Harvard Journal of Law & Technology
Volume 38, Number 4 Spring 2025

THE CONTRACTUAL DEATH AND REBIRTH OF PRIVACY

By Robin Bradley Kar & Xiaowei Yu***

ABSTRACT

This Article proposes, for the first time, the application of "shared meaning analysis" — a method of contract interpretation grounded in traditional contract principles, as developed in *Pseudo-Contract and Shared Meaning Analysis*, 132 HARV. L. REV. 1135 (2019) ("*Pseudo-Contract*") — to online privacy policies. The method identifies when policy text adds enforceable terms to a contract, as opposed to mere unenforceable boilerplate, addressing an underappreciated paradigm slip in contract law that is enabling widespread digital surveillance. Consumers routinely click "I agree" to online privacy policies — which purport to permit cookies, other tracking devices (like pixels and SDKs), and AI-driven data analysis — without reading or comprehending their text, leading to massive transfers of personal information that erode privacy, facilitate consumer and political manipulation, and threaten freedom and democracy. Critiquing the binary debate over whether online privacy policies are contracts at all, this Article argues for a more nuanced reform: courts, operating within their common law authority, should revive privacy by focusing contract interpretation on the shared meanings of any contracts over privacy formed in digital contexts. Through examples involving policy scope, unilateral modifications, and conflicts between shared meaning and deceptive boilerplate, this Article demonstrates how contract interpretation — once returned to its rightful focus on shared meaning — can be used to counter modern surveillance harms without requiring new legislation, complementing other privacy frameworks and restoring the proper moral relationship between contract and privacy.

* Professor of Law & Philosophy, University of Illinois, Urbana-Champaign. BA, Harvard University, JD, Yale Law School, PhD (legal, moral, and political philosophy), University of Michigan.

** Legal Researcher, SJD, University of Illinois, Urbana-Champaign.

TABLE OF CONTENTS

I. INTRODUCTION

The right to privacy includes a right for people "to determine for themselves when, how, and to what extent information about them is communicated to others."[1] Freedom of contract includes the freedom to give something away as well as the freedom not to.[2] These facts

1. ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967). For related views, see, for example, Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 816 (1999) (arguing that privacy rights are about control over personal information); James Rachels, *Why Privacy is Important*, 4 PHIL. & PUB. AFFS. 323, 326 (1975) (construing privacy as a matter of control over information depending on nature of interpersonal relationships); Edward Shils, *Privacy: Its Constitution and Vicissitudes*, 31 LAW & CONTEMP. PROBS. 281, 283 (1966) (arguing that privacy is about "control over resources that belong to them").

2. For a classic discussion of the origins and development of this idea, see Roscoe Pound, *The Liberty of Contract*, 18 YALE L.J. 454, 454 (1909) ("The idea that unlimited freedom of making promises was a natural right came after enforcement of promises when made, had

explain why courts in the United States have taken the seemingly unremarkable step of treating online privacy policies *as contracts* so long as they have been "agreed to" via general principles of contract formation.[3]

Though this move may seem unproblematic in principle, it is deeply flawed in practice. The contract law that courts use to allow transfers of control over personal information in online contexts is no longer traditional contract law, which historically focused on exchanges that are actually agreed upon as parts of the common meaning of the parties.[4] Instead — as documented most clearly in *Pseudo-Contract and Shared Meaning Analysis* — recent changes in technology and online contracting practices have created a largely unconscious "paradigm slip" in contract law, which has distorted the meanings and functions of many of its core concepts, such as "contract," "agreement," "term," and "interpretation."[5]

A "paradigm slip" occurs when "each small step in application [of a standing set of cases and doctrines] aims to preserve the purposes, basic concepts, and coherence of a body of doctrine, but the overall result is a largely unintended and more fundamental change in the meanings of its core concepts."[6] As the result of a paradigm slip in

---

become a matter of course. It began as a doctrine of political economy, as a phase of Adam Smith's doctrine which we commonly call *laisser* [sic] *faire*. It was propounded as a utilitarian principle of politics and legislation by Mill. Spencer deduced it from his formula of justice. In this way it became a chief article in the creed of those who sought to minimize the functions of the state, that the most important of its functions, was to enforce by law the obligations created by contract."). *See also* Wendell H. Holmes, *The Freedom Not to Contract*, 60 TUL. L. REV. 751, 752 (1986) ("According to traditional contract theory, then, the freedom of contract carried with it a correlative freedom not to contract.").

3. *See* RESTATEMENT (FIRST) OF CONSUMER CONTS. § 1 cmt. b (AM. L. INST. 2024) [hereinafter "RESTATEMENT, CONSUMER CONTRACTS"] ("[T]he . . . approach, which held that privacy notices can create contractual obligations, is indeed the dominant jurisprudence in this area."); *see also, e.g.*, *In re* Am. Airlines, Inc., Priv. Litig., 370 F. Supp. 2d 552, 557 (N.D. Tex. 2005) (noting that "[American Airlines'] website sets out its privacy policy, which is part of the contract of carriage with passengers"); Silver v. Stripe Inc., No. 20-CV-08196, 2021 WL 3191752, at *4 (N.D. Cal. July 28, 2021) (finding that "sign-in wrap" format confirmed user acceptance of privacy policy terms).

4. *See generally* Robin Bradley Kar & Margaret Jane Radin, *Pseudo-Contract and Shared Meaning Analysis*, 132 HARV. L. REV. 1135 (2019) (discussing this historical shift); *see also* RESTATEMENT (SECOND) OF CONTS. § 201 cmt. c (AM. L. INST. 1981) [hereinafter "RESTATEMENT, CONTRACTS"] (stating that when interpreting contracts, "the primary search is for a common meaning of the parties").

5. Kar & Radin, *supra* note 4, at 1140 ("At the end of this process, 'contract' — which now allows businesses to create legal obligations unilaterally without obtaining any actual agreement over many boilerplate 'terms' — is no longer contract. 'Agreement' is no longer agreement. 'Consent' is no longer consent; 'assent' is no longer assent; and 'terms' — which now include enormous streams of boilerplate text that are delivered but never read by anyone — are no longer terms with shared meaning. Contract, which was for centuries a legal regime grounded in actual agreement with common understanding, has in many instances become pseudo-contract — a system of private obligations with expanding contents that are created unilaterally by one party.").

6. *Id.* at 1142.

contract law, legal terms like "contract," which once referred primarily to agreements with shared meaning, now refer also to copious text that is unilaterally imposed on consumers without ever having been cooperatively communicated to create any shared meaning — or to both traditional contract and what we call "pseudo-contract." To highlight this subtle yet profound shift in meanings, we sometimes use scare-quotes around modern, extended uses of legal terms like "agreement," "term," and "contract."

Because of the paradigm slip in contract law, courts now regularly treat as contract not only content that is cooperatively communicated when people "agree" to online offers, but also the copious boilerplate text found in hyperlinked "terms and conditions" and privacy policies — text that few, if any, users ever read or could read.[7] This text regularly purports to waive privacy rights, permitting widespread surveillance of online behavior and the sale of personal information to third parties.[8] Yet this text regularly fails to meet the minimal standards of cooperative communication required to produce an actual agreement with shared meaning under traditional principles of contract law.[9]

This legal regime of pseudo-contract has enabled the widespread collection and sale of vast databases of personal information that record many of our most intimate and mundane choices. Fueled by powerful artificial intelligence algorithms and machine learning, these databases are rapidly analyzed and often sold to the highest bidder.[10] Sometimes, these processes shape online experiences to align with user preferences,

---

7. *See id.*; Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 1 (2014) (finding that "only one or two of every 1,000 retail software shoppers access the license agreement and that most of those who do access it read no more than a small portion"); Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO. COMMC'N & SOC'Y 128, 140 (2020).

8. *See, e.g.*, *infra* Part IV. In addition, this text often contains unilateral modification clauses, which empowers companies to change their privacy policies at their will. To remain apprised of such "terms," users are obliged to constantly check the updated terms to keep track of their contractual relationship with different sites. *See* Joel R. Reidenberg, *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 J.L. & POL'Y 485, 494 (2015) ("Another criticism is that website privacy policies often give websites the right to change their policies and relationships with third parties at any time. Here, the implication is that users will be expected to constantly re-check a website's privacy policy (and the policies of affiliated third parties, too) to keep abreast of a site's current privacy practices.").

9. *See* Kar & Radin, *supra* note 4, at 1140.

10. John F. Wasik, *How to Fight Back if Your Personal Financial Information Is Being Sold By Data Brokers*, FORBES (Sept. 6, 2023, 2:33 PM), https://www.forbes.com/sites/johnwasik/2023/09/06/how-to-fight-back-if-your-personal-financial-information-is-being-sold-by-data-brokers [https://perma.cc/E9GR-5KD8] (claiming that "personal information is a hot commodity," which is often sold to the "highest bidder."); *see also* Angela P. Doughty & Mayukh Sircar, *Going Once, Going Twice, Sold: Real Time Bidding Data Privacy Breach*, NAT'L L. REV. (July 8, 2022), https://natlawreview.com/article/going-once-going-twice-sold-real-time-bidding-data-privacy-breach [https://perma.cc/2G2K-WPHF] (discussing how real time bidding works and threatens data privacy).

creating interactions that feel engaging, convenient, and even welcome.[11] At other times, however, these processes are used to surveil users and manipulate users' beliefs, attitudes, and behaviors, rendering them more uniform and predictable for commercial or political ends.[12] How this data is used depends largely on the particular goals of the third parties who purchase the data. Because many of these third parties are subject to market forces, which operate as "by an invisible hand" (in Adam Smith's famous metaphor), market forces are shaping human behavior in ways that mark a qualitative shift in force and potency.

Shoshana Zuboff has termed these new conditions "surveillance capitalism,"[13] a phenomenon that is — we suggest — partly driven by the underappreciated paradigm slip in contract law. Under this economic regime, people are regularly surveilled for prediction and control and subjected to powerful influences that are rarely within their perception — even while thinking themselves "free."[14] Contemporary developments in artificial intelligence enable the detection of once unimaginable patterns in this data,[15] allowing third parties to exploit potent new levers of influence and control. In contemporary conditions, "freedom to contract" is, accordingly, placing us *everywhere in new chains* — to extend Rousseau's evocative metaphor to what has become a central social problem of our time.[16] We dub this situation the

---

11. *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1189 (2016) (describing Facebook's use of user-provided voter participation data to mobilize other users to vote).

12. *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) (disclosing how personal data is increasingly used to control and manipulate individuals, shaping their actions and beliefs, often to make them more regular and predictable, for commercial gain); *see also* Marietjie Botes, *Autonomy and the Social Dilemma of Online Manipulative Behavior*, 3 AI & ETHICS 315, 321 (2023) (noting how corporations covertly exploit personal data to shape beliefs and actions, reducing autonomy for commercial gain).

13. *See* ZUBOFF, *supra* note 12, at The Definition (defining "Surveillance Capitalism").

14. *Id.*

15. *See generally* HENRY A. KISSINGER, ERIC SCHMIDT & DANIEL HUTTENLOCHER, THE AGE OF AI: AND OUR HUMAN FUTURE (2021) (discussing AI's abilities to engage in stunning new forms of pattern detection and how that is transforming the world around human beings and what can be known from data).

16. JEAN JACQUES ROUSSEAU, THE SOCIAL CONTRACT 2 (Rose M. Harrington trans., G.P. Putnam's Sons ed., 1893) (1762) ("MAN is born free, and he is everywhere in chains."). Rousseau used this phrase to describe what he saw as the central paradox of social life in his time. *See, e.g.*, JUDITH SHKLAR, MEN AND CITIZENS: A STUDY OF ROUSSEAU'S SOCIAL THEORY 164 (1969) ("The chains of society, set against man's natural freedom, form the central riddle of Rousseau's politics."). Since then, the question of how to square individual autonomy with the legal enforcement of rules has often been framed in terms of the metaphor of a social contract, which has been fleshed out in many different ways. *See generally* THE SOCIAL CONTRACT FROM HOBBES TO RAWLS (eds. David Boucher & Paul Kelly) (1994) (framing the rise of modern social contract theory as a response to the breakdown of divine and feudal authority, with thinkers like Rousseau, Hobbes, and Locke crafting secular justifications for legal and political norms, followed by 20th century thinkers like Rawls and Gauthier, who seek to adapt the metaphor to address questions relating to modern pluralism

"contractual death of privacy," because it is a crisis precipitated in part by shifts in contract law. As we will demonstrate below, these challenges are so pervasive and profound that they signal an erosion of longstanding, reasonable expectations of privacy in many areas of life, posing significant downstream threats to human freedom and democracy.[17]

From a historical standpoint, this Article thus traces how the paradigm slip in contract law helped foster one of the most significant challenges to privacy and freedom of the modern era. As the paradigm slip progressed, privacy scholars raised alarm bells[18] — and rightly so. They proposed a range of solutions, many of which looked beyond or outside contract law to safeguard privacy and personal information.[19] Yet these approaches cannot fully address the root issues on their own because contract law is meant to support a moral freedom that lies at the core of privacy rights: the right for people "to determine for themselves when, how, and to what extent information about them is communicated to others."[20] Because of that intrinsic connection, contract law will inevitably shape privacy. Contract law's role will, however, remain distorted so long as contract law remains in its current

---

and rationality). The challenges to freedom that we face today may no longer be addressable solely in terms of the metaphor of a social contract, as this Article shows. We may need new concepts, metaphors, and ways of thinking to properly frame solutions to these new challenges, including the use of techniques like shared meaning analysis. It is also important to recognize that these more modern chains have downstream effects on our capacities to engage meaningfully in democracy and collective action. *See generally* ZUBOFF, *supra* note 12 (noting that surveillance capitalism constitutes a qualitatively novel phenomenon, which demands the formulation of new concepts, terminologies, and analytical approaches for its study).

17. *See generally* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999) (arguing that unchecked data collection in cyberspace erodes privacy expectations, threatening self-determination and democratic participation).

18. *See generally, e.g.*, Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 583 (2024) [hereinafter Solove, *Murky Consent*] (arguing that privacy consent is inherently murky, even in contracting contexts, and should rarely be regarded as either full or fully nonexistent consent); Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE L. REV. 308, 397 (2020) (arguing that platform power reveals the inadequacies of consent as a regulatory mechanism, in both practical and normative terms, thus rendering contracts over privacy problematic); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1487 (2019) (examining the failure of the gold standard of digital consent in real-world applications, thus problematizing the contractualization of privacy); Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent*, *in* PRIVACY, BIG DATA AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 44, 45 (Julia Lane, Victoria Stodden, Stefan Bender & Helen Nissenbaum eds., 2015) (analyzing how big data practices bypass traditional privacy protections, such as consent and anonymity, thus rendering contracts over privacy an inadequate protection for privacy concerns); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1886–88 (2013) [hereinafter Solove, *Privacy Self-Management*] (arguing that emphasis on individual consent in privacy law is problematic and insufficient for addressing systematic privacy concerns in the digital age).

19. *See* discussion *infra* Section IV.C.

20. WESTIN, *supra* note 1, at 7; *see* Schwartz, *supra* note 1, at 816; Rachels, *supra* note 1, at 326; Shils, *supra* note 1, at 283.

unjustifiable state. To date, no one has offered a solution to these problems that is sufficiently nuanced to capture the right *moral* relationship between privacy and contract in today's digital landscape.[21]

The paradigm slip in contract law has also received insufficient attention from privacy scholars, leading many debates to center on the overly general question whether privacy policies should be treated as contracts at all.[22] This framing misdiagnoses the complex sources of the problem and limits the imagination with respect to reform. The reason privacy rights have come under increasingly intense challenge over the last several decades is not that privacy policies are being treated as contracts per se but rather that courts are conflating pseudo-contract with contract. Privacy rights can be threatened both when fake, pseudo-contractual "terms" are treated as contract and also when individuals are deprived of traditional rights to contract over privacy.

To resurrect the proper relationship between privacy and contract and return individual control over personal information to a more traditional form, courts must resist the paradigm slip *within* contract law. This requires refocusing contract interpretation on its traditional object: the common meaning of the parties.[23] Courts can do this in digital contexts — where linguistic intuitions often become unmoored — by employing "shared meaning analysis," a method of contract interpretation designed specifically for that purpose and first introduced in *Pseudo-Contract and Shared Meaning Analysis*.[24] By distinguishing pseudo-contract from contract,[25] shared meaning analysis can help courts identify the proper scope and meaning of any actual agreements over privacy and data usage that are reached in the digital age.[26]

In effect, this Article thus extends shared meaning analysis to the critical realm of privacy protection, where we argue it must play a central role if privacy protection is to be meaningfully revitalized. To

---

21. *See* discussion *infra* Sections III.B, IV.C.

22. *See* discussion *infra* Section III.B.

23. *See* RESTATEMENT, CONTRACTS, *supra* note 4, § 201 cmt. c.

24. *See* Kar & Radin, *supra* note 4, at 1166 ("As the rapid explosion of boilerplate text in digital formats has begun to unsettle linguistic intuition, many courts have felt forced to try to assimilate all boilerplate text to 'contract.' This move ignores basic facts about how language works and erases the distinction between shared meaning (contract) and meaning that is not shared (pseudo-contract). Because this distinction is critical to discerning the common meaning of the parties, courts need a simple and workable method to anchor their linguistic intuitions and accurately locate the common meaning of the parties in today's world.").

25. *See id.* at 1143–44 (describing "shared meaning analysis" as offering a "simple conceptual test that courts can use to identify parties' shared meanings and separate contract from pseudo-contract in a principled and practical manner").

26. *See id.* at 1167–68 ("First, courts can identify with greater assurance which boilerplate text does — and does not — fall within the correct scope of parties' contracts. . . . Second, courts can discern hidden conflicts between boilerplate text and the common meaning of the parties that might otherwise go unnoticed. . . . Third, courts can better determine the actual meanings of many other remaining classes of boilerplate text, which are often not contractual at all.").

substantiate these claims, Part II begins with two vignettes designed to show how the same technological changes driving the paradigm slip have created profound new challenges to privacy, freedom, and democracy. Part III examines the legal developments that have led courts to treat online privacy policies as contracts, highlighting privacy scholars' concerns but noting that their concerns have sometimes been limited by an overly general framing of the debate — i.e., in terms of whether privacy policies should be treated as contracts at all. This focus has hindered the development of solutions that might operate *within* the general law of contracts, including the common law of contract interpretation. Part IV shows how shared meaning analysis can fill that gap by returning contract interpretation to its traditional focus,[27] enabling courts to mitigate many significant privacy risks through the common law of contract interpretation. We illustrate by applying the method to certain regularly occurring problems in the privacy context, including brief "contractual" transfers of privacy rights hidden in lengthy online privacy policies, unilateral modification clauses, and widespread forms of consumer deception created by digital contracts over privacy. We end by situating shared meaning analysis within a larger suite of privacy protection proposals, where we argue it must play a pivotal role.

In the process, this Article provides further support for the distinctions and methods of analysis first developed in *Pseudo-Contract and Shared Meaning Analysis*.[28] To revive privacy rights to their more traditional vibrancy and form, courts must return contract law to *its* more traditional form.[29]

---

27. *See* RESTATEMENT, CONTRACTS, *supra* note 4, § 201 cmt. c; *see also* Kar & Radin, *supra* note 4.

28. *See* Kar & Radin, *supra* note 4, at 1214 (explaining how the article collects a set of "linguistic, conceptual, practical, factual, normative, and doctrinal" reasons for courts to employ shared meaning analysis).

29. The central argument in *Pseudo-Contract* was, of course, that contract law should be returned to its more traditional form, but the arguments in that article did not relate to privacy. *See generally* Kar & Radin, *supra* note 4. This Article therefore adds a new and substantial line of argument in favor of curing the paradigm slip in contract law. Though we believe the proper moral relationship between contract and privacy can only be fully recaptured with a return to more traditional contract law principles, we acknowledge that there are also some limited cases where interests in private information should not be alienable at all. Hence, even in a perfect contract law regime, where the paradigm slip has been cured, there may be cases where people should not be allowed to convey personal information by contract. For examples, see Anita Allen, *The Duty to Protect Your Own Privacy*, *in* PRIVACY, SECURITY, AND ACCOUNTABILITY (Adam D. Moore ed., 2015), Ch. 1 (arguing that individuals sometimes have a moral duty to protect some private information, rooted in self-respect and concerns for the social conditions of autonomous agency, which can extend to items like oversharing sensitive financial or medical information or engaging in social media excess); ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011) (arguing that some privacies are foundational to a free society, and noting cases like children's data, workplace secrets, medical disclosures and lifeblogs, where people should sometimes be legally prevented from

II. THE CHANGING LANDSCAPE OF PRIVACY

Pseudo-Contract and Shared Meaning Analysis attributes the paradigm slip in contract law to a convergence of superficially plausible extensions of common law contract doctrines with technological shifts in how parties communicate when they contract.[30] Especially large transformations occurred over the last three decades, as online contracting began to replace many face-to-face transactions and the amount of boilerplate text that is regularly delivered to parties at the point of contracting rapidly proliferated in digital contexts.[31] These historical developments coincided with major advances in computational speed,[32] information storage capacities,[33] and the development of artificial intelligence algorithms and machine learning techniques capable of discerning previously unimaginable patterns in data.[34] As this Part will show in more detail, this data is now regularly collected, analyzed, and used to shape human behavior in ways that are qualitatively unprecedented and create major new challenges to human privacy, freedom, and democracy.

Many scholars have begun to recognize the severity of these emerging challenges.[35] But while there is widespread public agreement

---

contracting away private information). These are important cases, and we claim no monopoly on the legal or other solutions needed to protect privacy interests, including some that may be paternalistic. But we aim here to focus on the more core cases.

30. *See* Kar & Radin, *supra* note 4, at 1140–41.

31. *Id.*; *see also* John A. Rothchild, *Introduction*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 1, 1 (John A. Rothchild ed., 2016) ("The inception of electronic commerce may be dated to 1995, when the U.S. National Science Foundation privatized its internetworking project, the NSFNet, eliminating the acceptable use policy that had restricted the network's use to noncommercial purposes.").

32. *See generally* Diane Coyle & Lucy Hampton, *21st Century Progress in Computing*, 48 TELECOMMS. POL'Y (2024) (documenting a steep decline in the cost of computational speed since the 1990s, driven by innovations like multi-core processors and cloud computing).

33. *See Advances in Physical Storage and Retrieval Made the Loud Possible*, THE ECONOMIST (Jan. 29, 2024), https://www.economist.com/technology-quarterly/2024/01/29/advances-in-physical-storage-and-retrieval-made-the-cloud-possible [https://perma.cc/RD6V-FLG4].

34. *See* JANNA ANDERSON & LEE RAINIE, PEW RSCH. CTR., AS AI SPREADS, EXPERTS PREDICT THE BEST AND WORST CHANGES IN DIGITAL LIFE BY 2035 (2023), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2023/06/PI_2023.06.21_Best-Worst-Digital-Life_2035_FINAL.pdf [https://perma.cc/G3TV-N7XF] (discussing "splashy emergence" of AI and other applications and noting experts' views on AI's rapid evolution, including machine learning advancements that uncover complex data patterns).

35. *See, e.g.*, Coyle & Hampton, *supra* note 32 (examining whether the perception of significant technological innovation is merely illusory); Iqbal H. Sarker, *AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems*, 3 SPRINGER NATURE COMPUT. SCI. (2022), https://link.springer.com/article/10.1007/s42979-022-01043-x [https://perma.cc/U5CP-LKLK] (focusing on the development of effective AI models to address real-world problems).

about the importance of privacy, freedom, and democracy,[36] the general population still remains largely unaware of the full scope of contemporary threats to these values. This situation stems in part from the paradigm slip in contract law going unnoticed by the public and in part from a lack of understanding of the technological advancements that have amplified practices of data collection and analysis. To make contemporary challenges more vivid, we begin with two vignettes, set apart by 40 years, illustrating how similar personal choices and actions — undertaken at different times and through different modalities — can lead to markedly different impacts on privacy, freedom, and democracy.

A. Nico's Case in 1984

Imagine first the year 1984 — a time when personal computers were just emerging, the internet and online contracting were nonexistent, and Americans widely regarded their homes as central bastions of privacy.[37] Picture Nico, a thirty-year-old single woman and homeowner, who, on a weekend afternoon, leaves the privacy of her home to visit a nearby mall. As she navigates various public spaces, she is vaguely aware that passersby, fellow customers, and store employees might observe her actions. At a bookstore, she browses the shelves, lingering over romance novels — her guilty pleasure — but feels unconcerned as no one appears to take notice. Next, she stops at a CVS pharmacy to buy cough drops for a slight tickle in her throat. On impulse, she purchases contraception. Though she feels a slight

36. *See, e.g.*, Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. 1, 28 (2025)("[P]eople expect some degree of privacy in public, and such expectation is reasonable as well as important for freedom, democracy, and individual well-being"); Douglas Schuler, *Computing as Oppression: Authoritarian Technology Poses a Worldwide Threat*, 3 DIGIT. GOV'T: RSCH. & PRAC. 1, 3 (2022) ("[I]f 'advancement' (and 'modernization') just means doing what is being done already, only faster and to more people, then the call, at least in this case, is implicitly describing computing technology whose primary goals are reducing freedom and democracy."); *see generally* Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L. & TECH. 106 (2019) (analyzing how AI poses significant threats to privacy, electoral integrity, and the stability of democratic institutions).

37. For much of American history, people have viewed their homes as one of the most important loci of privacy. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 58–61 (2008). In part because privacy has typically been protected in the home, many people associate being at home with being in private. *See* Boyd v. United States, 116 U.S. 616, 630 (1886) (protecting "the sanctity of a man's home and the privacies of life"). As a result, Americans hold high expectations for privacy within their homes, and they tend to believe that privacy at home should not be compromised. *See* LEE RAINIE & MAEVE DUGGAN, PEW RSCH. CTR., PRIVACY AND INFORMATION SHARING 2 (2016), https://www.pewresearch.org/wp-content/uploads/sites/9/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf [https://perma.cc/CX98-SM47] ("For example, when presented with a scenario in which they might save money on their energy bill by installing a 'smart thermostat' that would monitor their movements around the home, most adults consider this an unacceptable tradeoff (by a 55% to 27% margin).").

discomfort as the cashier processes this item, no one else seems to notice, and she tucks the contraception into her pocketbook, giving it no further thought. On her way home, she grabs a meal at Burger King and buys some lotion and cotton balls at a grocery store. Once home, she calls a close friend to discuss the books she has been reading before settling down with a newspaper.

In the course of these activities, various people — including shop assistants, checkout clerks, fellow customers, or passersby — may have observed Nico and noticed various facts about her, such as her gender, purchases, interests, or location. Some might have inferred additional facts, such as aspects of her health (a possible cold), sexual activities (possibly active), or her favorite brands of lotion and cotton balls. Most of these observations would have nevertheless remained fragmented among people who would not have known her name or identity. Even if they did learn it — say, a cashier processing her credit card — they would lack personal incentives to remember and associate any personal information with her specifically. Likewise, absent unusual circumstances (like a private investigator tracking her), very few people who observed her would have had any market-based incentive to collect or share her information further.

Hence, despite leaving the privacy of her home for a public space where her choices and behavior were visible, most information about Nico likely went unnoticed or was quickly forgotten. In these circumstances, Nico relinquished very little de facto control over personal information she wished to keep private, and few people learned very much about her that she preferred not to disclose.

B. Amadea's Case in 2024

Now imagine it is 2024, and Nico's granddaughter, Amadea, is a 30-year-old single woman and homeowner who values her privacy in similar ways. While sitting in the perceived "privacy" of her home, she grabs her cellphone to purchase several items, instead of visiting a brick-and-mortar mall — as many people now do for routine purchases.[38] Feeling secure in this apparently "private" setting,[39] she goes to Amazon.com, where she sees a pop-up asking her to accept cookies.

---

38. This change reflects a common transformation in purchasing practices. The rapid rise of e-commerce has significantly impacted the traditional retail landscape, leading to a decline in brick-and-mortar stores and a shift in consumer patterns. *See* Hitmi Khalifa Al-Hitmi, *A Transition from Brick-and-Mortar to Online Stores and Its Role in Shifts in Consumer Buying Patterns*, 57 PSYCH. & EDUC. 375, 375 (2020). Online shopping platforms have emerged as a more convenient and accessible alternative, offering a wider range of products, lower prices, and personalized recommendations. *See id.* As a result, consumers have become increasingly reliant on digital shopping experiences, prioritizing ease of use and instant gratification over physical browsing and in-person interactions. *See id.*

39. *See supra* note 37 and accompanying text.

She clicks, "I accept," without reading any details, as most consumers now do.[40] She browses several books, including romance novels — her guilty pleasure, much like Nico's. But because Amadea's browsing history is linked to her name and profile,[41] and because Amazon uses information about her past online behavior to identify books that she may find appealing, Amadea is led to several books that tend to reinforce her political views, rendering her behavior more predictable.[42]

Amadea next visits an online CVS pharmacy, ordering cough drops, lotion, cotton balls, and contraceptives — relieved that the seemingly "discreet" nature of home delivery spares her the "public" discomfort of an in-person purchase. Yet the website retains her shopping history, merges it with data from third parties,[43] and employs sophisticated algorithms to construct a detailed profile of her preferences and other characteristics.[44] She then turns to an online New York Times ("NYT") newsfeed, which presents her with news that is carefully curated to appeal to her political preferences, further entrenching her views and rendering her behavior more predictable.[45] She orders food for delivery from Burger King and uses a social media app to videochat with a friend, discussing the books she is reading and her opinions

40. *See* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 10 (2014); Bakos et al., *supra* note 7 at 1–2.

41. Not only have these personalization techniques become prevalent in online contexts but there is now substantial evidence showing that people increasingly depend on data-driven AI technologies for activities such as shopping, consuming news, and seeking entertainment. *See* Anastasia Kozyreva, Philipp Lorenz-Spreen, Ralph Hertwig, Stephen Lewandowsky & Stefan M. Herzog, *Public Attitudes Towards Algorithmic Personalization and Use of Personal Data Online*, 8 HUMANS. & SOC. SCIS. COMMC'NS (2021). Social media platforms similarly use profiling techniques to personalize the experience of social media. *See* Will Oremus, Chris Alcantara, Jeremy B. Merrill & Artur Galocha, *How Facebook Shapes Your Feed*, WASH. POST (Oct. 26, 2021, 7:00 AM), https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works [https://perma.cc/59SN-5UAZ]; *see also* PAUL HITLIN & LEE RAINIE, PEW RSCH. CTR. FACEBOOK ALGORITHMS AND PERSONAL DATA (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/01/PI_2019.01.16_Facebook-algorithms_FINAL2.pdf [https://perma.cc/A4XW-YTPS].

42. *See generally* L. Elisa Celis, Sayash Kapoor, Farnood Salehi & Nisheeth Vishnoi, *Controlling Polarization in Personalization: An Algorithmic Framework*, *in* FAT* '19: PROCEEDINGS OF THE CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 160 (2019), https://doi.org/10.1145/3287560.3287601 [https://perma.cc/ANY6-GH3D] (discussing how online personalization algorithms, by prioritizing user preferences, can reinforce existing political views and amplify polarization).

43. One popular way to gain access to more data is by making transactions with data brokers. Data brokers are companies that "collect and maintain data on hundreds of millions of consumers, which they analyze, package, and generally sell without consumer permission or input." MAJORITY STAFF OF OFF. OF OVERSIGHT AND INVESTIGATIONS, A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES, at i (2013). By using algorithms, data brokers put consumers into different categories that are sold to marketers to target customers. *See id.*

44. *See generally* ZUBOFF, *supra* note 12 (discussing how technology companies are collecting massive amounts of personal data from users and using it to create predictive models that can influence and control human behavior).

45. *See* Celis et al., *supra* note 42.

on the latest election cycle.[46] Each websites and app she uses has privacy policies that she has clicked "I accept" to at some point in time, and she habitually clicks "I accept" to any cookie pop-ups that appear.

C. Describing the Qualitative Break

Let us now consider how these similar activities — differentiated primarily by the modalities used to engage in them given technological changes over the last 40 years — may affect the relative control that Amadea and Nico have over their personal information and choices. The first point to notice is that Amadea's actions may have *felt* more "private" to her in 2024 than Nico's did in 1984. After all, Amadea remained within the "privacy" of her own home while Nico ventured into "public" spaces to shop.[47]

Yet these feelings, while understandable, are deceiving. By clicking "I agree" to numerous privacy policies and cookie notifications, Amadea has enabled each website in 2024 to collect, organize, and store information about her choices indefinitely, merging it with other sources of data to produce a detailed portrait of the inner workings of her mind.[48] In contrast to the fragmented observations of Nico in 1984, retained only in the fleeting memories of disconnected observers, Amadea's information in 2024 is preserved in digital and machine-readable formats.[49] This data is quickly analyzed by sophisticated and often opaque algorithms — frequently powered by artificial intelligence — to make significant inferences about her.[50] Moreover, strong

---

46. Social media platforms pervasively use algorithms in recommendations, such as YouTube's video suggestions, Facebook's News Feed, and TikTok's "For You Page." *See generally* Kozyreva et al., *supra* note 41 (noting the widespread usage of algorithmic personalization systems in multiple countries).

47. *See supra* note 37 and accompanying text.

48. *See supra* notes 41, 43, 44 & 46 and accompanying texts.

49. In Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198–99 (1998), Kang describes contrasts between in-person and online shopping experiences, highlighting differences in the types of information generated by each. He suggests that offline shopping typically leaves behind only ephemeral traces of information. *Id.* at 1198. By contrast, online shopping produces detailed, computer-processable data that remains permanent, allowing for a more comprehensive tracking of consumer behavior. *Id.* at 1198–99.

50. The inference economy, where personal data is collected, analyzed, and used to make inferences about individuals' behaviors, preferences, and interests, poses increased privacy challenges. *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361 (2022). Recent AI technologies can now be trained on this data to predict or reproduce patterns of thought, speech, action, and attitude. *See generally* Kissinger et al., *supra* note 17 (exploring the implications of AI on society, politics, and the human condition); CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016) (revealing that the increasing reliance on big data and algorithms in various sectors of society has unintended consequences that perpetuate inequality and undermine democracy); FRANK PASQUALE, THE BLACK BOX SOCIETY:

political and market-driven incentives now exist to influence her behavior,[51] leading many third parties — not just the websites Amadea visited — to enter into contractual agreements to acquire information about her choices and characteristics. This type of data sharing is routinely "permitted" by "contract" — or, more accurately, pseudo-contract — when consumers click "I agree" to online privacy policies, cookies, or other disclosures. Many seemingly "free" apps and website services are, in fact, monetized by selling information gleaned from online activities that are surveilled in these ways.

These shifts have significant implications for the relative amounts of privacy and freedom that Nico and Amadea enjoy. Beginning with privacy, the online pharmacy that Amadea uses might be able to infer that Amadea is at the beginning of her second trimester of pregnancy — something she may not have disclosed to anyone else yet — based on her sudden switch to larger quantities of unscented lotion. The pharmacy might share that information with advertisers specializing in products for expectant mothers. This example is far from hypothetical; it mirrors a well-documented 2012 incident, where an algorithm inferred a woman's pregnancy from just such facts and revealed it to her father.[52]

Similarly, combining data on Amadea's purchases with neighborhood epidemiological trends, a third-party or governmental entity might infer she likely has COVID-19 based on her cough medicine purchase.[53] Such entities might bar her untested entry into some venues —

THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2016) (exploring how powerful corporations use secret algorithms and big data to shape and control the economy and the flow of information); BERNHARD ANRIG, WILL BROWNE & MARK GASSON, THE ROLE OF ALGORITHMS IN PROFILING, IN PROFILING THE EUROPEAN CITIZEN: CROSS-DISCIPLINE PERSPECTIVE 65 (M. Hildebrandt & S. Gutwirth eds., 2008) (discussing roles of algorithms in data mining and how they are increasingly used to profile citizens).

51. *See* Das Narayandas & Arijit Sengupta, *Using AI to Adjust Your Marketing and Sales in a Volatile World*, HARV. BUS. REV. (Apr. 12, 2023), https://hbr.org/2023/04/using-ai-to-adjust-your-marketing-and-sales-in-a-volatile-world [https://perma.cc/QR22-NDE8] (highlighting how firms use AI to collect and analyze customer data, predicting behavior to gain competitive market advantages); *see also* Ali Swenson, Dan Merica & Garance Burke, *AI Experimentation is High Risk, High Reward for Low-Profile Political Campaigns*, ASSOCIATED PRESS (June 17, 2024), https://www.ap.org/news-highlights/spotlights/2024/ai-experimentation-is-high-risk-high-reward-for-low-profile-political-campaigns [https://perma.cc/AR2Q-B5TA] (illustrating how political campaigns leverage AI tools to target voters with personalized content, exploiting data to shape electoral outcomes).

52. Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES (Aug. 11, 2022, 4:17 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did [https://perma.cc/WLD2-WQNN].

53. David Ramli, *The Humble Cough Drop Could be Used to Map Omicron's Spread*, JAPAN TIMES (Mar. 16, 2022), https://www.japantimes.co.jp/news/2022/03/10/world/science-health-world/covid-omicron-cough-drops [https://perma.cc/8MQV-PWCQ].

something that has happened in Beijing[54] — or governments might leverage this data to impose quarantines. Data on Amadea's news consumption and usage patterns could also be sold to companies like Cambridge Analytica, which might infer her political views and deploy targeted chatbots to her social media channels. Fueled by artificial intelligence, these chatbots could deliver misinformation that is carefully curated to influence her political behavior, beliefs, and voting tendencies — exacerbating political polarization and weakening the foundations of democratic deliberation.[55]

Likewise, the romance novels that Amadea reads — her guilty pleasure, echoing Nico's — will not remain as private as Amadea hopes, being easily discernible by any company with access to her data.[56] Her "private" social media interaction with her friend may also be less confidential than she assumes, as details of her contacts and conversations could be archived, retrieved, and linked to her later, enabling others to map her social connections and even her intimate romantic behavior.[57]

Hence, while conducting these activities from the "privacy" of her own home may have spared Amadea the short term embarrassment or discomfort of explicit public scrutiny, she would have "purchased" these momentary feelings at the cost of significant, yet dimly perceived, losses of control over substantial aspects of her privacy, freedom, and autonomy. When scaled to collective levels, these erosions of personal agency carry broader consequences, distorting individual and group deliberation and threatening democratic self-governance.

Between 1984 and 2024, profound changes have clearly occurred, which fundamentally alter the way people live and perform many everyday activities. Many members of the general public are cognitively aware that recent technologies raise privacy concerns,[58] but they often

---

54. *See Beijing Tests Shoppers Buying Fever Drugs to Root Out Covid*, BLOOMBERG (Jan. 24, 2022, 4:31 AM), https://www.bloomberg.com/news/articles/2022-01-24/beijing-tests-shoppers-buying-fever-drugs-to-root-out-covid [https://perma.cc/Q6KD-NF7S].

55. This already happened in the Facebook-Cambridge Analytica data breach. *See* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [https://perma.cc/CBY9-4QHE].

56. *See What Are Shopping Profiles?*, AMAZON, https://www.amazon.com/gp/help/customer/display.html [https://perma.cc/K7WR-7HWR] (explaining how Amazon profiles shoppers based on their searches and browsing histories to give tailored recommendations to shoppers based on their inferred tastes and preferences).

57. *See* Blog Zone, *The Influence of Social Media on Dating Behavior and Expectations*, MEDIUM (Mar. 29, 2024), https://medium.com/@blog-zone/the-influence-of-social-media-on-dating-behavior-and-expectations-b73a06626004 [https://perma.cc/VM9N-MDLW].

58. *See generally* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022) (developing a taxonomy of privacy harms in the digital age); *see also* Manheim & Kaplan, *supra* note 36 (examining the potential threats that AI poses to privacy and democratic institutions).

fail to grasp the full severity of the risks tied to routine online activities conducted in spaces that feel relatively "private." This disconnect arises partly from a lack of awareness about the capabilities of recent developments in data collection and analysis — particularly relating to artificial intelligence — and partly from not understanding what they are "agreeing" to when they click "I agree" to many online "terms and conditions" or privacy policies. Furthermore, while the benefits of these technologies, such as personalized experiences, are often made apparent, the risks typically remain obscured, buried in boilerplate text that is seldom read or understood. Consequently, many routine activities that posed minimal privacy risks in 1984 now occur within powerful surveillance regimes that are only dimly perceived by the public.

Problems of commercial surveillance are now widely understood in the literature.[59] Scholars like Shoshanna Zuboff argue that these expanded surveillance practices have ushered in a new socio-economic paradigm known as "surveillance capitalism."[60] What is less well recognized is the degree to which many of the same technological changes that have allowed for the storage and analysis of big data have simultaneously created the paradigm slip in contract law, undermining its ability to ensure that privacy waivers occur only through actual agreement with shared meaning. One common retort to growing privacy concerns in the digital age is that people should be able to voluntarily trade away their privacy rights for things they value more[61] — a principle that holds in theory. Yet, in the digital age, much of this "trading away" occurs through pseudo-contract rather than contract: boilerplate text, tied to an "I agree" click, that is too lengthy and complex for most users to read or understand.[62]

As shown in *Pseudo-Contract and Shared Meaning Analysis*, pseudo-contractual text mimics traditional contractual text in superficial ways, but it is delivered in uncooperative manners, which fail to produce the mutual understandings, or shared meanings, that were once

---

59 . *See generally, e.g.*, OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (2021) (framing commercial surveillance as a pervasive issue extensively explored in contemporary scholarship on personal data commodification); ZUBOFF, *supra* note 12 (positioning commercial surveillance as a dominant, critically examined phenomenon in contemporary academic and public discourse); Greg Elmer, *Panopticon-Discipline-Control*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES 21 (Kirstie Ball, Kevin Haggerty & David Lyon eds., 2014) (situating the Foucauldian analysis of the panopticon within a widely recognized scholarly discourse on surveillance, including its commercial applications).

60. *See generally* ZUBOFF, *supra* note 12.

61. *See e.g.*, Solove, *Murky Consent*, *supra* note 18; Bietti, *supra* note 18; Richards & Hartzog, *supra* note 18, at 1477; Barocas & Nissenbaum, *supra* note 18, at 61; Solove, *Privacy Self-Management*, *supra* note 18, at 1886; Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1905 (2013).

62. On the distinction between pseudo-contract and contract, see Kar & Radin, *supra* note 4, at 1140. For a discussion of these facts about how privacy rights are "traded away," see Obar & Oeldorf-Hirsch, *supra* note 7, at 141.

the traditional focus of contract enforcement.[63] The same technological shifts that exacerbate privacy challenges have thus reshaped contract law,[64] eroding its ability to ensure privacy waivers are truly free, informed, and consensual. In its current state, contract law not only fails to safeguard privacy but — due in large part to an underacknowledged paradigm slip — has also become a significant driver of one of the most profound erosions of privacy, freedom, and democracy in the modern era.

III. THE CONTRACTUAL DEATH OF PRIVACY

This Part examines the relatively recent but increasingly entrenched practice of treating online privacy policies as contracts, provided they are "agreed to" under general principles of contract law that routinely permit clickwrap and browsewrap mechanisms of formation.[65] We refer to these developments, which have solidified over recent decades, as the "contractualization of online privacy policies."

In the online context, privacy policies are collections of text used by digital service providers — such as websites, software, platforms, Internet of Things ("IoT"), or Large Language Model ("LLM") providers — to describe the types of personal data collected, the methods and purposes of data processing and protection, and the scope of third-party data sharing.[66] These policies often describe "secondary uses" of information — "uses *beyond* those necessary to complete the contemplated transaction"[67] — that frequently exceed user expectations. Because of the contractualization of online privacy policies, the extensive pseudo-contractual text in these policies has begun to play a pivotal role in

63. *See* Kar & Radin, *supra* note 4, at 1140.

64. For a brief description of how changes in technology have reshaped contract law, thus producing a "paradigm slip" from a traditional regime of contract law to one in which text that is never cooperatively communicated is treated as "contract" without shared meaning, see *id.*

65. *See* RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 1 ("Such data-privacy provisions may be included in the standard contract terms, or they may be posted on websites, appended to mobile applications, or provided to consumers at retail locations where consumers complete their transactions.").

66. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 15 (1998); *see also* Alfredo J. Perez, Sherali Zeadally & Jonathan Cochran, *A Review and An Empirical Analysis of Privacy Policy and Notices for Consumer Internet of Things*, 1 SEC. & PRIV. (SPECIAL ISSUE) 1, 2 (2018); Isabel Wagner, *Privacy Policies Across the Ages: Content of Privacy Policies 1996–2021*, 26 ACM TRANS. ON PRIV. & SEC., at 32: 13 (May 2023).

67. FEDERAL TRADE COMMISSION, PRIVACY ONLINE, *supra* note 66, at 8. This distinction is important because consumers regularly publicize information in online contexts for specific purposes necessary to complete a contemplated transaction. When they do so, the act of voluntary disclosure is presumably sufficient, in typical cases, to waive control over that information for those limited purposes. But what online privacy policies regularly do is purport to permit many further *secondary* usages of information, which are rarely explicitly contemplated by consumers.

overriding background rules and defining the boundaries of privacy and data practices in many digital contexts.

This legal regime severely erodes privacy, as tech companies have effectively gained the legal power to collect, use, and transfer vast amounts of personal data through "terms" imposed on unsuspecting consumers via hyperlinks to online privacy policies or pop-up banners. This Part explores this legal trend, along with the primary reactions of privacy scholars, who have raised compelling criticisms that merit close attention.[68] Yet their efforts have had limited success in curbing this trend. We call these developments the "contractual death of privacy."

A. The Contractualization of Online Privacy Policies

Returning to Amadea's scenario, imagine it is 2024, and Amadea seeks to access the latest news on the NYT website. Upon doing so, she is prompted to create or log into an account, encountering hyperlinks to the online Terms of Service ("ToS") and a Privacy Policy. Amadea faces a choice: either proceed by creating or logging into a NYT account, thereby "accepting" the ToS and Privacy Policy to read the article, or forgo the article and search for free alternatives via Google or elsewhere. If she opts for the former, courts will interpret her decision as "acceptance" of the extensive boilerplate "terms" in the NYT's ToS and Privacy Policy,[69] presumptively shielding the company from liability for any use or sharing of her data consistent with these documents.[70] Moreover, these online documents often contain arbitration clauses that, by mandating arbitration, effectively eliminate rights to class actions and jury trials, significantly hindering the individual enforcement of even the privacy rights described in these documents.[71]

---

68. *See* Section III.B.

69. *See* RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 11, reporter's notes a.

70. For a look at these terms, see N.Y. TIMES, *Terms of Service*, (May 10, 2024), https://help.nytimes.com/hc/en-us/articles/115014893428-Terms-of-Service, [https://perma.cc/4U58-UCPN] ("If you reside outside of the European Economic Area, your acceptance of these Terms of Service constitutes your consent to the processing activities described in our Privacy Policy under the laws of your jurisdiction. . . . If you choose to use certain NYT products or services displaying or otherwise governed by these Terms of Service . . . you will be agreeing to abide by all of the terms and conditions of these Terms of Service between you and NYT.").

71. Regarding arbitration clauses, see generally Judith Resnik, *Diffusing Disputes: The Public in the Private of Arbitration, the Private in Courts, and the Erasure of Rights*, 124 YALE L.J. 2804 (2015) (noting the mass proliferation of arbitration clauses in online contracts, which waive class actions and jury trials, eviscerating statutory rights). Regarding jury trials, see generally SUJA A. THOMAS, THE MISSING AMERICAN JURY: RESTORING THE FUNDAMENTAL CONSTITUTIONAL ROLE OF THE CRIMINAL, CIVIL, AND GRAND JURIES (2016) (arguing that arbitration clauses, common in modern contracts, displace jury trials, undermining constitutional rights and legal accountability); *see also* Chao Liu & Adam Schwartz, *Stop*

As illustrated by this example, privacy policies are now frequently presented in online contexts through clickwrap or browsewrap mechanisms.[72] Provided a reasonably conspicuous hyperlink is provided, followed by a voluntary "acceptance" by clicking "I accept" or continuing with use of a digital service, the dominant practice in the United States is, increasingly, to treat all this text as creating contract terms, absent a generally available defense like unconscionability.[73] Although this contractual shift is relatively recent,[74] it has gained momentum due to emerging online contracting practices and is now firmly established.[75] Indeed, "[s]tarting with *Northwest Airline* in 2004 and concluding [in 2021] with *Brown v. Google LLC*, . . . there have been 48 cases in which consumers brought breach-of-contract claims for violations of privacy notices."[76] While not all cases have treated privacy policies as contracts,[77] the vast majority have, provided consumers received constructive notice and a meaningful opportunity to decide whether to accept — e.g., by deciding whether to click "I accept" or whether to continue using the relevant services.[78]

Forced Arbitration in Data Privacy Legislation, ELEC. FRONTIER FOUND. (Apr. 19, 2022), https://www.eff.org/deeplinks/2022/04/stop-forced-arbitration-data-privacy-legislation [https://perma.cc/9WPJ-T7AP] (asserting that online contracts routinely embed arbitration clauses, barring class actions and jury trials, thus obstructing data privacy rights enforcement).

72. Thomas Haley*, Illusory Privacy*, 98 IND. L. J. 75, 82 (2022) ("Over the last thirty years, courts charted a course from shrinkwrap to clickwrap that generally deems terms of service enforceable contracts. Privacy policies often come along for the ride.").

73. *See* RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 1 reporter's note a ("A question that has come to the fore in recent times is whether privacy policies posted by businesses, which govern the businesses' data collection, use, and protection practices, are contracts. While a business's general statements of policy (in any area, including privacy) should not be viewed as contracts, a notice that purports to create consent-based rights and obligations should generally be viewed within the subject matter of a consumer contract, in the same way that notices regarding the scope of warranty, remedies, or dispute resolution do. Comment 10 provides a clear answer: Privacy policies that attempt to create consent-based rights and obligations are treated as attempts to form consumer contracts, and the Restatement's rules apply to them.").

74. *Id.*, reporter's note b ("Consumer actions for breach of contract against businesses for violations of privacy notices are relatively recent, and the case law is evolving.").

75. *Id.* ("Consumer actions for breach of contract against businesses for violations of privacy notices are relatively recent, and the case law is evolving. . . . [A] great majority of courts have followed . . . cases, which held that terms in privacy notices give rise to contractual obligations as long as all the necessary elements for contract formation are met.").

76. *Id.* (citing *In re* Northwest Airlines Priv. Litig., No. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004) (noting that Northwestern Airlines offered "no persuasive argument why [the privacy policy] does not form the basis of a contract," even while dismissing breach of contract claim because plaintiffs failed to plead damages from any breach); Brown v. Google LLC, No. 20-cv-03664, 2021 WL 6064009 (N.D. Cal. Dec. 22, 2021) (denying motion to dismiss action that contained breach of contract claims relating to Google's online privacy policy)).

77. *See, e.g.*, *In re* Northwest Airlines Priv. Litig., 2004 WL 1278459, at *6.

78. *See* RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 1 reporter's note b ("The presumptive inclusion of privacy notices in the definition of 'consumer contracts' reflects a basic and longstanding principle of contract law–that the rules do not vary with the subject

This growing trend of treating privacy policies as contracts can coexist with statutory regulations, such as those creating default privacy rights or inalienable rights.[79] Still, when privacy policies are deemed contracts, the scope of privacy and permissible data practices is often dictated largely by pseudo-contractual text, overshadowing background rules that might otherwise establish alienable privacy rights or reasonable expectations of privacy.[80] Two recent, high-profile cases illustrate this shift. In *In re Facebook, Inc.*, a federal court ruled that whether Facebook users consented to data sharing with other entities like Cambridge Analytica was "one of contract interpretation governed by California law."[81] In coming to this conclusion, it noted that "California law requires the Court to pretend that users actually read Facebook's contractual language before clicking their acceptance, even though we all know virtually none of them did."[82] Similarly, in *In re Google Assistant Privacy Litigation*, the court found that users of Google Assistant Enabled Devices ("GAEDs") formed valid contracts with Google by digitally "accepting" its Privacy Policy, shaping their privacy rights.[83] The plaintiffs sufficiently alleged breach of contract claims, citing inconsistencies between the Privacy Policy and Google's activities — specifically, recording private conversations when GAEDs were not in use and sharing these recordings with third parties without explicit, further consent.[84] This trend, which we term the "contractualization of online privacy policies," is often traced back to the

matter of the purported agreement. A qualitative and quantitative analysis of recent cases confirms that this principle is generally applied.").

79. For example, in terms of state privacy statutes, the California Consumer Privacy Act grants California residents with a series of privacy rights, including the right to delete personal information and the right to correct inaccurate personal information. *See* CAL. CIV. CODE § 1798.105–06 (West 2023). Importantly, these rights cannot be waived by contract. *See id.* § 1798.192 (West 2023). Regarding federal privacy statutes, the Gramm-Leach-Bliley Act (GLBA) imposes specific disclosure obligations. *See* 15 U.S.C. § 6803(a)(1)–(2).

80. When we speak of "reasonable expectations of privacy" we mean to refer not to constitutional doctrines that use this phrase but rather to expectations of privacy that arise from background legal or informal norms, which make it reasonable to assume that personal information or data would be used only for limited purposes, such as to complete an explicit transaction.

81. *In re* Facebook, Inc., 402 F. Supp. 3d 767, 789 (N.D. Cal. 2019).

82. *Id.*

83. *In re* Google Assistant Priv. Litig., 546 F. Supp. 3d 945, 964 (N.D. Cal. 2021).

84. *Id.*

2005 case *JetBlue Airways Corp. Privacy Litigation*,[85] which has proven especially influential.[86]

This contractual turn is also increasingly evident in Federal Trade Commission ("FTC") actions. While the FTC does not handle individual contract claims, it can safeguard consumer privacy under Section 5(a) of the FTC Act, which authorizes it to take action against "unfair or deceptive acts or practices in or affecting commerce . . . ."[87] In the context of online privacy policies, the FTC has increasingly adopted a contractual framework to identify unfair practices.[88] For instance, Fred H. Cate notes that many of the FTC's enforcement actions in this area can be distilled to "suing Web site operators when they fail to follow those policies."[89] Similarly, Daniel Solove and Woodrow Hartzog acknowledge that "enforcing broken promises of privacy" is a core focus of many FTC actions.[90] Take the FTC's settlement with Flo, a period and fertility-tracking app: the FTC intervened because "Flo promised to keep users' health data private and only use it to provide the app's services to users" but instead shared it with multiple third parties.[91] The proper contractual interpretation of Flo's privacy policy was pivotal to this FTC action. Thomas Haley echoes these facts,

---

85. In *JetBlue*, a group of airline customers filed a class-action lawsuit against the airline, alleging violations of privacy rights as outlined in the privacy policy on JetBlue's website. *See In re* JetBlue Airways Corp. Priv. Litig., 379 F. Supp. 2d 299, 303–04 (E.D.N.Y. 2005). JetBlue had allegedly shared passenger information with a government contractor without the customers' consent, and the passengers argued that this constituted a breach of JetBlue's online privacy policy. *Id.* The court considers the possibility of a contract, but it emphasizes the plaintiffs' failure to adequately plead specific damages resulting from any alleged breach, which leads to the dismissal of the breach of contract claim. *Id.* at 324–27.

86. *See* RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 1 reporter's note a ("[T]he *JetBlue* approach, which held that privacy notices can create contractual obligations, is the dominant jurisprudence in this area."). The Restatement goes on to say that "a great majority of courts follow two . . . cases . . . , which held that terms in privacy notices give rise to contractual obligations as long as all the necessary elements for contract formation are met." *Id.* (citing *In re* JetBlue Airways Corp. Priv. Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005); *In re* Am. Airlines, Inc., Priv. Litig., 370 F. Supp. 2d 552 (N.D. Tex. 2005)).

87. FTC Act, 15 U.S.C. § 45(a)(1).

88. Privacy scholars have argued that privacy policies were not originally intended for contractual purposes. *See* Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 590–95 (2014) [hereinafter Solove & Hartzog, *FTC Common Law*]. Nonetheless, our focus is not on the intent behind privacy policies. Rather, we highlight that the enforcement of privacy policies in FTC actions is in fact grounded in the contractualization of privacy policies. Understanding the FTC's actions regarding privacy protections is incomplete without considering the contractual model.

89. Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 355 (Jane K. Winn ed., 2006).

90. *See* Solove & Hartzog, *FTC Common Law*, *supra* note 88, at 667.

91. Press Release, FED. TRADE COMM'N, *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data* (Jan. 13, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about [https://perma.cc/LWT6-QQKP].

arguing that a central issue in many FTC enforcement actions is "whether the [privacy policy] sufficiently disclose[s] the challenged practices to enable consumers to consent," enabling contract interpretation of any relevant "terms."[92] In this regime, the FTC's definition of unfair practices is often heavily influence by contract, and, increasingly, pseudo-contract. Because nearly any data practice can be deemed "permissible by contract" if detailed in an "agreed-upon" privacy policy, the FTC's enforcement actions are often limited to ensuring that "the website follows its own policy and provides reasonable security."[93]

These contractual developments can also hinder courts and the FTC in tackling deception. When courts treat privacy policies as contracts, or the FTC implicitly enforces them on a contractual basis, the failure to distinguish pseudo-contract from contract can obscure significant instances of actual consumer deception.[94] Data markets create systematic incentives for companies to communicate beneficial terms cooperatively while hiding harmful text — which might conflict with reasonable expectations of privacy arising from other sources, including their own cooperative communications — in extensive online privacy policies that users rarely read or understand. Actual deception often arises from conflicts between pseudo-contractual text and these reasonable expectations of privacy. Yet, once this pseudo-contractual text is considered part of an "agreed-upon" "contract," detecting this deception for what it is becomes exceedingly difficult.[95]

Despite widespread criticism of the contractualization of online privacy policies by many privacy scholars, these developments have garnered support from some prominent academics in corporate law, contract law, and law and economics.[96] In a 1999 article, for example, Scott Killingsworth, a leading corporate law scholar, argued that a privacy policy "bears all the earmarks of a contract," asserting that "the website's promise and the user's use of the site and submission of personal data are each sufficient consideration to support a contractual

92. *See* Haley, *supra* note 72, at 86 (noting that handling these cases regularly "requires resort to contractual interpretation").

93. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 DICK. L. REV. 587, 606 (2007).

94. *See* Kar & Radin, *supra* note 4, at 1192–207.

95. For illustrations of these phenomena and concrete proposals to address the problems, see *infra* Sections IV.B–C.

96. Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and A New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 189 (2016) ("As privacy policies began to emerge, scholarship argued that contract law should play a role in their enforcement. This view made sense, especially considering that some policies contained statements assuring users that the policies would be binding upon them.").

obligation."[97] Similarly, Omri Ben-Shahar and Lior Strahilevitz, experts in contract law, digital contracting, and law and economics, argue that using contracts to govern privacy and data practices aligns with market mechanisms' core logic.[98] Because they believe that "markets for data are the solution, not the problem,"[99] they suggest that "contracting over privacy is of course permissible."[100] While the trajectory of contract law was uncertain in 1999, it has firmly moved in this direction since that time.

B. Privacy Scholars' Criticisms

Privacy scholars generally advocate treating privacy policies not as binding contracts but as mere statements of corporate policy,[101] arguing that they should not play such a dominant role in defining the scope of privacy rights and permissible data practices.[102] Normatively, they typically oppose relying on market mechanisms implemented via the "notice-and-choice" approach[103] to address privacy concerns, contending that individual contracts and private actions are inadequate to address

97. Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 91 (1999).

98. Omri Ben-Shahar & Lior Strahilevitz, *Contracting Over Privacy: Introduction*, 45 J. LEGAL STUD. S1, S3 (2016) ("There are several specific market mechanisms by which privacy might be regulated, rather than by the government. The primary one is contract. Since the privacy practices that firms employ are part of the contract between the firm and the consumer (often included in the terms of service), this contract becomes a platform for regulation of the parties' privacy rights. Consumers who give up some privacy receive in return something that they value more, often a price discount.").

99. *Id.* at S2.

100. *Id.* at S5.

101. In the privacy literature, privacy policies traditionally are viewed as self-disclosure documents, which promote accountability, transparency, and the legitimacy of data practices. They are said to help consumers make informed decisions about data usage, even while simultaneously holding consumers responsible for their choices and companies accountable for providing adequate notification. *See* Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 104, 104 (2018); Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves et. al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 41–42 (2015).

102. *See* Solove & Hartzog, *FTC Common Law*, *supra* note 88, at 590 ("[S]cholars and practitioners almost take for granted that a privacy policy is a separate document, not a contract or even a set of privately enforceable promises, and that the FTC is the primary enforcer.").

103. In a "notice and choice" regime, "notice" of a privacy policy is generally understood to arise through presentation of a conspicuous hyperlink, whereas "choice" arises when users are given an option over data practices, often in the form of an opt-out provision. *See* Solove & Hartzog, *FTC Common Law*, *supra* note 88, at 592; *see also* FEDERAL TRADE COMMISSION, PRIVACY ONLINE, *supra* note 66, at 9. For critical discussion of reliance on such mechanisms to protect privacy, which rely in part on normative arguments, see Solove & Hartzog, *FTC Common Law*, *supra* note 88.

the scale and nature of contemporary privacy risks.[104] As the contractualization of online privacy policies advanced, privacy scholars therefore sounded the alarm.[105]

Frequently, their concerns are framed as objections to the "notice-and-choice" approach to privacy, which extends beyond contract law, yet their critiques of the "notice-and-choice" paradigm apply equally to the contractualization of online privacy policies.[106] Privacy scholars tend to highlight two overlapping dimensions of criticism: one grounded in practical feasibility, the other in normative justification. Practically, they point to operational difficulties in digital contexts with providing adequate notice and securing genuine consent for the data practices commonly found in online privacy policies.[107] From a justificatory perspective, they argue that the diminished consent typically obtained online is insufficient to shape prevailing privacy and data practices legitimately.[108]

1. Practical Obstacles Relating to Intelligibility, Decision-Making and Asymmetry

Privacy scholars have identified three key practical barriers to obtaining quality consent when online privacy policies are treated as contracts: obstacles to intelligibility, failures of rational decision-making, and asymmetries in information and power.

Intelligibility Obstacles. The challenge of intelligibility stems in part from the fact that online privacy policies are rarely read or understood by the average consumer. A recent empirical study found that the average time consumers take to "agree" to privacy policies is far less the time consumers needed to read them,[109] indicating that many

104. *See*, *e.g.*, Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMEND. INST. (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/79M8-B7L3] ("Current approaches to crafting privacy legislation are heavily influenced by the antiquated private law ideal of bottom-up governance via assertion of individual rights, and that approach, in turn, systematically undermines prospects for effective governance of networked processes that operate at scale.").

105. *See, e.g.*, *infra* Sections III.B.1–2.

106. It is worth noting that the practice of publicizing online privacy policies initially emerged not as an innovative contracting mechanism but as a response to more basic "notice-and-choice" principles that often arise within privacy law. *See* Waldman, *supra* note 101, at 131. Many industries have favored the "notice-and-choice" approach in part to establish the benefits of self-regulation and prevent other forms of regulation. *See* Solove & Hartzog, *FTC Common Law*, *supra* note 88, at 592–94. Under this "notice-and-choice" framework, consent is typically given by inaction rather than requiring an explicit agreement before data practices commence. *See id.* Though not every case where notice-and-choice principles have been met would qualify as a contract, under standard principles of contract formation, when a contract has been formed, there has typically been both notice (in the form of an offer) and choice (in the form of acceptance). *See id.* at 592–95.

107. *See, e.g.*, *infra* Sections III.B.1–2.

108. *See, e.g.*, *infra* Section III.B.2.

109. *See generally* Obar & Oeldorf-Hirsch, *supra* note 7.

"agree" without reading.[110] The Pew Research Center reports that while 97% of American users encounter requests to approve online privacy policies, "only about one-in-five adults overall say they always (9%) or often (13%) read a company's privacy policy."[111] These policies are often lengthy, with many exceeding the U.S. Constitution in word count.[112] One estimate calculates that reading all privacy policies would take an individual an average 244 hours annually,[113] equivalent to one-and-a-half months of full-time work. Studies from as early as 2008 estimate that reading privacy policies would cost each American internet user approximately $3,534 annually, totaling in a national cost of approximately $781 billion per year for the United States.[114] These costs, likely even higher today, make reading impractical and often irrational in many digital contexts. These facts help explain why so few users ever read the extensive boilerplate text in privacy policies.

Moreover, even if consumers did read online privacy policies, few would be able to comprehend them. These policies frequently employ technical jargon, which can challenge even specialists like engineers, computer scientists, and data scientists. A representative study reveals that even well-educated users, such as those with graduate degrees, often lack adequate understanding of key practices and concepts referenced, such as "cloud computing, online security, and the data trade for personal information online."[115] When made aware of how cloud service providers manage their data, users typically express disapproval.[116]

While intelligibility issues can arise with boilerplate text in many contracting contexts,[117] privacy policies pose unique challenges due to their frequent descriptions of data practices involving complex

---

110. *Id.* at 140.

111. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kamar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/PRG4-3EB6].

112. Blanca Bosker, *Facebook Privacy Policy Explained: It's Longer Than the Constitution*, HUFFPOST (May. 25, 2011), https://www.huffpost.com/entry/facebook-privacy-policy-s_n_574389 [https://perma.cc/ADV5-6CMG].

113. Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 274 (2012).

114. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 565 (2008).

115. Masooda Bashir, April D. Lambert, Carol Hayes & Jay P. Kesan, *Online Privacy and Informed Consent: The Dilemma of Information Asymmetry*, 52 PROC. OF THE ASS'N FOR THE INFO. SCI. & TECH. 1, 8 (2015).

116. *Id.*

117. *See generally* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012) [hereinafter RADIN, BOILERPLATE] (arguing that boilerplate contracts are ubiquitous, nonnegotiable, and rarely read, such that their enforcement erodes individual rights and undermines the rule of law by enabling companies to systematically strip consumers of legal protections through fine-print terms).

algorithms and machine learning, which even many experts struggle to grasp.[118] Unlike traditional computer algorithms, many modern AI and machine learning systems rely on patterns of statistical inference or neural networking models, making their operations especially opaque.[119] Explaining the full workings of "black-box" algorithms to consumers is virtually impossible, and even articulating the fundamental differences between these newer and more traditional forms of computation can be challenging.

Additionally, some AI systems evolve autonomously, and are trained on vast datasets, creating further obstacles to intelligibility.[120] Most consumers remain unaware of the full power of emerging algorithms to detect patterns in big data — patterns unimaginable just decades ago, such as the likely chemical structures of undiscovered antibiotics or chess strategies that can outwit grandmasters.[121] When faced with algorithms capable of mimicking human language, generating realistic images from text, or performing complex facial recognition,[122] consumers are not yet equipped to anticipate the behavioral patterns or levers of influence that might be extracted from their online activities. A recent Pew Research Center survey underscores this fact, revealing that 74% of Facebook users are unaware that the platform even uses algorithms to profile their traits and interests, despite this

118. James Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Leaning Algorithms*, BIG DATA & SOC'Y, Jan.–June 2016, at 4.

119. *Id.* at 4–5.

120. Edd Gent, *Artificial Intelligence Is Evolving All By Itself*, SCI. (Apr. 13, 2020), https://www.science.org/content/article/artificial-intelligence-evolving-all-itself [https://perma.cc/8JYV-DSEX]. For example, AI can sometimes develop its own languages that humans cannot decipher. In response to such challenges, the only effective intervention can sometimes be to shut down the program. Mathew Field, *Facebook Shuts Down Robots After They Invent Their Own Language*, TELEGRAPH (Aug. 1, 2017), https://www.telegraph.co.uk/technology/2017/08/01/facebook-shuts-robots-invent-language/ [https://perma.cc/GM8W-HFTY].

121. Regarding antibiotic discovery, see Anne Trafton, *Artificial Intelligence Yields New Antibiotic*, MIT NEWS (Feb. 20, 2020), https://news.mit.edu/2020/artificial-intelligence-identifies-new-antibiotic-0220 [https://perma.cc/CC6D-UY3C]. Regarding chess strategies, see Matthew Sadler & Natasha Regan, *DeepMind's Superhuman AI is Rewriting How We Play Chess*, WIRED (Feb. 3, 2019, 1:00 AM), https://www.wired.com/story/deepmind-ai-chess/ [https://perma.cc/H67H-YDRM].

122. Regarding human linguistic behavior, see Adam Zewe, *AI That Can Learn the Patterns of Human Language*, MIT NEWS (Aug. 30, 2022), https://news.mit.edu/2022/ai-learn-patterns-language-0830 [https://perma.cc/X7N8-WBA5]. Regarding artistic image creation, see Atte Oksanen, Anica Cvetkovic, Nalan Akin, Rita Latikka, Jenna Berdahl, Yang Chen et al., *Artificial Intelligence in Fine Arts: A Systematic Review of Empirical Research*, COMPUTS. IN HUM. BEHAV.: ARTIFICIAL. HUMS., Aug.–Dec. 2023, at 1. Regarding facial identification, see Kate Baggaley, *How Facial Recognition Systems Will Reshape Your Daily Life*, NBC NEWS (Sept. 14, 2017 2:12 PM), https://www.nbcnews.com/mach/tech/how-facial-recognition-systems-will-reshape-your-daily-life-ncna801336 [https://perma.cc/TZ3X-AGBT].

giant tech company disclosing these practices accessibly on its website.[123]

Failures of Rational Decision-Making. Even if individuals read and understood online privacy policies, many would struggle with rational decision-making. It is widely recognized that most people do not deliberate like the idealized "homo economicus" of classical economics paradigms,[124] instead displaying well-documented heuristics and biases.[125] These decision-making challenges are especially acute in complex scenarios like this, where the costs and benefits of options are difficult to assess. The complexity and opacity of online privacy policies often result in "both the inability to calculate probabilities and amounts for risks and related costs for the various possible individual strategies, . . . [and] the inability to process all the uncertain and stochastic information related to information security costs and benefits."[126] This problem, which heightens reliance on heuristics and biases, is well-documented in the privacy context.[127]

One key finding is particularly relevant in this context: empirical studies show that individuals are more likely to share personal data with tech companies when they *feel* in control, even if that sense of control is illusory.[128] This "feeling in control" heuristic can be illustrated by revisiting to the contrast between Nico and Amadea.[129] In 1984, Nico felt she had little control over publicly observable information about her choices when she left her home to visit the mall. By contrast, Amadea felt more in control when she engaged in analogous activities

---

123. HITLIN & RAINIE, *supra* note 41.

124. *See generally* Elizabeth Anderson, *Beyond Homo Economicus: New Developments in Theories of Social Norms*, 29 PHIL. & PUB. AFF. 170 (2000).

125. For a classical discussion, see generally Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCI. 1124 (1974). Richard Thaler and Cass Sunstein discuss similar topics from the perspective of behavioral economics. *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2009). For discussions of how some of these heuristics and biases appear in the specific context of privacy policies, see generally, e.g., Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us about Privacy*?, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES (Alessandro Acquisti et al. eds., 2008); Ian Kerr, Jennifer Barrigar, Jacquelyn Burkell & Katie Black, *Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY (Ian Kerr, Valerie Steeves & Carole Lucock eds., 2009); Zareef A. Mohammed & Gurvirender P. Tejay, *Examining the Privacy Paradox Through Individuals' Neural Disposition in E-Commerce: An Exploratory Neuroimaging Study*, 104 COMPUTS. & SEC. 1 (2021).

126. Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, *in* ECONOMICS OF INFORMATION SECURITY 165, 172 (L. Jean Camp & Stephen Lewis eds., 2004).

127. *See* Solove, *Privacy Self-Management*, *supra* note 18, at 1886–88.

128. Laura Brandimarte, Alessandro Acquisiti & George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCH. & PERSONALITY SCI. 340, 341 (2013).

129. *See supra* Section II.A (describing the story of Nico), II.B (describing the story of Amadea).

in 2024, because she felt secure in the "privacy" of her own home. Yet despite these perceptions, Amadea had significantly less control than Nico over the information and inferences collected and shared about her choices. A critical issue with online privacy policies is that they are often "agreed to" in settings that foster intuitive but misplaced feelings of privacy and control.

These dynamics help explain the so-called "privacy paradox," where significant discrepancies exist between individuals' privacy attitudes and behaviors.[130] Many claim to value their privacy highly, yet frequently "agree" to surrender sensitive personal data to companies for minor discounts or conveniences.[131] While intelligibility issues contribute to this paradoxical behavior, so too do failures of rational decision-making and the deceptive sense of control that pervades many online contexts.

Another systematic barrier to rational decision-making arises stems from corporations deliberately nudging consumers into choices that conflict with their reflective interests through strategic website and contract design. Scholars use the term "dark patterns" to refer to "user interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions."[132] Dark patterns are increasingly common in the digital landscape,[133] driven by market incentives that disadvantage corporations that fail to use them, in unregulated markets. Examples include

---

130. For a survey of the privacy paradox literature, see Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox--Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior — A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038, 1040–43 (2017).

131. *Id.*

132. Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 44 (2021).

133. The California Privacy Rights Act and the EU's Digital Services Act start to define and regulate dark patterns. *See* CAL. CIV. CODE § 1798.140(l) (West 2023) ("'Dark pattern' means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation."); *see also* Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), O.J. (L 277), recital 67 ("Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions."). The FTC acknowledges the significant difficulties that dark patterns present to consumers. *See* FED. TRADE COMM'N, STAFF REPORT: BRINGING DARK PATTERNS TO LIGHT (2022). The academy also recognizes the prevalence of dark patterns. *See generally, e.g.*, Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty et. al., *Dark Patterns at Scale: Findings From a Crawl of 11k Shopping Websites*, 3 PROC. ACM HUM.-COMPUT. INTERACTION (2019); Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba & Alberto Bacchelli, *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, 2020 PROC. CHI CONF. ON HUM. FACTORS IN COMPUTING SYS.

persistent consent requests via unavoidable pop-ups[134] and cookie consent banners that highlight the "accept all" button over the "decline" option.[135] More critically, the algorithms processing data transferred via pseudo-contract are becoming so advanced that they can detect subtle, nuanced, and highly targeted levers of consumer and political influence. Given the rapid evolution of technologies and data practices, no regulatory framework can keep pace to address all these emerging mechanisms of influence and control.

Unfortunately, the assumption of a "liberal self" — capable of autonomous choice and rational self-determination even in complex digital markets — has often dominated policy debates on privacy protection.[136] Because assumptions of rationality are typically needed to justify the view that contracting over private data serves the core functions of markets, many privacy scholars remain sharply critical of the growing contractualization of online privacy policies.

Asymmetries in Information and Power. Another significant barrier to contractual approaches to privacy stems from systematic asymmetries in information and power between consumers and tech companies. Information asymmetries, often exacerbated by the intelligibility obstacles outlined earlier, arise from multiple sources in the context of online privacy policies. A notable example is the disparity in access to information about data processing and sharing: companies have direct and comprehensive access to details about the data they collect, their processing methods, and the entities they share data with, while consumers rarely have access to such specifics.[137] Take the Privacy Policy of Philips, which appears in its Sonicare app.[138] This policy has been described as "troublesome" because it states, in highly general terms, that Philips may share personal data with third parties who will process it "for their own purposes."[139] For individual users, who often face multiple privacy policies daily, discerning the identity of these third parties or their purposes is nearly impossible. Meanwhile, corporations and third parties contracting over this data typically have access to sophisticated models to price the data and pinpoint its uses, while consumers struggle to assess the basic costs and benefits of agreeing to privacy policies.[140]

---

134. Martine Brenncke, *Regulating Dark Patterns*, NOTRE DAME J. INT'L & COMP. L. 1, 38, 71 (2024).

135. *Id.* at 33.

136. *See* Cohen, *supra* note 61, at 1905.

137. *See* Solove, *Privacy Self-Management*, *supra* note 18, at 1889–91.

138. Jennifer Schlesinger & Andrea Day, *Most People Just Click and Accept Privacy Policies Without Reading Them — You Might Be Surprised at What They Allow Companies To Do,* CNBC (Mar. 15, 2019, 1:49 PM EDT), https://www.cnbc.com/2019/02/07/privacy-policies-give-companies-lots-of-room-to-collect-share-data.html [https://perma.cc/84DH-AJR3].

139. *Id.*

140. *See* Solove, *Privacy Self-Management*, *supra* note 18, at 1888.

Information asymmetries also arise when the workings of algorithms are far less transparent to consumers than to corporations. For example, a search engine might present "privacy-sensitive" and "privacy-intrusive" options, but without equal access to information about their implementation, users can struggle to understand the implications of these choices, often realizing the consequences only when problematic data uses arise and are brought to their attention.[141]

Power asymmetries, which are conceptually distinguishable from information asymmetries, further complicate the landscape, as online privacy policies are typically drafted by sophisticated multinational corporations. These corporations often present policies to consumers on a take-it-or-leave-it basis,[142] leaving individual consumers — who are typically dispersed and relatively powerless — little room to negotiate the "terms." In any event, similar terms are frequently replicated across competing products within an industry, also on a take-it-or-leave-it basis.[143] For example, users of services like Facebook or Google face a stark choice: "accept" the privacy policies or forgo the service, losing vital connections on these platforms. Refusing services from highly networked tech giants like these, which often have similar terms, effectively equates to opting out of crucial benefits associated with the Internet and social networking in modern society. Such a decision can have profound consequences for social and economic engagement.[144] These asymmetries in information and power provide further reasons why many privacy scholars remain deeply concerned about the contractualization of online privacy policies.[145]

2. Justificatory Obstacles Related to Quality of Consent

In part because of the practical consent issues outlined above, many privacy scholars argue that treating privacy policies as binding contracts lacks adequate justification.[146] While these scholars are

---

141. *See* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE SEC. & PRIV. 26, 26 (2005).

142. *See* Solove, *Murky Consent*, *supra* note 18, at 600, 607.

143. For example, unilateral modification clauses can be found in almost every privacy policy. *See infra* Section IV.B.2.

144. *See* Richards & Hartzog, *supra* note 18, at 1487.

145. For Bietti, the type of consent that is regularly obtained in this context not only fails to ethically justify loss of control over personal information but is also "being weaponized by powerful industry actors to forward their agenda." *See* Bietti, *supra* note 18, at 382.

146. *See, e.g.*, Solove, *Murky Consent*, *supra* note 18, at 596 ("Most privacy consent is a fiction. When the law allows dubious or nonexistent consent to masquerade as valid consent, it grants unwarranted legitimacy to data collection, use, and disclosure"); Bietti, *supra* note 18, at 315–16 ("[C]onsent is structurally incapable of empowering individuals in the platform economy. . . . This is not an argument about the validity of individual instances of digital consent, but rather the justifiability of relying on notice and consent as a default practice.");

acutely aware of the privacy challenges posed by online contracting practices, they are often less versed in the doctrinal nuances and evolutionary trajectory of contract law itself. Instead of engaging substantively with those legal dynamics, they typically frame their justificatory concerns by defining an idealized level of consent — one they believe should be required before individuals can legitimately relinquish control over their information[147] — and then point out substantial gaps between this standard and current practices of contracting over privacy.[148]

Prominent scholars such as Neil Richards and Woodrow Hartzog have proposed what they term a "gold standard" of consent, which they view as an aspirational benchmark across many contexts, including privacy.[149] They argue that this standard requires that parties not only comprehend the full implications — both benefits and risks — of data processing activities but also voluntarily trade their privacy rights, knowing the risks, for the service or product offered.[150] Often characterized as "knowing and voluntary" consent, this standard represents an exacting ideal.[151]

The practical problems outlined above — encompassing issues of intelligibility, cognitive limitations in decision-making, and asymmetries in information and power — suggest that this gold standard of consent is rarely met with respect to all the "terms" in online privacy policies. When users ostensibly "agree" to privacy policies through clickwrap or browsewrap mechanisms, pervasive intelligibility barriers and information asymmetries frequently hinder full knowing consent,[152] while power asymmetries and the absence of meaningful alternatives often compromise the voluntariness of contractual consent.[153] For these scholars, these conditions thus foster a climate of uninformed and involuntary consent, significantly undermining the legitimacy of treating the extensive boilerplate text in online privacy policies as contracts.

These critiques extend beyond consent-specific concerns. More generally, privacy scholars often contend that contractual approaches

---

Barocas & Nissenbaum, *supra* note 18, at 45 ("In the case of consent, too, commonly perceived operational challenges have distracted from the ultimate inefficacy of consent as a matter of individual choice and the absurdity of believing that notice and consent can fully specify the terms of interaction between data collector and data subject.").

147. *See* sources cited *supra* note 146. *See also* Richards & Hartzog, *supra* note 18, at 1464; NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019) [hereinafter KIM] (arguing that consent is necessary for broad autonomy).

148. *See* KIM, *supra* note 147, at 49–116.

149. *See* Richards & Hartzog, *supra* note 18, at 1464.

150. *Id.*

151. *Id.*

152. *See supra* Section III.B.1.

153. *See* Richards & Hartzog, *supra* note 18, at 1488 ("Our point is that most consumers in the digital environment have highly limited options for consent, much less for bargaining. This is particularly the case where monopoly power or something like it applies.").

to privacy and data management are fundamentally ill-equipped to address the privacy challenges posed by modern digital platforms.[154] Richards and Hartzog, for example, assert that treating online privacy policies as binding contracts is a "poor fit for data practices."[155] Daniel Solove further problematizes the contractual approach, arguing that relying on contract law to address nuanced questions of the quality of consent is misguided, suggesting that, at best, contract law "just poses more questions."[156] These views reflect the prevailing views of privacy scholars.[157]

C. The Limited Impact of Privacy Concerns

Despite the compelling nature of the concerns raised by privacy scholars, their arguments have thus far had little impact on the increasingly entrenched trend of treating online privacy policies as contracts, provided general principles of contract formation are met. This limited traction stems in part from a disciplinary disconnect: many privacy scholars, who are not typically experts in contract law, have yet to wrestle fully with the internal dynamics of contract law, particularly the recent paradigm slip into a legal regime of pseudo-contract. Hence, while they are keenly attuned to the importance of privacy and data rights, they have not always recognized how the obstacles they identify — relating to intelligibility, bounded rationality, asymmetries of information and power, and justificatory gaps — are not unique to privacy policies but rather endemic to digital contracting more broadly due to the paradigm slip.[158]

---

154. *See, e.g.*, Bietti, *supra* note 18, at 313, 315–16.

155. *See* Richards & Hartzog, *supra* note 18, at 1479.

156. *See* Solove, *Murky Consent*, *supra* note 18, at 630.

157. Solon Barocas and Helen Nissenbaum assert that faith in contract law to handle the complex questions raised by privacy policies is misplaced because it is impossible to for privacy policies to clarify and regulate the complicated interactions between consumers and companies involving Big Data. *See* Barocas & Nissenbaum, *supra* note 18, at 45. While less focused on contract law per se, Elettra Bietti argues that centering data privacy regulation on a notice and consent approach is unjustifiable in the digital context due to the structurally unjust and exploitative nature of the platform economy. *See* Bietti, *supra* note 18, at 397. While contract law may seem like a suitable framework for implementing basic notice and consent principles relevant to privacy, Thomas Haley argues that the real world applications of contract law to this context render these notice and consent principles ineffective and ultimately "worthless." *See* Haley, *supra* note 72, at 104.

158. *See, e.g.*, RADIN, BOILERPLATE, *supra* note 117, at 23–29; Bakos et al., *supra* note 7 at 2; BEN-SHAHAR & SCHNEIDER, *supra* note 40, at 14–25; RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 1 reporters' notes a ("Informed consent to the standard contract terms is, by and large, absent in the typical consumer contract. This empirical fact is recognized by the courts in formulating the rules stated in this Section. . . . courts routinely enforce standard contract terms, even in the absence of informed consent to those terms, if several minimum requirements are met."); Lucian A. Bebchuk & Richard A. Posner, *One-Sided Contracts in Competitive Consumer Markets*, *in* BOILERPLATE: THE FOUNDATION OF MARKET CONTRACTS 3, 4 (Omri Ben-Shahar ed., 2007).

Unfortunately, the paradigm slip is real: courts have firmly established that "contracts" can be formed, quite generally, in online contexts through clickwrap and browsewrap mechanisms, where pseudo-contract is routinely assimilated to contract.[159] Hence, unless a standard contract defense applies, the extensive pseudo-contractual text in these online documents now adds "terms" to these "contracts," whether the text is ever read or understood, provided that a consumer manifests assent to a basic transaction after receiving: "(1) reasonable notice of the [standard contract] term and of the intent to include the term in the consumer contract, and (2) reasonable opportunity to review the [standard contract] term."[160] These rules are broadly applicable in contract law, independent of the subject matter of the contract.[161]

These principles pose challenges across multiple domains, affecting not only privacy but also to arbitration, class actions, indemnity waivers, choice-of-forum clauses, software licenses, and beyond.[162] But many of these problems stem from the general, highly problematic paradigm slip *within* contract law — i.e., from a traditional contract law regime to one of pseudo-contract[163] — suggesting that a more comprehensive solution *within* contract law may be needed. Because privacy scholars have not yet fully grappled with these broader dynamics of contract law, they have typically concentrated on either outright rejection of the contractualization of online privacy policies or advocating that privacy should be treated as a special subject matter for contracting purposes.[164] Such approaches, however, face significant resistance due

159. *See* RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 2 reporters' notes f ("A traditional analysis focusing exclusively on all the decisions by state supreme and appellate courts through 2022 reveals that courts routinely hold that the clickwrap method is effective in adopting the terms, as long as a clear notice alerts the consumer that such terms are intended to be part of the contract."); *id.* § 2 reporter's note g ("Another common procedure in electronic and web-based transactions dispenses with the 'I Agree' click. The website includes a link to another page with the standard terms, and consumers, by proceeding with the purchase or simply by continuing to use the website, are deemed to have adopted the standard terms as part of the contract.").

160. *Id.* § 2 (a).

161. *Id.* § 1 reporters' note b ("The presumptive inclusion of privacy notices in the definition of 'consumer contracts' reflects a basic and longstanding principle of contract law — that the rules do not vary with the subject matter of the purported agreement. A qualitative and quantitative analysis of recent cases confirms that this principle is generally applied.").

162. *See* Kar & Radin, *supra* note 4, at 1203–06; *see generally* RADIN, BOILERPLATE, *supra* note 117.

163. *See* Kar & Radin, *supra* note 4, at 1142.

164. *See* DAN SOLOVE, THE DIGITAL PERSON 91 (2004) ("The market can work well, but not in the absence of structural legal protections. A set of laws and rights is necessary to govern our relationship with bureaucracies. These laws must consist of more than default rules that can be contracted around or property entitlements that can be bartered away."); Barocas & Nissenbaum, *supra* note 18, at 45 ("In the case of consent, too, commonly perceived operational challenges have distracted from the ultimate inefficacy of consent as a matter of individual choice and the absurdity of believing that notice and consent can fully specify the terms of interaction between data collector and data subject."); Bietti, *supra* note

to the prevailing trajectory of modern contract law and online contracting practices.[165]

The current focus has also led privacy scholars to overlook proposals that might operate within the general common law of contracts to address their concerns. The next Part presents just such a proposal, arguing for its vital role in modern privacy protection — not as the sole solution but as an essential complement to existing statutory frameworks and other proposals if privacy protection is to be brought back to significant life.

IV. THE CONTRACTUAL REBIRTH OF PRIVACY

The technological changes and evolving mechanisms of contract formation described in the last Part led *Pseudo-Contract and Shared Meaning Analysis* to identify a "paradigm slip" in contract law — from a legal regime that once enforced actual agreements reached through cooperative language use to one where parties merely assume the risk of unilateral private obligations created by pseudo-contractual text that is rarely read or understood in online contexts.[166] The article highlighted a complex constellation of linguistic, [167] conceptual, [168]

18, at 315 ("[C]onsent is structurally incapable of empowering individuals in the platform economy."); Haley, *supra* note 73, at 104 ("The fundamental disconnect between when consumers provide data and when platforms find novel, useful, and troubling applications for that data renders contractual regulation worthless.").

165. *See e.g.*, RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 1 reporters' notes b, § 2 reporters' notes f.

166. *See id.* at 1138–44.

167. Linguistically, these developments fail to recognize the degree to which contract meaning depends upon forms of linguistic cooperation that are regularly violated when boilerplate text that is too extensive or complex to create any shared meaning is treated as if it is part of an actual agreement. *Id.* at 1160–65.

168. Conceptually, this has led courts to conflate shared meaning (traditional contract) with meaning that is not shared (pseudo-contract), thus "shift[ing] and distort[ing] the meanings of many core contract law concepts — including 'assent,' 'agreement,' 'interpretation,' 'term,' 'bargain,' and even 'contract' itself." *Id.* at 1214.

practical,[169] factual,[170] normative,[171] and doctrinal[172] problems stemming from this underrecognized shift.[173] The privacy risks posed by treating online privacy policies as contracts reflect an additional layer of challenges, partially rooted in the paradigm slip, which that article did not fully explore.

The article also proposed shared meaning analysis, a method courts can use to discern the common meaning of the parties in modern contexts and counter this complex constellation of problems.[174] This Part explores shared meaning analysis, detailing how it serves as a general approach to contract interpretation, rooted in traditional contract law principles and fundamental truths about contract meaning. It then applies the method to tackle three prevalent issues in online privacy policies: questions of proper contractual scope, unilateral modification clauses, and hidden conflicts and deception.

While shared meaning will not solve every privacy risk outlined in this Article, it provides a nuanced, case-by-case method to determine contract meaning that can enhance — and prove essential to — any comprehensive, multi-pronged strategy to revitalize privacy in today's digital landscape. The Part concludes by comparing this approach, which operates within the common law of contracts, with several others in the literature and illustrating its role within a broader suite of contemporary privacy strategies.

A. Shared Meaning Analysis

Shared meaning analysis is anchored in a core principle of contract law: when interpreting a contract, "the primary search is for a common

---

169. These conceptual problems create further practical problems for markets, because when courts and others find it hard to distinguish pseudo-contract from the common meaning of the parties, the legal regime of pseudo-contract "incentiviz[es] new and expanding forms of mass-market deception, especially in many consumer markets, and an inexorable race to the bottom for pseudo-contractual 'terms' of poor quality." *Id.* (citing George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488 (1970) for classical treatment of how problems like these can create races to the bottom).

170. These developments also rest on factual assumptions that are false — and, indeed, often technologically naïve and outdated — because they "fail to recognize just how many noncontractual functions boilerplate text now serves" in online contexts like these. *Id.*; *see also id.* at 1207–13.

171. These developments wrest contract law from its traditional sources of justification, which focused on the legal enforcement of actual agreements with shared meaning. *Id.* at 1214–15.

172. *Id.* at 1215 ("These developments have, in turn, begun to create serious tensions and incoherencies in legal doctrine.").

173. *Id.* ("Like a tangled yarn, these different problems — the linguistic, conceptual, practical, factual, normative, and doctrinal problems with the paradigm slip into pseudo-contract — are highly interwoven and very difficult to separate out and discern, let alone address, in piecemeal fashion.").

174. *Id.* at 1166–67.

meaning of the parties."[175] Contract interpretation must therefore always be grounded "in a nuanced and careful assessment of the common understandings that parties produce when they use language to form contracts."[176] When courts engage in contract interpretation, they rely on linguistic capacities that typically operate unconsciously but in accordance with principles that philosophers of language have been able to identify.[177] *Pseudo-Contract and Shared Meaning Analysis* thus draws on the work of one such philosopher, Paul Grice, to make those principles clear and specify them for communications that create contract meaning.[178] It is well-established that Grice's linguistic insights are applicable to a broad range of legal questions,[179] including not only

175. *See* RESTATEMENT, CONTRACTS, *supra* note 4, § 201 cmt. c. In fact, the article describing shared meaning analysis starts with a recognition of this fact and uses it to frame its approach. *See* Kar & Radin, *supra* note 4, at 1138.

176. Kar & Radin, *supra* note 4, at 1143.

177. *Id.* at 1150.

178. *See id.* at 1151–53. For conversations that aim at the maximally efficient exchange of information, Grice suggests that people rely on four specific conversational maxims, which he calls the Maxims of Quantity (Don't say too much or too little for the conversational purposes at hand), Quality (Try to make your contribution one that is true), Relation (Be relevant to the purposes of the conversation), and Manner (Be perspicuous). Paul Grice, *Logic and Conversation*, *in* 3 SYNTAX & SEMANTICS 41, 45–46 (Peter Cole & Jerry L. Morgan eds., 1975) [hereinafter Grice, *Logic and Conversation*]. For conversations that aim to produce an actual agreement with a common meaning of the parties, Kar and Radin suggest that courts and parties regularly presuppose the following four maxims:

> (1) "*The [Contractual] Maxim of Quantity* instructs parties to say neither too much nor too little given the shared purpose of the conversation and the practical interests and attention of the parties." Kar & Radin, *supra* note 4, at 1151.
>
> (2) "*The Contractual Maxim of Quality* instructs parties to offer or agree to commit themselves only to that which they are willing and able to do." *Id.* at 1152.
>
> (3) "*The Contractual Maxim of Relation* instructs parties to commit themselves to a contract (as opposed to a merely informal promise) only when they mean to make a formal legal commitment — that is, when they mean to confer legal standing on the other party to be able demand compliance, to grant that party the power to invoke the formal power of the state in cases of noncompliance, and to submit to rather than trying to remove any other background legal rules that distinguish contracts as legally enforceable obligations from mere informal promises." *Id.* at 1153.
>
> (4) "*The [Contractual] Maxim of Manner* instructs parties to make their contributions clear and perspicuous by avoiding obscurity of expression, ambiguity, undue length, and lack of coherence in orderly presentation." *Id.* at 1151.

179. For examples of citations to Grice's work in other legal areas, see, e.g., Janet E. Ainsworth, *In a Different Register: The Pragmatics of Powerlessness in Police Interrogation*, 103 YALE L.J. 259, 260–61, 268–70 (1993) (discussing police interrogations); Scott Brewer, *Exemplary Reasoning: Semantics, Pragmatics, and the Rational Force of Legal Argument by Analogy*, 109 HARV. L. REV. 923, 933 n.20, 990–93 (1996) (discussing use of analogy in legal argument); Tun-Jen Chiang & Lawrence B. Solum, *The Interpretation-Construction Distinction in Patent Law*, 123 YALE L.J. 530, 563–64 (2013) (discussing patent law); Richard Craswell, *Interpreting Deceptive Advertising*, 65 B.U. L. REV. 657, 716–19 (1985) (discussing

contract meaning[180] but also questions of constitutional and statutory interpretation.[181]

A key insight from *Pseudo-Contract* is that contract meaning, like meaning in many contexts, depends upon presuppositions of linguistic cooperation.[182] The article demonstrates how these presuppositions are critical for identifying contract meaning across diverse scenarios, such as distinguishing between offers and assertions,[183] separating conditions on promises from consideration,[184] interpreting *pari passu* clauses in sovereign bonds between sophisticated parties,[185] assessing the legal effect of boilerplate warranty waivers,[186] and Judge Cardozo's landmark ruling in *Wood v. Lucy*, *Lady Duff Gordon*,[187] which implied a contractual duty to use reasonable efforts in an exclusive licensing agreement despite no explicit clause.[188] They define the "shared meaning" of a contract as "the meaning parties produce and agree to during contract formation that is most consistent with the presupposition that both were using language cooperatively to form a contract."[189] They argue that "shared meaning is what courts have for centuries meant to

---

advertising law); B. Jessie Hill, *Putting Religious Symbolism in Context: A Linguistic Critique of the Endorsement Test*, 104 MICH. L. REV. 491, 505–06 (2005) (discussing Establishment Clause of the First Amendment); John Mikhail, *The Constitution and the Philosophy of Language: Entailment, Implicature, and Implied Powers*, 101 VA. L. REV. 1063, 1068–69 (2015) (discussing the Constitution); Geoffrey P. Miller, *Pragmatics and the Maxims of Interpretation*, 1990 WIS. L. REV. 1179, 1182–83, 1226–27 (1990) (discussing statutory interpretation); Henry E. Smith, *The Language of Property: Form, Context, and Audience*, 55 STAN. L. REV. 1105, 1106–08, 1131–33 (2003) (discussing property law); Ryan C. Williams, *The Ninth Amendment as a Rule of Construction*, 111 COLUM. L. REV. 498, 534–36, 544 (2011) (discussing Ninth Amendment).

180. *See, e.g.*, Jeffrey M. Lipshaw, *Lexical Opportunism and the Limits of Contract Theory*, 84 U. CIN. L. REV. 217, 242–43 (2016); Henry E. Smith, *Modularity in Contracts: Boilerplate and Information Flow*, 104 MICH. L. REV. 1175, 1175–76 (2006); Peter Meijes Tiersma, Comment, *The Language of Offer and Acceptance: Speech Acts and the Question of Intent*, 74 CAL. L. REV. 189, 206–12 (1986); *see also* Richard Craswell, *Do Trade Customs Exist?*, *in* THE JURISPRUDENTIAL FOUNDATIONS OF CORPORATE AND COMMERCIAL LAW 118, 130–38 (Jody S. Kraus & Steven D. Walt eds., 2000) (applying Grice's theory to Uniform Commercial Code trade custom law).

181. *See* sources cited *supra* note 179; *see also, e.g.*, ANDREI MARMOR, THE LANGUAGE OF LAW 20–21 (2014); Lawrence B. Solum, *Constitutional Texting*, 44 SAN DIEGO L. REV. 123, 149–50 (2007); Lawrence B. Solum, *Semantic Originalism* 1–2 (unpublished manuscript) (Nov. 22, 2008), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1120244 [https://perma.cc/R6M9-46E3]. For discussion of Grice's impact outside of law, *see* J.R. Searle, *Grice on Meaning: 50 Years Later*, 26 TEOREMA 9, 18 (2007) (Spain) (crediting Grice with "revolutioniz[ing] and deepen[ing] our conception of language" and producing one of the "two crucially important ideas that came out of the philosophy of language practiced in Oxford in the 1950's").

182. *See* Kar & Radin, *supra* note 4, at 1150.

183. *Id.* at 1157.

184. *Id.* at 1160.

185. *Id.* at 1184.

186. *Id.* at 1197.

187. 118 N.E. 214 (N.Y. 1917).

188. *See* Kar & Radin, *supra* note 4, at 1150 (citing *Wood*, 118 N.E. at 215).

189. *Id.* at 1143.

refer to by focusing contract interpretation on a search for the common meaning of the parties."[190]

The point of incorporating insights from the philosophy of language is not to supplant the intuitive linguistic judgments courts typically use to interpret contracts. Rather, it is to reveal how courts have increasingly lost their way in digital contexts, failing to discern accurately the common meaning of the parties in these settings.[191] One issue is that "[c]ontemporary boilerplate text is often so long that it would wildly violate the Maxim of Quantity if it were considered to add 'terms' to a 'contract.'"[192] Additionally, "[m]uch of it is . . . difficult enough to understand that it violates the Maxim of Manner — which says to speak clearly and perspicuously."[193] Yet, because digital methods of communication and contract formation superficially resemble traditional, cooperative offers followed by cooperative acceptances, courts have started to treat all the extensive pseudo-contractual text in online privacy policies as if it reflects a shared meaning of the parties.

To assist courts in navigating digital contexts and identifying the true common meaning of the parties in these settings, *Pseudo-Contract* proposes a two-step approach. First, "[w]hen approaching a legal dispute over a particular piece of boilerplate text, courts should . . . determine whether a contract was formed."[194] Second, courts should assess separately whether the disputed text was communicated in a sufficiently cooperative manner to produce a common meaning of the parties.[195] To engage the appropriate linguistic intuitions without requiring knowledge of Grice's technical maxims, *Pseudo-Contract* suggests that courts envision the digital interaction as part of a face-to-face conversation, and then pose the following question about the disputed boilerplate text:

> Could this boilerplate text have plausibly contributed to an oral conversation that contributes terms to a contract consistent with the presupposition that both

190. *Id.* at 1154; *see also id.* at 1143 (suggesting that this definition "captures the most important considerations that have guided courts and helped them to discern the common meaning of the parties for centuries, in both historical and contemporary circumstances"); *id.* at 1144 ("[S]hared meaning analysis applies generally to many varieties of contract, ranging from consumer clickwrap purchases to much larger transactions with high-end boilerplate text between sophisticated parties.").

191. *Id.* at 1168 ("The point of the conceptual test is to place linguistic understanding on firmer ground when the more complex ways that boilerplate text is often conveyed in the digital world make it less easy to understand than in an oral hypothetical. The conceptual test should be understood in that spirit of usefulness.").

192. *Id.* at 1155.

193. *Id.*

194. *Id.* at 1166.

195. *Id.* at 1166–67.

> parties were observing the cooperative norms that govern language use to form a contract?[196]

When boilerplate text passes this test, it falls within the boundaries of parties' actual agreement and contract, and "courts can rely on their ordinary linguistic intuitions to interpret the contract meaning of the text."[197] Text that fails this test, however, should be deemed mere "pseudo-contract," which does not contribute to any shared meaning and should not be enforced as contract.[198]

While shared meaning analysis is a novel proposal in the literature, in another sense, it merely serves as a practical heuristic to ensure courts apply traditional contract interpretation correctly in complex digital contexts. Shared meaning analysis offers advantages over many other proposals for handling problematic boilerplate because it is firmly rooted in traditional contract law principles and facts about how contract meaning can be produced.[199] Highlighting these benefits,[200] *Pseudo-Contract* argues that shared meaning analysis offers "a principled but flexible method of discerning the common meaning of the parties, which courts can integrate into their common law reasoning, thus creating a tool with sufficient scope, accuracy, power, and coherence to cure the paradigm slip into pseudo-contract."[201]

B. Applications to Three Common Problems in Online Privacy Policies

This Section applies shared meaning analysis to three prevalent issues in online privacy policies: (1) the proper scope of online contracts over data, (2) the validity of unilateral modification clauses, and (3) pervasive consumer deception arising from hidden conflicts between pseudo-contractual and actual contractual text. These examples are illustrative, not exhaustive. The goal is to demonstrate how courts can leverage shared meaning analysis to tackle a wide array of privacy-related challenges in a distinctive, effective, and case-specific way.

---

196. *Id.* at 1167.

197. *Id.*

198. *Id.*

199. *See, e.g.*, *id.* at 1172 ("Unlike prior proposals for dealing with the problems created by boilerplate text, shared meaning analysis flows from the core principles that justify contract enforcement by the state based on actual agreement with common meaning.").

200. *See, e.g.*, *id.* at 1168–72 (explaining the benefits of shared meaning analysis over other prominent proposals in the contract law literature, including reliance on defenses like unconscionability or public policy, Karl Llewellyn's proposal that contract formation includes blanket assent to all boilerplate text "not unreasonable or indecent," paternalistic regulations, and mandatory disclosure regimes).

201. *Id.* at 1172.

1. The New York Times Privacy Policy and Questions of Contractual Scope

Beginning with a key example, let us revisit the NYT's website. Figure 1 illustrates what users encounter when attempting to read a NYT article without logging in: they must either create or log into a personal account, providing an identifiable email address as a personal identifier, then click "Continue."

Beneath the "Continue" button, a statement reads, "By continuing, you agree to the Terms of Service and acknowledge our Privacy Policy." Though in smaller font than the surrounding text, hyperlinks to the Terms of Service ("ToS") and Privacy Policy are underscored, indicating their significance and that additional text can be obtained by clicking. Clicking a hyperlink directs users to new pages, displaying the full ToS or Privacy Policy. By clicking "Continue," users will be deemed to "accept" a "contract." However, because courts often overlook how parties establish a true common meaning in digital contexts, they frequently assume that all text in these lengthy hyperlinks adds binding "terms" to this "contract."[202]

Figure 1: What users see when they navigate to a New York Times article without having logged in.[203]

Shared meaning analysis advocates a more cautious approach. If all this text were imagined as contributing to a hypothetical oral

202. Pressing the "Continue" button will constitute not only consent to use the email address for login purposes but also an agreement with the NYT's ToS and Privacy Policy. The NYT uses these further online policies to seek an agreement for various data processing activities and uses through a single click. This is sometimes called bundling. *See* Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617, 637 (2021).

203. (June 2, 2022).

conversation, then — starting at the first stage of the analysis — the primary text in Figure 1 could have been communicated cooperatively enough to inform users they are entering a contract by clicking "Continue." Inputting an email address for login would represent a knowing and voluntary disclosure of that specific information for registration purposes. It is, however, a separate question how much of the additional text at these lengthy hyperlinks is communicated cooperatively enough to contribute to a common meaning of the parties. This question is pursued — separately — at the second stage of shared meaning analysis.

Unlike a home sale, where parties negotiate terms extensively before finalizing an agreement, here users simply aim to read an article. Yet the ToS spans nearly 8,700 words,[204] and the Privacy Policy nearly 11,000 words.[205] Few, if any, readers would be willing to engage in this much oral conversation just to access an article. Attempting to communicate such voluminous and complex content orally in this context would violate Grice's Maxim of Quantity[206] — say no more or less than needed for a conversation's purpose — and the Maxim of Manner,[207] which says to be clear. Shared meaning analysis thus indicates that this hyperlinked text does not create any shared meaning; it is merely pseudo-contract and should not be enforced as contract.

One might reasonably question the commercial feasibility of rejecting the contractual assimilation of all this text. However, a closer examination of the Privacy Policy — our primary focus here[208] — reveals that much of it serves no real contractual function anyway and need not be treated as contract. For example, 1,395 words simply restate legal rules, such as the rights of California residents under state law,[209] while another 340 words in Section 12 provide the company's contact information.[210] A significant portion describes primary uses of information in transactions where users knowingly disclose data for specific, well-understood purposes like registration, billing, user-

---

204. In this example, we refer to the NY Times Term of Service last updated May 10, 2024 (on file with authors) [hereinafter NY Times ToS].

205. In this example, we refer to the NY Times Privacy Policy dated July 1, 2024 (on file with authors) [hereinafter NYT Privacy Policy].

206. See *supra* note 178 for further discussion of these specific maxims and how they relate to cooperative uses of language to form contracts on a Gricean approach.

207. *Id.*

208. For extensive discussions that are focused instead on terms of service (as opposed to online privacy policies), see Kar & Radin, *supra* note 4, at 1173–213.

209. NYT Privacy Policy, *supra* note 205, at Section 4. (B).

210. A representative example from this portion of the policy says: "If you have any questions, email us at privacy@nytimes.com or write us at:

The New York Times Company
620 Eighth Avenue
New York, N.Y. 10018
Attn.: Privacy Counsel

We can also be reached by phone at 1-800-NYTIMES (see a list of our local telephone numbers outside the United States)." *Id.* at Section 12.

generated content, or service calls.[211] This text does not function as contract because it merely confirms what users already understand: that their voluntarily disclosed information will be used for those purposes. Other sections outline practices that NYT can undertake, in its discretion, without any contract[212] or reiterate background informational norms that apply regardless of contract.[213] Ultimately, for most of the extensive text in this Privacy Policy, there is no commercial or practical need for either the NYT or users to secure a "contractual agreement."

The *NYT* Privacy Policy exemplifies a broader, yet often overlooked, pattern in online documents of these kinds. In *Pseudo-Contract and Shared Meaning Analysis*, Kar and Radin note that many modern online "contracts," formed via clickwrap or browsewrap mechanisms, contain vast amounts of boilerplate text that, in fact, serve no contractual purposes and are rarely, if ever, treated or litigated as contract.[214] They term this "ride-along" text, as it accompanies briefer sections intended to serve contractual roles but is delivered at the point of contract formation in bundled forms that often obscure these brief sections.[215] Because of these facts, the widespread assumption that all this digital text must be treated as "contract" is "technologically naïve and outdated," failing to "recognize just how many noncontractual functions boilerplate text now serves"[216] in today's digital world.

Yet, nestled within the NYT's extensive Privacy Policy is a small but critical portion of text that, if treated as contract, poses substantial

---

211. *See, e.g.*, *id.* at Section 1. (A) i. ("When you sign up for a Times Service (whether via a subscription or a free account as a registered user), we collect personal identifiers such as your contact information, including your name and email address, and account credentials. We may also ask you to create an account name. Once you're registered, we assign you a unique ID number. This ID number helps us recognize you when you're signed in.").

212. *See, e.g.*, *id.* ("To process payments or donations, we collect and use your payment information. This can include your name, your address, your telephone number, your email address, your credit or debit card information and any other relevant information.").

213. *See, e.g.*, *id.* ("With your consent, we may record interviews with you and ask for your permission to use your voice and likeness for a variety of purposes including marketing, advertising and/or Times events.").

214. *See* Kar & Radin, *supra* note 4, at 1207–13. In the context of more general "Terms of Conditions," Kar and Radin note that "[t]he text that is typically disputed as contract is actually quite narrow," and that the "vast majority of these disputes involve forum selection clauses, arbitration clauses, exculpatory clauses, covenants not to compete, or the scope of end user licenses of intellectual property." *Id.* at 1165. Because this section of the current Article is focused instead on online privacy policies, here the most common examples of text that serves contractual purposes are different. As the main text shows, some of the most common examples relate instead to the collection, analysis, use, and sharing of information in ways that are not reasonably expectable based on background informational norms, which tend to be highly context specific. On the shape of those informational norms, see HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE 129–57 (2010) [hereinafter NISSENBAUM].

215. *See* Kar & Radin, *supra* note 4, at 1168.

216. *Id.* at 1214. For further examples, *see also id.* at 1207–13. This problem can, of course, also arise in non-digital contexts. But digital contracting allows for the relatively inexpensive "communication" of increasingly extensive sets of text in otherwise routine social settings.

privacy risks. The document says it effectively permits the NYT to surveil users' online activities, merge this data with external sources, employ sophisticated algorithms to uncover additional insights into users' preferences, usage patterns, and other characteristics, and potentially sell this data to third parties with diverse objectives. To highlight this fact, consider the following five excerpts, which would likely capture users' attention if not buried in nearly 11,000 words of ride-along text:

(1) "When you use Times Services, we *collect* some *information automatically*. The *technologies* we use to assist with this data *collection* include *cookies, web beacons, tags* and *scripts* and *software development kits* (or SDKs). We may also use *newer technologies*, such as *clean rooms*, *matching services* described below (such as *Unified ID 2.0* and *LiveRamp's Authenticated Traffic Solution*) and *Comscore's Unified Digital Measurement (UDM) 2.0*, as *many browsers* begin to *deprecate* third party *cookies*."[217]

(2) "We *collect information* about certain *internet* and *network activity* on Times Services, including your *interactions* with our *websites* and *apps*, such as the URLs of *any pages* you *visit* on our *sites* and *apps*, the URL of the *website from which you came* to our sites, *how long you spent* on a page, *access times*, *search queries*, and *other details* about your *use* of and *actions* on our Services."[218]

(3) "We *infer new information* from *other data* we *collect*, including using *automated means* such as *machine learning*, which may include *third party machine learning services* or *large language models*. These inferences include information about your *likely preferences* or *other characteristics* (e.g., article topics, writers, teams or markets of interest to you)."[219]

(4) "We *track* your *interests* and *reading habits* (*e.g.*, the articles you read) . . . using *technology* like *algorithmic recommendations* and *machine learning*, which may include *third party machine learning services* or *large language models*."[220]

(5) "There are situations when *we disclose* your *information* to *third parties* beyond our service providers."[221]

---

217. *See* NYT Privacy Policy, *supra* note 205, at Section 1. (A) iii. (emphases added).
218. *See id.*
219. *See id.* at Section 1. (B) (emphases added).
220. *See id.* at Section 2. (B) (emphases added).
221. *See id.* at Section 3. (C) (emphases added).

The most important difference between shared meaning analysis and current judicial approaches lies in this: most courts would treat (1)–(5) as creating binding contractual terms, whereas shared meaning analysis would not. Hence, courts employing shared meaning analysis would reject any contractual agreement permitting NYT to conduct extensive surveillance, build detailed behavioral profiles of users, or sell user data to third parties.

Even within this more privacy-protective framework, companies could, of course, still obtain genuine agreements to (1)–(5) or portions thereof. The onus would, however, fall on corporations to find clear and effective methods to isolate these proposed agreements and communicate them in sufficiently cooperative manners to create a shared meaning between parties in specific contexts. For example, the NYT might design a website with clickwrap options offering multiple paths to "continue." A hypothetical site that does this, as shown in Figure 2, might include a first option ("Continue to Full Privacy Protected Services"), which excludes (1)–(5), a second option ("Continue to Premium Personalized Services"), which allows only (1)–(4) for personalization without data selling, and a third option ("Continue to Personalized Services with Data Selling"), which encompasses (1)–(5). Given the varying costs and values of these options, the NYT might need to set subscription rates for each service.[222]

222. The NYT claims in its privacy policy that its subscription rates factor in the value of personal information collected. Specifically, the policy states:

> The value of any financial incentive we offer is reasonably related to the value of any personal information you provide to us. We estimate the value of your personal information by considering, without limitation, the expenses we incur from collecting your personal information and/or providing the financial incentive to you, the revenue generated by your use of the financial incentive, and any improvements we can make to our products and Times Services based on information obtained through the financial incentive program.

See NYT Privacy Policy, *supra* note 205, at Section 1. (A) i. But there is currently no way to choose among different options because no one reads the full privacy policies and there is no mechanism to clarify how different choices might have different values to consumers.

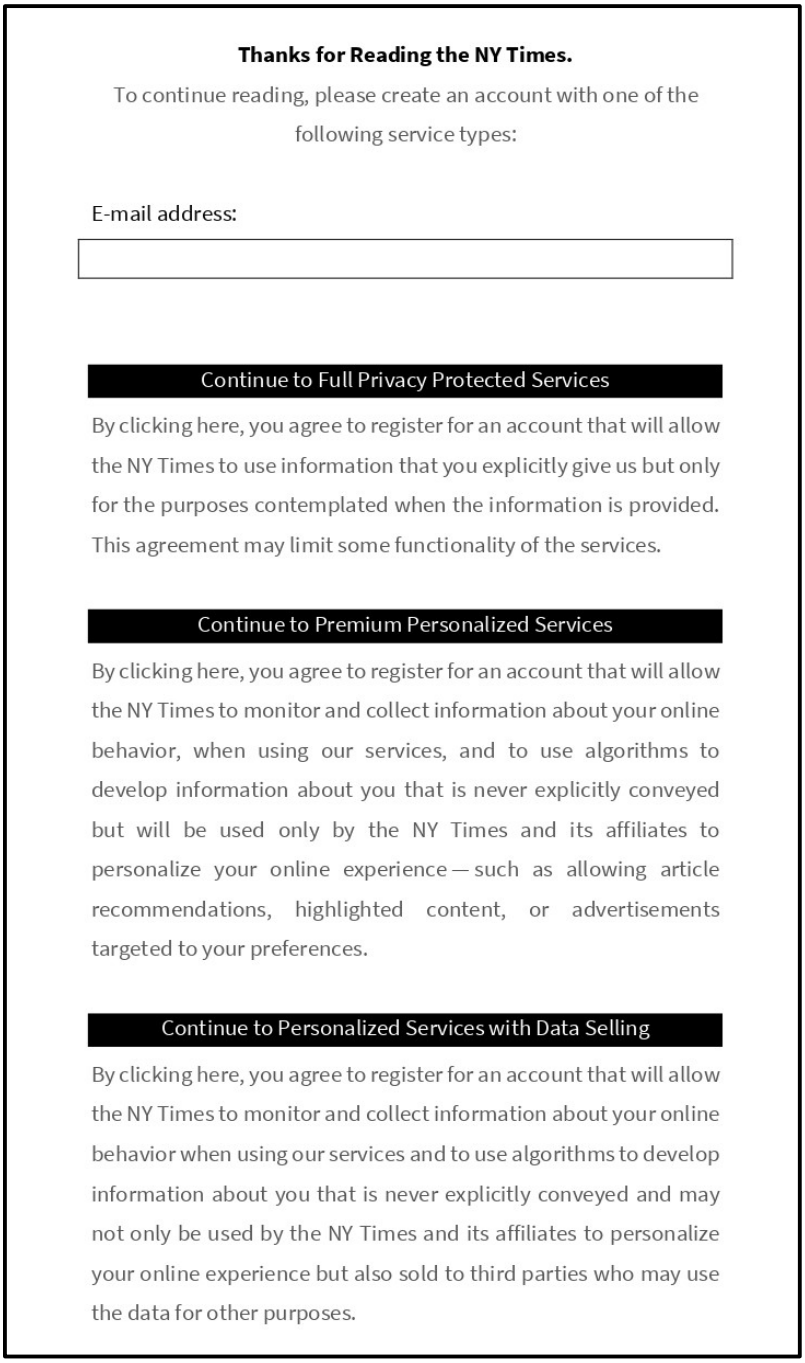

Figure 2: Hypothetical, Revised New York Times Website

Websites like this could, of course, also include hyperlinks to additional information, such as lengthy privacy policies, containing text that serves various non-contractual purposes. However, this linked text would not contribute "terms" to any contract and, if it conflicted with the more prominently presented terms, would be disregarded in any contract dispute as inconsistent with the parties' actual agreement.

By enabling courts to define the proper scope of contract more accurately in digital settings, shared meaning analysis would encourage corporations to isolate any genuine contractual proposals in their privacy policies and present them clearly and conspicuously. Given that many privacy rights are currently eroded by pseudo-contract rather than true contract, this legal regime would better align consumers' privacy behaviors with their privacy values — across countless daily situations, and as "by an invisible hand," in Adam Smith's evocative metaphor.

2. Unilateral Modification Clauses

Expanding on this example, we now address the troubling phenomenon of unilateral modification clauses. Thomas Haley notes that an "[a]nalysis of the 122 top websites reveals that every one includes in its platform terms a unilateral modification provision."[223] The NYT's Privacy Policy is no exception, containing the following statement within its nearly 11,000 words of mostly ride-along text: "[W]e must periodically update this Privacy Policy. We will post any changes on this page by updating this policy."[224]

By placing unilateral modification clauses in their online privacy policies, companies aims to secure contractual rights to unilaterally change the agreements reached over privacy and data usage agreements at will,[225] often without meaningfully informing users or obtaining their genuine consent.[226] When these clauses are enforced as contract, users must continually monitor extensive policy updates across numerous sites just to understand their current "agreements."[227] The challenges highlighted in the last section — where cooperative communication of extensive boilerplate text is infeasible at the initial point of contract — are amplified exponentially with frequent policy updates. Haley

223. *See* Haley, *supra* note 72, at 100.

224. *See* NYT Privacy Policy, *supra* note 205, at Section 11.

225. We say "in part" because there are also many legitimate reasons that corporations can have to change the non-contractual text in their online privacy policies — and, indeed, they must in some circumstances. We discuss those other cases below, *see infra* notes 237–41 and accompanying text.

226. Leah R. Fowler, Jim Hawkins & Jessica L. Roberts, *Uncertain Terms*, 97 NOTRE DAME L. REV. 1, 4–5 (2021) ("Under these provisions, companies can alter terms sometimes without even notifying users, let alone asking them for permission. And unilateral amendments are by and large legal. More often than not, courts are willing to enforce these one-sided changes.").

227. *See* Reidenberg, *supra* note 8, at 494.

underscores this fact: "If it would take hundreds of hours for the average American to read all the platform agreements to which they are party, how long would it take to monitor every such agreement and analyze the changes thereto when they occur? The task would become Sisyphean."[228] Moreover, enforcing unilateral modification clauses, provided in pseudo-contract, undermines the core principle that contracts embody commitments that should be modifiable only through a new, mutually agreed-upon contract, allowing corporations to unilaterally strip consumers of privacy rights that were never exchanged as part of any actual contract.[229]

Yet courts routinely enforce unilateral modification clauses, subject only to good faith and fair dealing constraints,[230] which restrict modifications that conflict with a "consumer's justified and reasonable expectations and the common purpose of the contract."[231] This reliance on good faith and fair dealing offers only limited protection, as it is a notoriously vague standard,[232] functioning more like a stopgap to prevent only the most glaring abuses. In truth, consumers entering a contract should be able to expect that its original terms will be upheld, not altered unilaterally, absent a new agreement with shared meaning.[233]

---

228. *See* Haley, *supra* note 72, at 103.

229. *See id.*

230. *See, e.g.*, Fagerstrom v. Amazon.com, Inc., 141 F. Supp. 3d 1051, 1066 (S.D. Cal. 2015) (citing RESTATEMENT OF THE LAW SECOND, CONTRACTS § 205, cmts. a and d (1981), and holding that a contract-modification clause was not illusory because the business was bound by the duty of good faith, and that, consequently, the seller "must exercise this discretion in a manner consistent with 'the spirit of the bargain' and [consumers'] justified expectations under the contract" (quoting Scribner v. Worldcom, Inc., 249 F.3d 902, 910 (9th Cir. 2001))); *see also* McKee v. Audible, Inc., No. 17–1941, 2017 WL 4685039, at *13 (C.D. Cal. July 17, 2017); Sevier Cnty. Schs. Fed. Credit Union v. Branch Banking & Tr. Co., 990 F.3d 470, 478 (6th Cir. 2021).

231. *See* RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 4, reporter's note b.

232. For a classic statement of this problem, see, e.g., Clayton P. Gillette, *Limitations on the Obligation of Good Faith*, 1981 DUKE L.J. 619, 619 (1981) ("Scholarship addressed to the good faith provisions of the Uniform Commercial Code primarily discusses the intractable difficulty of defining the scope of the obligation to perform and enforce one's contract in good faith."). Similar concerns have been raised by Robert S. Summers, *'Good Faith' in General Contract Law and the Sales Provisions of the Uniform Commercial Code*, 54 VA. L. REV. 195 (1968); Dugan, *Good Faith and the Enforceability of Standardized Terms*, 22 WM. & MARY L. REV. 1 (1980); Robert Hillman, *Policing Contract Modifications Under the U.C.C.: Good Faith and the Doctrine of Economic Duress*, 64 IOWA L. REV. 849 (1979).

233. Some scholars also suggest reliance on the doctrine of unconscionability to curtail the binding effect of boilerplate text when it is fundamentally unfair. *See, e.g.*, Brady Williams, *Unconscionability as a Sword: The Case for an Affirmative Cause of Action*, 107 CAL. L. REV. 2015 (2019); Colleen McCullough, *Unconscionability as a Coherent Legal Concept*, 164 U. PENN. L. REV. 779 (2016). However, the likelihood of the unconscionability doctrine being applied in this situation appears to be significantly low. The Restatement acknowledges that this doctrine is only invoked "when the one-sidedness of a term in the contract is extreme." *See* RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, §§ 4, 6(c). But courts regularly enforce unilateral modification clauses that are found in online contracts, which suggests that they do not generally consider them to "shock the conscience," "oppressive",

Corporations often attempt to sidestep violations of good faith and fair dealing by notifying users of changes. For example, the NYT Privacy Policy states:

> If we make a significant or material change in the way we collect, use or share your personal information, we will notify you at least 30 days prior to the changes taking effect. We will do this via email or prominent notice within Times Services. If you object to any change, you can stop using the Times Services.[234]

Because courts fail to distinguish contract from pseudo-contract, they frequently permit unilateral contract modifications of online privacy policies when such notice mechanisms are in place.[235] Yet there is a stark difference between frequently notifying users of changes in online documents that are far too extensive to read and cooperatively proposing and securing acceptance of a true contractual modification with shared meaning. That distinction is lost when courts conflate pseudo-contract with contract, allowing ineffective "notice" to yield enforceable "contract" modifications.

Shared meaning analysis would approach unilateral modification clauses differently. For reasons outlined previously, the brief text relating to the unilateral modification clause discussed here — hidden in almost 11,000 words of ride-along text and never cooperatively communicated to produce any shared meaning — would be pseudo-contract. It would, therefore, add no legally enforceable terms to any contracts, requiring NYT to obtain an actual agreement with shared meaning, cooperatively communicated and mutually agreed to, to expand its contractual rights over personal data.[236] This approach would foster a significantly more privacy-protective regime.

"unreasonably harsh," or "fundamentally unfair," *id.* at cmt. 3, especially when they offer notifications for material changes and provides an avenue for users to reject any modifications. The unconscionability doctrine might be used to police some of the most egregious problems in this setting, much as use of the duty of good faith and fair dealing — but the two doctrines also have similar limitations.

234. NYT Privacy Policy*, supra* note 205, at Section 11.

235. *See* RESTATEMENT, CONSUMER CONTRACTS, *supra* note 3, § 3(a) ("A business's proposed modification of a standard contract term in a consumer contract governing an ongoing relationship is adopted if the business demonstrates that: (1) the consumer received reasonable notice of the proposed modified term and a reasonable opportunity to review it.").

236. Though contract formation typically requires both mutual assent and consideration in the first instance, *see* RESTATEMENT, CONTRACTS, *supra* note 4, § 17, modifications of contracts, which adjust ongoing contractual relations, are sometimes permitted without new consideration, if, for example, "the modification is fair and equitable in view of circumstances not anticipated by the parties when the contract was made." *Id.* § 89 cmt. a ("This Section relates primarily to adjustments in on-going transactions."). But the fact that new consideration is not always needed should not change the fact that new mutual assent is needed before new rights are stripped from consumers.

Once again, one might question the commercial feasibility of this approach, considering corporations' legitimate need to update online privacy policies without constant renegotiation. But such concerns are largely unfounded, as very little text in these policies is even contractual. The NYT should, for example, be free to update its contact address if it relocates its headquarters,[237] or revise its detailed restatements of California privacy law if the law changes.[238] Similar points apply to other classes of ride-along text common in online privacy policies, such as service descriptions, usage instructions, or answers to frequently asked questions.[239] Because no one treats ride-along text as contractual anyway — i.e., not users, companies, or courts employing shared meaning analysis — the NYT would not need a new contractual agreement, on the present approach, before revising most of its privacy policy.[240]

Where shared meaning analysis would create major differences in practice would, instead, be in relation to any *actual* contracts over data — that is, any distinct mutual understandings formed through the cooperative use of language. To illustrate, consider the three offers in Figure 2, which depict how the NYT might operate under our proposed legal framework. The website in Figure 2 cooperatively presents three distinct offers with varying terms: (1) "Full Privacy Protected Services," (2) "Premium Personalized Services," and (3) "Personalized Services with Data Selling." If the NYT secures a clickwrap for one option (e.g., "Full Privacy Protected Services"),[241] then it could not unilaterally change the terms to another option (e.g., "Personalized Services with Data Selling").[242] The NYT could not do this even if it were to provide notice of the attempted change, and this conclusion would not depend on any assessments of good faith, fair dealing, or unconscionability. By tackling the pervasive problems that arise from pseudo-contractual unilateral modification clauses, shared meaning analysis would significantly enhanced privacy protections across numerous digital contexts, with cumulative effects that go far beyond this single example.

---

237. *See* NYT Privacy Policy, *supra* note 205, at Section 12 (setting forth contact information).

238. For the sections on California law, *see id.* at Section 4. (B).

239. *See id.* at Section 10. (describing what the third-party services are and how users can contact them).

240. There may, of course, still be many good legal and commercial reasons to provide users with regular notices of any such revisions.

241. *See supra* Figure 2 (text of offer for Full Privacy Protected Services).

242. *See supra* Figure 2 (text of offer for Personalized Services with Data Selling).

3. Hidden Conflicts and Deception

We now examine another pervasive issue stemming from the paradigm slip in contract law. In a legal regime that conflates pseudo-contract with contract, markets incentivize companies to embed "terms" detrimental to consumers' privacy rights within extensive online privacy policies — rarely read or understood — while prominently displaying consumer-friendly terms through clear, cooperative communication.[243] When both types of text are deemed "contract," it becomes challenging to detect pervasive deception arising from conflicts between contract and pseudo-contract.[244] This Section demonstrates how this issue manifests in online privacy policies and how shared meaning analysis can effectively resolve it.

To demonstrate, examine Figure 3, which displays the digital communications that Burger King employs when customers visit its website to order food, beverages, or other items. As depicted in Figure 3, visitors to the Burger King website are first greeted with product images, followed by a pop-up banner stating, "By clicking 'Accept All Cookies', you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. Privacy Policy." Clicking the hyperlinked "Privacy Policy" redirects users to a separate webpage with a lengthy privacy policy, yet few consumers ever click on that link. Instead, their attention is drawn to the much larger "Accept All Cookies" button at the bottom right, while a smaller, barely noticeable, "Decline" button is also present.

243. *See* Kar & Radin, *supra* note 4, at 1214 ("[T]he legal regime of pseudo-contract is incentivizing new and expanding forms of mass-market deception, especially in many consumer markets, and an inexorable race to the bottom for pseudo-contractual 'terms' of poor quality.").

244. *Id.* at 1140 ("The fake 'terms' in a regime of pseudo-contract invite burgeoning forms of deception that are difficult for courts to discern because they are hidden under the mantle of 'contract.'").

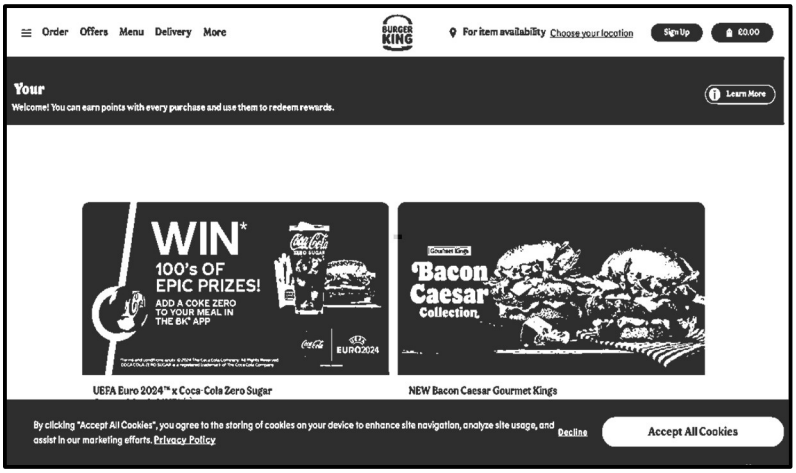

Figure 3: Burger King homepage.[245]

By embedding a link to the Privacy Policy in this banner, Burger King effectively and strategically attempts to incorporate the entire lengthy text of its Privacy Policy into this digital offer. Under current approaches to contract law, a user clicking "Accept All Cookies" would be construed as "agreeing" to all the extensive pseudo-contract "terms" in this linked Privacy Policy, which spans approximately 4,000 words.[246]

Shared meaning analysis would propose a different approach. Consistent with prior examples, at the first stage, it would recognize that an agreement has been formed based on the website's visible interface: the banner presents clear terms that could feasibly be part of a hypothetical oral conversation for this transaction, alongside a straightforward method of acceptance. Yet, at the second stage a distinct question arises: could the additional 4,000 words in the online Privacy Policy have been orally communicated in a cooperative manner to create a shared meaning? It could not, as few would engage in such extended dialogue simply to order food at a fast-food restaurant. Thus, only the brief text on the website in Figure 3 would create actual contract terms, while the remaining 4,000 words in the Privacy Policy would be deemed pseudo-contract.[247] The resulting contract would permit only

245. *Burger King Homepage* (Dec. 8, 2023) (on file with authors).

246. *See Privacy & Cookies Policy*, https://burgerking.co.uk/privacy-policy [https://perma.cc/97FG-C8T9] [hereinafter *Burger King's Privacy Policy*].

247. Trying to communicate this lengthier policy would violate both the Contractual Maxim of Quantity (which says to say neither too much or too little for the conversational purposes at hand) and the Contractual Maxim of Manner (which says to be clear). *See supra* note 178. It would have contributed nothing to the common meaning of the parties.

"the storing of cookies on [the user's] device to enhance site navigation, analyze site usage, and assist in our marketing efforts."[248]

This example initially resembles the previous one, but we now explore how hidden conflicts between the pseudo-contract and contract can lead to consumer deception that courts struggle to detect when they fail to differentiate the two. A closer examination of the Privacy Policy reveals that it says, in pseudo-contract: "We use cookies *and/or other similar technologies* such as device-IDs or in-App codes to collect and store certain information."[249] A further provision says: "*In addition to our use of cookies* detailed above, we may also use *other common tracking technologies* to collect your personal information. We use the Global site tag, Google Analytics and Google Tag Manager."[250]

This pseudo-contractual text thus claims to permit more extensive data collection practices than most users would reasonably expect from "accepting all cookies." Moreover, the Burger King Privacy Policy extends beyond cookies and these tracking technologies; while it contains a subsection entitled "Cookies and Other Technologies," the policy's scope is wider, detailing, like the NYT policy, the automatic collection of various usage data[251] and potential sharing with third parties.[252] It is inherently deceptive to take, by pseudo-contract that is rarely read or understood, rights that users would not anticipate surrendering based on the cooperative language exchanged when forming contracts. Yet, in a legal regime that equates pseudo-contract with contract, courts routinely view these rights as exchanged by "contract," not lost through deception.

Similarly, clicking the "Decline" button — if users can even see it — does not actually opt users out of all cookies under the current legal framework. The Privacy Policy's pseudo-contractual text indicates that such rejection only disables "non-essential" cookies while maintaining so-called "necessary cookies."[253] To completely disable all

---

248. *See supra* Figure 3.

249. *See Burger King's Privacy Policy*, *supra* note 246 (emphasis added).

250. *Id.* (emphases added).

251. *Id.* (describing that a variety of information, including technical, location, and other information will be "automatically collect[ed] . . . from you each time you visit our Services.").

252. *Id.* ("We are working closely with third parties (including, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, and search information providers)."). Although the Policy does not explicitly say that Burger King shares or sells personal data to third parties, it implies it.

253. Burger King does not explicitly mention the implications of clicking the "Decline" button. However, by examining the description of cookie usage on their website, it is clear that Burger King does not mean to exclude what they call "strictly necessary" cookies if a consumer hits "Decline" because those are thought of as a separate class of cookies that are "required" for the proper functioning of their website. *See id.* ("Strictly necessary cookies. These are cookies that are required for the operation of our website and under our terms with you. They include, for example, cookies that enable you to log into secure areas of our website, use a shopping cart or make use of e-billing services.").

cookies, per the Privacy Policy's "terms," users must manually adjust their browser settings, potentially leading to diminished site navigation experience.[254] More troubling, the "Decline" button does not halt tracking via non-cookie methods or third-party services;[255] for example, opting out of Google Analytics — a service tracking website traffic — requires users to act directly on Google's platform.[256]

Through its hyperlinked Privacy Policy, Burger King creates a profound divide between users' expectations and legal realities. The buttons' labels — "Accept All Cookies" or "Decline" — are at odds with pseudo-contractual text that courts currently rely on to interpret the legal implications of these actions in contract formation. Selecting either option produces outcomes that diverge from any reasonable user's understanding: clicking "Accept All Cookies" permits tracking technologies extending far beyond cookies, while clicking "Decline" fails to terminate even all cookie-based surveillance.

This example exhibits all the hallmarks of deceptive practices prevalent in digital contracting. Burger King employs hidden boilerplate text to secure a broad contractual "agreement" for surveillance and data sharing, which contradicts the typical intent behind clicking "Accept All Cookies" — or, in some cases, even "Decline" — to obtain rights that are inconsistent with users' expectations. Such deception is obscured and rarely treated as such when courts, conflating pseudo-contract with contract, fail to see these hidden conflicts as deception.

Unfortunately, this form of deception is all too common. In a legal regime that equates pseudo-contract with contract, companies that refrain from such deceptive practices face competitive disadvantages, forced either to raise prices — to offset the revenue lost from forgoing surveillance and data sharing that competitors regularly exploit — or suffer reduced profit margins. Shared meaning analysis would empower courts and the FTC to detect these pervasive forms of consumer deception across numerous digital contexts, yielding significant benefits for privacy and data protection.

---

254. *Id.* ("The effect of disabling cookies depends on which cookies you disable but, in general, the website may not operate properly if all cookies are switched off. If you want to disable cookies on our website, you need to change your website browser settings to reject cookies.").

255. In its Terms & Conditions ("T&C"), Burger King states that "[t]he Terms are a binding legal contract between you and BKUK . . . . Your use of the Services means that you agree to be bound by the Terms. Do not use the Services if you do not accept the Terms." *Terms of Use*, https://www.burgerking.co.uk/terms-of-use [https://perma.cc/7XLF-2AMB]. With respect to privacy, the T&C asserts, "[b]y using the Services, you acknowledge that you have reviewed and understand our Privacy Policy." *Id.* This suggests that even if customers click the "Decline" button, as long as they continue to use the website, their actions signify consent to the Privacy Policy. In other words, they agree to both the use of cookies and other non-cookie technologies.

256. *Burger King's Privacy Policy*, *supra* note 246 ("To opt-out of Google Analytics tracking, go to http://tools.google.com/dlpage/gaoptout.").

C. Locating Shared Meaning Analysis within a Larger Suite of Proposals

The foregoing examples demonstrate how shared meaning analysis can be applied to online privacy policies to tackle a wide range of modern privacy risks. The proposal is distinctive because it operates *within* the common law of contracts — unlike other existing approaches — to address pervasive distortions in data markets caused by the paradigm slip in contract law. It does so by advocating a return to traditional principles of contract interpretation, guided by a deeper understanding of how language can produce shared meaning. This common law focus lends the proposal unique power and effectiveness, though we claim no monopoly on methods needed to address modern privacy threats.

Shared meaning analysis would likely work most effectively when paired with a broader set of established proposals in the literature. The approach can sometimes enhance, support, or provide more effective and distinct methods to achieve the objectives of several well-known proposals. While detailed exploration of the other proposals exceeds this Article's scope, positioning our approach alongside these familiar theories will highlight their complementary relationships.

Contextual Integrity. Helen Nissenbaum's theory of "contextual integrity" is among the most influential contemporary frameworks for privacy and data protection. She argues that privacy rights depend, by default, on "context-relative informational norms" — background norms "specifically concerned with the flow of personal information," including "transmission, communication, transfer, distribution, and dissemination . . . from one party to another, or others."[257] Privacy rights are upheld when these norms are honored and violated when they are breached.[258] These norms emerge from a diverse array of non-contractual sources and contexts,[259] though Nissenbaum acknowledges that information rights can also be transferred, including by contract.[260]

Viewed from this standpoint, a key problem with a legal regime of pseudo-contract is that corporations can secure pseudo-contractual rights that override these background informational norms without

257. *See* NISSENBAUM, *supra* note 214, at 104.

258. *See id.*

259. *See id.* at 132–37.

260. Barocas and Nissenbaum agree with O'Neil and Manson that consent is a "selective waiver" of rights and obligations. *See* Barocas & Nissenbaum, *supra* note 18, at 65. This waiver is not requested only under two conditions, "either concerning actions for which individuals are presumed to have reasons to waive rights and obligations, or concerning actions that promise significant benefits to others and to society at large." *Id.* at 65–66. And a well-functioning and non-distorted contract law should contribute to the fulfillment of the first condition. This is, of course, just to recognize that as Alan Westin has famously put the point, the right to privacy includes a right for people "to determine for themselves when, how, and to what extent information about them is communicated to others." WESTIN, *supra* note 1, at Part 1.

obtaining the fully informed consent morally required for such transfers. Shared meaning analysis tackles this issue broadly, while remaining highly sensitive to the specific circumstances of language use, thereby significantly safeguarding contextual integrity. In numerous scenarios, these informational norms would be more effectively preserved, except when corporations secure actual agreements with shared meaning that reflect alternative mutual understandings. Thus, shared meaning analysis aligns with many of Nissenbaum's objectives,[261] particularly in a context where she justifiably expresses skepticism about the efficacy of current legal and regulatory mechanisms to protect contextual integrity.[262]

Regulatory Techniques. Expanding on the last point, shared meaning analysis can also advance goals that some have pursued through regulations, which are often ill-suited for the task. First, substantive privacy regulations that block individuals from voluntarily disclosing personal information should generally be avoided due to the fundamental moral right to share such information.[263] Consequently, many comprehensive privacy regulations emphasize rules to enhanced informed

261. For example, Barocas and Nissenbaum cite with approval the idea that "consent is not required for acceptable, expected behaviors, but only for those that depart from it. The burden on notice, therefore, is to describe clearly the violations of norms, standards, and expectations for which a waiver is being asked and not to describe everything that will be done and not done in the course of treatment or research, which both the researcher and the subjects can safely presume." *See* Barocas & Nissenbaum, *supra* note 18, at 65.

262. *See id.* at 58 ("We accept that informed consent is a useful privacy measure in certain circumstances and against certain threats and that existing mechanisms can and should be improved, but, against the challenges of big data, consent, by itself, has little traction.").

263. Of course, this point should not be overstated, as there may be some circumstances in which paternalistic limits on contracting may be warranted — because some things should be market-inalienable, because of limitations on capacity, or for other reasons. For discussion, see, e.g., Anita Allen, *The Duty to Protect Your Own Privacy*, *in* PRIVACY, SECURITY, AND ACCOUNTABILITY 19 (Adam D. Moore ed, 2015) (arguing that an ethical duty to protect one's privacy imposes some moral limits on disclosing personal information to preserve dignity and autonomy); ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011) (same). There are also some clearly paternalistic and largely uncontroversial privacy regulations, such as the Children's Online Privacy Protection Act, which currently restricts children under 13 from engaging in online activities that involve data collection unless parents' consent is given. *See* 15 U.S.C. § 6502(a). Where there are justifications to limit peoples' abilities to freely disclose personal information, there is, however, nothing in the current proposal to refrain from doing so. The current theory is nevertheless focused on the much more common cases where personal information can, as a moral matter, be freely disclosed by contract, even if not by pseudo-contract.

consent,[264] such as mandatory disclosure regimes[265] or mandatory opt-out provisions.[266] Yet, substantial evidence indicates that mandatory disclosure regimes rarely foster genuine understanding across diverse contexts,[267] and, worse, they can harm consumers by enabling corporations to avoid liability for unfair or deceptive practices through compliance with largely ineffective disclosure rules.[268]

Shared meaning analysis can fulfill many objectives of these procedural regulations in the context of data contracts, while avoiding these pitfalls and the need for new domestic legislation. Extensive research highlights ways corporations can foster more mutual understanding through digital communications,[269] yet market incentives in a legal regime of pseudo-contract often favor deception or ineffective communication. By distinguishing pseudo-contract from contract and only enforcing the latter, courts could shift these incentives, encouraging corporations to pursue such research to achieve genuine shared understandings around data usage. This legal framework would better align privacy behaviors with privacy values, a process that would adapt naturally to evolving digital practices — a strength, not a flaw, of this common law proposal. Regulatory change is, unfortunately, often too slow to keep pace with this evolution, allowing corporations to exploit

---

264. One of the most common proposals is to point to the General Data Protection Regulation (GDPR) of the European Union (EU), *see, e.g.*, *Guidelines on Transparency under Regulation 2016/6/679 of the Article 29 Data Protection Working Party*, at 9 (Apr. 11, 2018), as a benchmark for the high standard of consent that many privacy scholars believe should be required before privacy rights are waived or transferred by consumers. The GDPR model mandates, for example, that valid consent must be "freely given, specific, informed and unambiguous." Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1).

265. *See*, *e.g.*, the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552; the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6803(a)(1)–(2). For arguments favoring mandatory disclosure regimes, see, e.g., M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012) (proposing revitalizing notice through design-based solutions and mandatory disclosure regimes that account for human cognitive biases and decision-making limitations).

266. For example, the California Consumer Privacy Act empowers California residents with the right to opt-out of sale or sharing personal information. CAL. CIV. CODE § 1798.120 (West 2022).

267. For a comprehensive discussion, see BEN-SHAHAR & SCHNEIDER, *supra* note 40; *see also* Matthew A. Edwards*, Empirical and Behavioral Critiques of Mandatory Disclosure: Socio-Economics and the Quest for Truth in Lending*, 14 CORNELL J.L. & PUB. POL'Y 199 (2005) (discussing lending); Geoffrey A. Manne, *The Hydraulic Theory of Disclosure Regulation and Other Costs of Disclosure*, 58 ALA. L. REV. 473 (2007) (discussing securities); Lauren E. Willis, *Decisionmaking and the Limits of Disclosure: The Problem of Predatory Lending: Price*, 65 MD. L. REV. 707 (2006) (discussing lending).

268. For important discussion, see *id.*

269. *See, e.g.*, Calo, *supra* note 265, at 1033 (arguing that mandated notice could be delivered in new forms based upon design psychology); Waldman, *supra* note 101, at 121.

rapidly shifting methods to evade the "purview of current privacy protections."[270]

Furthermore, in the United States, complex First Amendment considerations significantly restrict states' ability to regulate the analysis, disclosure, and sale of certain information.[271] But no such First Amendment issues arise for a common law approach that merely seeks to interpret correctly the actual agreements parties have reached for their personal data. Thus, shared meaning analysis can accomplish some important regulatory objectives while avoiding constitutional challenges.

FTC Actions. Privacy harms, "often small and dispersed,"[272] are frequently unrecognized by individuals,[273] even when they collectively cause significant societal damage.[274] These facts provide compelling reasons not to rely solely on private lawsuits — such as those asserting breach of contract or otherwise involving contract interpretation — to address all the issues in this Article. In the U.S privacy context, the FTC's critical role is widely acknowledged, with Chris Jay Hoofnagle describing FTC actions as "among the best alternatives for regulation of privacy,"[275] particularly vital in circumstances of rapid technological and economic change.[276] Similarly, Kate Crawford and Jason Schultz urge the FTC to investigate complaints against private entities to uncover potential privacy harms that courts and individuals might overlook.[277] Danielle Citron and Frank Pasquale advocate for stronger FTC oversight, especially in cases where data is used to "score" individuals for various purposes.[278]

While shared meaning analysis is a common law approach to contract interpretation, seemingly focused on private law actions, its use could significantly enhance the FTC's ability to protect privacy values as well. The paradigm slip in contract law has impacted FTC actions, as the FTC often relies on prevailing approaches to contract formation and interpretation when seeking to enforce privacy-related promises. By adopting shared meaning analysis and distinguishing pseudo-contract from contract, the FTC could significantly strengthen its enforcement capabilities for privacy protection. As previously discussed, the

---

270. Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 94 (2014).

271. *See*, *e.g.*, Balkin, *supra* note 11, at 1194 (noting that the First Amendment can create special problems for attempts to regulate the "analysis, disclosure, and sale of data that is lawfully within one's possession").

272. Solove, *Privacy Self-Management*, *supra* note 18, at 1891.

273. *See id.*

274. *See generally* Citron & Solove, *supra* note 58 (discussing privacy harms).

275. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY xv (2016).

276. *Id.*

277. *See* Crawford & Schultz, *supra* note 270, at 127.

278. *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 20–27 (2014).

FTC would also be able to identify and respond better to certain unfair and deceptive practices that frequently arise in data contracts over but are challenging to detect when pseudo-contract is assimilated to "contract."[279] Shared meaning analysis could also prove effective in many settings even if the FTC is significantly defunded.

Self-Help Techniques. Currently, nearly 90% of Americans use various privacy self-help techniques,[280] such as covering computer cameras, using encrypted messaging apps, deleting sensitive documents, adjusting browser settings, or providing false information to marketing inquiries.[281] These techniques undoubtedly play a vital role in safeguarding privacy in many contexts. However, they offer only de facto protection rather de jure (i.e., as a legal right) and cannot address all the issues stemming from the paradigm slip in contract law. Shared meaning analysis could reduce the need for some self-help measures, while reasserting legal oversight over data markets.[282]

Fiduciary Theories. Recent scholarship suggests that some privacy rights should stem from fiduciary duties, introducing the concept of "information fiduciaries" to describe entities with duties over information arising from special relationships of trust, loyalty, or care.[283] Jack Balkin, for example, emphasizes that trust and confidence are essential for the collection, analysis, use, and sharing of certain information,[284] arguing that online service providers like Facebook and Uber, which routinely collect, use, and share personal data, should be classified as information fiduciaries with obligations to protect their customers' data.[285] Likewise, Neil Richards and Woodrow Hartzog propose that privacy law should integrate fiduciary duties, such as "loyal collection" (i.e., companies should collect only the minimal data necessary for specific purposes), "loyal personalization," and "loyal

279. For further discussion, see *supra* Section III.A.

280. *The State of Privacy in Post-Snowden America*, PEW RSCH. CTR. (Sept. 21, 2016), https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/U6ZJ-NDGA].

281. *See* Steven H. Hazel, *Privacy Self-Help*, 36 BERKELEY TECH. L.J. 305, 313 (2021).

282. We use the term "state of nature" intentionally to refer to some forms of pseudo-contractual exchanges that are not, in our view, expressions of true, unregulated freedom of contract. Part of the problem with the paradigm slip is that many have lost their grip on what words like "freedom of contract" even mean.

283. *See* Balkin, *supra* note 11, at 1205. Balkin explains: "The idea of fiduciary duties gives us a way out of the neo-Lochnerian model that binds First Amendment freedoms to contractual freedom. It also offers us a way of explaining why certain kinds of information are *matters of private concern* that governments can protect through reasonable regulation. My central point is that certain kinds of information constitute matters of private concern not because of their *content*, but because of the *social relationships* that produce them." *Id.*

284. *See id.* at 1208.

285. *See id.* at 1209, 1221.

service" (i.e., companies should refrain from data practices that unfairly discriminate against customers).[286]

When fiduciary relations exist, they may impose critical, information-related duties independent of contract, though such duties can sometimes be modified or waived by contract. Shared meaning analysis would safeguard these fiduciary norms by preventing their alteration or erosion through pseudo-contract. Moreover, while cooperative linguistic norms apply to create shared meanings even between arms'-length parties,[287] there are special reasons to require fiduciaries to use language cooperatively when contracting. Thus, even if courts hesitate to apply shared meaning analysis in some contexts, they should have few concerns when interpreting contracts with fiduciaries.

Privacy Harms. Finally, we believe Danielle Citron's and Daniel Solove's influential work on privacy harms underscores the significance of our proposal.[288] They note that harm is often a required element of legal causes of action or a prerequisite for remedies,[289] a requirement that can hinder the law's ability to address modern privacy challenges, as many individual privacy harms are minor or intangible — such as anxiety, inconvenience, or frustration — and inconsistently recognized by courts.[290] Though small individually, these harms, when aggregated across millions, cause significant societal damage, often eluding traditional judicial frameworks that prioritize immediate, tangible, and individualized injuries.[291]

Citron and Solove note that "[c]rabbed conceptions of harm have led courts to dismiss cases that are a key lynchpin for privacy law enforcement."[292] To bridge this gap, they propose a typology of privacy harms they argue should be legally recognized,[293] encompassing both tangible harms (physical and economic) and intangible harms (reputational, discriminatory, relational, psychological, and autonomy-related).[294]

Whether or not these broader harms are recognized as "harm" under existing legal frameworks, we believe this work illuminates the full scope and impact of individual and social harms caused by the ongoing failure to address the paradigm slip in contract law. We therefore see this work as underscoring the urgent need to return contract law to its

---

286. Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 1025–27 (2022).

287. *See, e.g.*, Kar & Radin, *supra* note 4, at 1144–66 (showing how contract meaning depends, quite generally, on norms of linguistic cooperation).

288. *See* Citron & Solove, *supra* note 58.

289. *See id.* at 796.

290. *Id.* at 796-97, 799 n.27.

291. *Id.* at 797.

292. *Id.* at 862.

293. *See id.* at 830.

294. *See id.* at 831.

more traditional shape, particularly in a digital landscape where other legal proposals have fallen short on their own.

D. Pulling the Threads Together

Let us now revisit the vignettes from the article's outset and pull together various strands to paint a fuller picture. In 2024, when Amadea accessed the NYT website to read an article, she was engaging in a daily activity akin to Nico's in 1984. Due to changes in modality, however, Amadea — unlike Nico — had to click "I agree" to an online privacy policy to proceed. We have now uncovered many troubling details within that NYT Privacy Policy. Amadea may have clicked without reading, partly out of habit or convenience, because she wouldn't understand its lengthy terms anyway. She may have viewed reading this Article as a minor act, unlikely to reveal much about her.

Yet this was just one of many daily activities that she — unlike Nico — engaged in while using digital services, each one of which required an additional "contractual" click. Amadea's experience ordering at Burger King, for example, diverged from Nico's: Amadea was subjected to an online privacy policy there too, which overrode background context-relative informational norms, potentially undermining aspects of fiduciary duties or applicable privacy statutes. While surveillance of Amadea's activities by any single entity — like the NYT or Burger King — might seem minor, her data was aggregated with information from other companies, like CVS, Amazon, and the social media platforms described in these vignettes, enabling a far more comprehensive surveillance of her daily actions and choices. These processes led to the creation of detailed profiles of her activities, preferences, and traits, which were sold on secondary markets to unknown parties, exposing her — unlike Nico — to powerful new forms of consumer and political manipulation.

The cumulative effect of these pseudo-contractual privacy invasions was thus profound, even though Amadea, operating from the perceived "privacy" of her home, probably felt much safer, and much more free, than Nico did in 1984. We believe shared meaning analysis is essential to addressing the full scope of these challenges driven by major technological, legal, and social shifts, which now expose countless aspects of daily life to extensive forms of digital surveillance. As this Section highlights, integrating shared meaning analysis with the broader proposals discussed in this Section would amplify both its effectiveness and theirs.

V. CONCLUSION

We conclude by highlighting a well-known puzzle in contemporary privacy law. Ari Ezra Waldman notes that "[p]rivacy law . . . has never seemed stronger,"[295] yet he cautions that "our privacy seems more in danger now than ever, with frequent admissions of nefarious data use practices from social media, mobile apps, and e-commerce websites, among others."[296]

We contend that this troubling state stems, in part, from privacy scholars' limited engagement with the contract law dynamics driving the paradigm slip into a legal regime of pseudo-contract. If data markets are indeed to become "the solution," rather than "the problem," as Omri Ben-Shahar and Lior Strahilevitz assert,[297] courts must address core distortions in data markets by adopting shared meaning analysis. This approach would restore the rightful moral relationship between contract and privacy, seamlessly applying across countless digital transactions, as if "by an invisible hand." Without this return to traditional contract, however, we will remain in the current status quo, with privacy laws incapable of restoring this rightful moral relationship on their own.

When historians look back at the last few decades, they will surely recognize a profound turning point in social and economic relations, driven by heightened commercial surveillance enabled partly by pseudo-contract. This data, prized by third parties for its ability to uncover powerful new levers of consumer and political manipulation, is increasingly sold to entities with self-interested, sometimes nefarious motives. This shift is so drastic that scholars like Shoshanna Zuboff argue we have entered a new era of "surveillance capitalism,"[298] a transformation in social and economic relations as momentous as the 19th century Industrial Revolution.[299] Zuboff insists that "only law can . . . challenge"[300] the problems inherent in this new order, even while acknowledging that current privacy laws "will not be enough to interrupt surveillance capitalism."[301] Unfortunately, her own work is "surprisingly light on remedial prescriptions."[302]

In this Article, we have sought to address this critical gap in Zuboff's work along with the broader limitations of privacy scholarship

295. Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 775 (2020).

296. *Id.* at 774–75.

297. *See* Ben-Shahar & Strahilevitz, *supra* note 98, at S2–S3.

298. *See generally* ZUBOFF, *supra* note 12.

299. *Id.* at 29–37.

300. *Id.* at 483.

301. *Id.* at 486.

302. Mariano-Florentino Cuéllar & Aziz Z. Huq, *The Age of Surveillance Capitalism*, 133 HARV. L. REV. 1280, 1294 (2020) ("After such terror, some guidance on how to respond might be nice. But Zuboff's prescriptive path is sketchily marked indeed.").

highlighted by Waldman, proposing that courts adopt shared meaning analysis to determine when text in an online privacy policy adds actual terms to a contract.

When looking back, historians will also seek to identify the full causes of this shift toward surveillance capitalism. Obvious factors include the rapid transition from in-person to digital market exchanges, technological advancements enabling massive increases in storage capacity, enhanced CPU processing speeds, and new computational methods — like artificial intelligence and machine learning — that can detect once unimaginable patterns in data and levers of consumer and political manipulation. This Article has demonstrated that a further critical, yet still overlooked, cause is the paradigm slip in contract law itself, which has facilitated vast transfers of personal data under the guise of "contract." These processes enable corporations to build increasingly detailed psychological profiles of individuals as they engage in routine activities on their computers and smartphones — often in settings of perceived privacy, such as at home or when using a cellphone outside others' physical view. Yet, the accumulation of these small, unfelt invasions is scaffolding, leading to a pervasive framework of surveillance that is barely recognized by the general public.

Historians will, therefore, also have to record another causal fact: how courts respond to the paradigm slip in contract law that contributes to these mounting problems. Specifically, will courts view themselves as trapped in decades of precedential entanglement, forcing them to conflate pseudo-contract with contract, even while awaiting elusive regulatory solutions? Or will they take the time to examine more carefully how contract interpretation should align with the realities of language use in digital contexts? Contract meaning depends, most fundamentally, not on legal precedent but rather on what parties *do* with language, in specific social contexts and against the backdrop of linguistic norms that allow for shared meanings, and actual mutual understandings, to be produced.[303] Legally, the sole traditional aim of contract interpretation is to discern this shared meaning.[304] Whether courts currently recognize it or not, they therefore possess both the common law authority and a legal duty to get contract meaning right in digital settings, thereby returning data markets to a much more justifiable and undistorted state. History will judge their choice.

303. *See* Kar & Radin, *supra* note 4, at 1138–44.

304. *See* RESTATEMENT, CONTRACTS, *supra* note 4, § 201 cmt c. (stating that when interpreting contracts, "the primary search is for a common meaning of the parties").