their business practices.

1. Context

For privacy as contextual integrity, context is a social domain or sphere, as theorized in social and political theory, with goals, purposes, people, norms, and values (e.g., healthcare, family, commerce, finance, politics, etc.).[130] For an organization collecting information, the context is declared by the organization in what service they offer (e.g., health care, education, retail). A platform's context is similarly defined by the exchange when the user shares their data on the exchange. For example, eHarmony is a "trusted data site for singles" and ZipRecruiter helps people find meaningful employment. The context (i.e., dating or finding employment) drives the goal, purpose, actors, values, and norms of the platform — including norms of appropriate flow of information.[131]

---

126. Martin et al., *supra* note 4, at 180–81.

127. Martin, *supra* note 97, at 1403.

128. Kirsten Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms*, 30 BUS. ETHICS Q. 65, 70 (2020).

129. *See supra* Part II.

130. Martin et al., *supra* note 125, at 126 ("Contexts in this sense are constituted by respective roles, activities, purposes, values, and norms. Among the norms, those governing information flows are associated with respective contexts in their characteristic ontologies, such as those defining contextual roles or capacities of actors (e.g., student, physician, senator, rabbi, etc.), and types or categories of information (e.g., diagnosis, blood type, vote, grades, marital status, criminal record, etc.).").

131. Helen Nissenbaum, *Respecting Context to Protect Privacy: Why Meaning Matters*, 24 SCI. & ENG'G. ETHICS 831, 838 (2018).

Importantly, context is not defined by where a company is most profitable. Users do not, under the theory of privacy as contextual integrity, share information with a social network, for example, in order for the platform owner to exploit that data in another more profitable business. Instead, users share data within a specific context defined by why they are engaging with the platform. This means that the norms of appropriate flow as to what information; the conditions under which information is collected; and how the data is stored, used, and shared are defined by the platform's exchange. For search, the context is matching the user to relevant content; for social networking, the context may be to "bring you closer to the people and things you love"[132] or "to share their experiences, connect with friends and family, and build communities."[133] Importantly, advertising is in a different context with different goals and purposes.[134] Platforms can exploit users by sharing or using data in a context different from the one in which the individuals shared the data.

2. Information Type

Appropriate information types are then defined by the context in which the data is collected or shared. Information appropriate for one context (e.g., insurance) could be inappropriate for a very different context (e.g., retail).[135] For a dating app, where the context is matching people to hang out, the appropriate information to gather would be to facilitate a match. Similarly, for LinkedIn, the context would be professional, with the goal to "connect the world's professionals to make them more productive and successful."[136] However, data collected outside the purpose and values of the platform (e.g., to be used for advertising or to sell to others for a non-contextual use) would be a privacy violation. Platforms can justify the collection of user data, even a lot of user data, so long as the type of information is appropriate for that context and is in furtherance of the goals of that platform's context.

---

132. *We Bring You Closer to the People and Things You Love*, INSTAGRAM, https://about.instagram.com/about-us [https://perma.cc/FZ6D-HQSK].

133. *Facebook Community Standards*, FACEBOOK, https://transparency.fb.com/policies/community-standards [https://perma.cc/7EL5-HWLV].

134. *See Ads Manager*, FACEBOOK, https://www.facebook.com/business/tools/ads-manager [https://perma.cc/5KM2-GK6B] ("It's an all-in-one tool for creating ads, managing when and where they'll run, and tracking how well your campaigns are performing towards your marketing goals.").

135. *See* Martin et al., *supra* note 4, at 210.

136. *About LinkedIn*, LINKEDIN, https://about.linkedin.com [https://perma.cc/BZ92-PVBP].

3. Actors

For privacy as contextual integrity, the actor is the subject, sender, and recipient for a given transmission of information. Further, recipients function within a particular contextual role, such as doctor, teacher, friend, since an actor can have more than one role in life.[137] As noted by Professor Helen Nissenbaum, actors can have more than one role, and one must always define the context in which the actor collected the data.[138] For a large company with many platforms and businesses (e.g., Meta, Google, Amazon, Apple), users share information with a specific platform and for a specific contextual purpose. For the email example from above, users share information to enable email rather than with the company generally, and sharing data with actors — even within the larger company — outside the context of email would be a privacy violation.

Understanding that people share information with recipients in contextual roles has practical implications for platforms. For example, consumers engage with a firm for email and share their data for email services. But prioritizing the ad network as the reason why consumers choose an email service only because that is where the firm has a larger profit margin misses the importance of asking "in what context?" when someone shares their data or engages with a firm. The context or social domain, in identifying the privacy norms for the theory of contextual integrity, is the primary context from the perspective of the subject sharing information (e.g., email) and not from the perspective of where the business would like to later exploit that same data (through advertising).

4. Transmission Principles

Transmission principles are the conditions or constraints under which the information is collected or transmitted. Notice and consent is one such transmission principle, as are the phrases "with third-party authorization" or "as required by law."[139] For platforms, mere notification is not sufficient to ensure the privacy interests of users are met. For privacy as contextual integrity, the appropriate information type, actors, and uses of data are defined by the context in which the user engages with the platform and not the statements made in the privacy notice.

The creation of new information about a data subject through the creation of inferences has been the target of recent analysis, particularly

137. Helen Nissenbaum, *Invited Talk: Contextual Integrity*, INT'L ASS'N CRYPTOLOGIC RSCH., at 19:54 (Oct. 4, 2019), https://iacr.org/cryptodb/data/paper.php?pubkey=29951 [https://perma.cc/U6UH-4DAK].

138. *Id.*

139. Nissenbaum, *supra* note 131, at 840.

in the use of these inferences to make decisions about the data subject without their knowledge.[140] For example, a hospital, in the medical context, drawing inferences about a patient's condition without asking them directly could be considered appropriate.[141] However, a university in the education context or an ad network in the marketing context drawing the same inference could be considered a privacy violation — either for using an inappropriate transmission principle (an expectation to ask the person directly rather than infer the knowledge based on collected data) or because of the information type is inappropriate for the context.

5. Purpose, Use, and Practice

The use or practice of the recipient is not one of the five attributes of privacy as contextual integrity but is considered to be defined by the context's goals and purposes.[142] Appropriate data uses and practices are those in furtherance of the goals and purposes of the context. Further, contextual uses are those that conform to the entrenched norms of the context and "reinforc[e] the purposes and goals of respective contexts."[143] Noncontextual uses are inappropriate because they promote the advantage of others without serving contextual ends and values.[144] For platforms, privacy as contextual integrity provides broad latitude for the contextual uses of consumer data that are aligned with legitimate contextual norms.[145] To respect privacy as contextual integrity, platforms are limited as to not only the types of data collected and stored, but also in terms of the recipients and usage of that data. For example, a dating platform that collects user data, in order to facilitate a match between the user and other exchange actors, would be considered to violate users' privacy if that same data was used for a purpose that was outside the context of matchmaking. For example, if that dating platform used the user data collected for matchmaking in order to offer mortgages or loans, the platform would be violating the norms of privacy by using the data in a different context.

---

140. Sandra Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioral Advertising*, 35 BERKELEY TECH. L.J. 367, 370–71 (2020); Wachter, *supra* note 6, at 149, 203–04; Solow-Niederman, *supra* note 6, at 360–63.

141. *See* Meredith Broussard, *An AI Told Me I Had Cancer*, WIRED (Mar. 15, 2023), https://www.wired.com/story/artificial-intelligence-cancer-detection [https://perma.cc/A9VN-2VC7].

142. *See* NISSENBAUM, *supra* note 26, at ch. 7.

143. Martin et al., *supra* note 4, at 200.

144. *See id.* at 190–91.

145. Ido Sivan-Sevilla, Helen Nissenbaum & Patrick Parham, *On Comments Submitted to the FTC on Commercial Surveillance and Lax Data Security Practices*, DLI @ CORNELL TECH (Dec. 9, 2022), https://www.dli.tech.cornell.edu/post/on-comments-submitted-to-the-ftc-anpr-on-commercial-surveillance-and-lax-data-security-practices [https://perma.cc/Q22W-VU8S].

B. Privacy as Contextual Integrity as Fixing Mistakes

Privacy as contextual integrity solves the problems created by the privacy shortcuts in Part III. First, and contrary to privacy as concealment, information that is revealed or collected has privacy norms that govern the collection, use, and sharing of that data. Privacy as contextual integrity diminishes the justification to create a lure for consumers to "give up" or "trade" away their privacy since users share data regularly but never give up their privacy. As summarized by me and Professor Nissenbaum:

> One immediate consequence of defining informational privacy as contextual integrity is the sharp difference it reveals between "giving up" privacy and giving up information. . . . Privacy is not lost, traded off, given away, or violated simply because control over information is ceded or because information is shared or disclosed — only if ceded or disclosed inappropriately. That people are willing, even eager to disclose, release, and share information is quite compatible with placing a high value on privacy so long as such flows are appropriate. Giving up information, however much, is not the same as giving up privacy if the flow is appropriate.[146]

In this way, users are not faced with a dilemma to have functionality or privacy; privacy as contextual integrity explains why users expect to share information and be provided with functionality, while having their privacy norms (i.e., norms of appropriate flow for privacy as contextual integrity) be respected. For the *hiQ* case, users have privacy preferences regarding data collected about them. In fact, platforms including LinkedIn compete for users based on those data governance policies. LinkedIn has a legitimate business reason to protect users through the data governance policies that govern their exchange.

Second, privacy as contextual integrity removes the justification for the exploitation of data created by privacy as protection from intrusion. Where this shortcut claimed that platforms and platform owners were able to use consumer data with no privacy implications, privacy as contextual integrity limits the use of collected data to use only in furtherance of the goals and purposes of the platform's context. For example, privacy as contextual integrity would not justify the use of consumer data collected for email, social networking, or education to be used for advertising, since the use would be in a different context and

146. Martin et al., *supra* note 4, at 190–91.

not in furtherance of the goals of the context in which the data was shared (whether done by third parties or by the platform owner).[147]

Privacy as contextual integrity should be attractive for practice because the theory has been used and validated in empirical work. Simplistic approaches to privacy do not hold up in empirical work, forcing scholars to declare that respondents and consumers are acting irrationally or in a paradoxical manner.[148] For privacy as contextual integrity, study after study show that respondents find the collection, storage, sharing, and use of information that is in furtherance of a particular context to be appropriate.[149] In fact, the theory justifies why sharing data with regulators or "digital helpers" may be completely appropriate if within the context of the platform.[150] Further, more information may be needed to innovate on the platform in order to improve the platform and its efficiency or functionality.

However, privacy as contextual integrity does not justify an argument that consumers give up or trade privacy when they engage with a platform. Nor does privacy as contextual integrity support the exploitation of data for the benefit of the firm outside the context in which it was shared — but neither do surveys of consumers. While privacy as contextual integrity provides a roadmap for practitioners for how to respect privacy and justifies the collection, sharing, and use of consumer data in furtherance of the platform's context, the theory does not justify creating a lure for consumers to share their data only to exploit that data in another context.

V. CONCLUSION

Digital platforms are increasingly important in how we live our lives. And for digital platforms with market dominance, privacy and data governance polices can serve as vehicles to abuse power, where the collection, storage, sharing, and use of data benefit the platform owner but harm market actors on the platform. However, privacy

147. *See* Martin et al., *supra* note 104, at 35.

148. Martin et al., *supra* note 4, at 179; Solove, *supra* note 17, at 3.

149. Martin et al., *supra* note 4, at 208; Martin, *supra* note 97, at 1393; Martin, *supra* note 128, at 79–80; Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J.L. & TECH. 111, 120–21 (2017).

150. Van Loo, *supra* note 23, at 8 ("Access by regulators and digital helpers is thus essential to data management. Yet privacy's dominant normative skepticism of third-party access helps set up businesses to use pretexts to reframe beneficial third-party access as an intrusion on the customer."). Van Loo correctly sees a need to harmonize "anti-intrusion" privacy concerns and "allied access," meaning allowing third parties access without saying there is a privacy violation. *See id.* Privacy as contextual integrity is a theory and definition that *allows* for the flow of data to be appropriate — even to third parties — as long as the flow is within the appropriate norms for the given context. In fact, Van Loo uses data management to mean "the diverse set of interests that people have in their data beyond intrusions" which is covered in privacy as contextual integrity. *Id.* at 12.

shortcuts have not only obscured the abuse of power through privacy and data governance policies but have provided the justification for the creation of honeypot platforms: platforms that serve as lures for users and allow the firm to later exploit user data in a secondary platform or business. Fortunately, existing privacy scholarship provides guidance for policy and practice to recognize the privacy preferences of consumers on digital platforms.