ARTICLE

MURKY CONSENT: AN APPROACH TO THE FICTIONS OF CONSENT IN PRIVACY LAW

DANIEL J. SOLOVE[*]

ABSTRACT

Consent plays a profound role in nearly all privacy laws. As Professor Heidi Hurd aptly said, consent works "moral magic"—it transforms things that would be illegal and immoral into lawful and legitimate activities. As to privacy, consent authorizes and legitimizes a wide range of data collection and processing.

There are generally two approaches to consent in privacy law. In the United States, the notice-and-choice approach predominates: organizations post a notice of their privacy practices and people are deemed to consent if they continue to do business with the organization or fail to opt out. In the European Union, the General Data Protection Regulation ("GDPR") uses the express consent approach, where people must voluntarily and affirmatively consent.

Both approaches fail. The evidence of actual consent is nonexistent under the notice-and-choice approach. Individuals are often pressured or manipulated, undermining the validity of their consent. The express consent approach also suffers from these problems—people are ill-equipped to decide about their privacy, and even experts cannot fully understand what algorithms will do with personal data. Express consent also is highly impractical; it inundates individuals with consent requests from thousands of organizations. Express consent cannot scale.

In this Article, I contend that most of the time, privacy consent is fictitious. Privacy law should take a new approach to consent that I call "murky consent." Traditionally, consent has been binary—an on/off switch—but murky consent exists in the shadowy middle ground between full consent and no consent. Murky

[*] Eugene L. and Barbara A. Bernard Professor of Intellectual Property and Technology Law, George Washington University Law School. I would like to thank my research assistant Tobi Kalejaiye for her excellent work. Thanks to Ifeoma Ajunwa, Josef Ansorge, Omri Ben-Shahar, Eduardo Bertoni, Brian Bix, Danielle Citron, Ella Corren, Oscar Gandy, Bob Gellman, Mike Hintze, David Hoffman, Chris Hoofnagle, Nancy Kim, Florencia Marotta-Wurgler, Allyson Haynes Stuart, Ari Waldman, Rebecca Wexler, and Tal Zarsky for helpful feedback.

consent embraces the fact that consent in privacy is largely a set of fictions and is at best highly dubious.

Because it conceptualizes consent as mostly fictional, murky consent recognizes its lack of legitimacy. To return to Hurd's analogy, murky consent is consent without magic. Rather than provide extensive legitimacy and power, murky consent should authorize only a very restricted and weak license to use data. Murky consent should be subject to extensive regulatory oversight with an ever-present risk that it could be deemed invalid. Murky consent should rest on shaky ground. Because the law pretends people are consenting, the law's goal should be to ensure that what people are consenting to is good. Doing so promotes the integrity of the fictions of consent. I propose four duties to achieve this end: (1) duty to obtain consent appropriately; (2) duty to avoid thwarting reasonable expectations; (3) duty of loyalty; and (4) duty to avoid unreasonable risk. The law can't make the tale of privacy consent less fictional, but with these duties, the law can ensure the story ends well.

CONTENTS

INTRODUCTION

Consent plays a profound role in nearly all privacy laws. With the consent of individuals, a wide range of data collection and processing is permissible.[1]

Consent pervades many areas of law, from contract to sexual assault to plea bargaining to waiver of rights, and it has proven to be a contentious and difficult issue wherever it is involved.[2] There is no exception for privacy law—consent is one of privacy law's most vexing issues. This Article focuses on consent in privacy law, which I call "privacy consent." I will concentrate on the collection, use, and disclosure of personal data involved with many transactions people make every day, from using apps to buying products to browsing the Internet to purchasing products and services. Because consent differs quite substantially in different contexts, my arguments are tailored to privacy consent only.

Consent is a golden ticket: it provides tremendous power to collect, use, and disclose data. Philosophy and law professor Heidi Hurd considers consent to be a form of "moral magic."[3] Consent, she aptly notes, "turns a trespass into a dinner party; a battery into a handshake; a theft into a gift; an invasion of privacy into an intimate moment; a commercial appropriation of name and likeness into a biography."[4] The magic that consent conjures is legitimacy. Consent legitimizes activities that would otherwise be illegitimate, immoral, or illegal. Legitimacy bestows power.

Unfortunately, privacy consent is fraught with problems. 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.

Privacy laws vary widely about which types of consent to require, and many fail to require *meaningful* consent. By "meaningful" consent, I am referring to consent that is informed, not coerced or unduly manipulated, and where individuals have the capability to make an appropriate risk assessment about the costs and benefits of consenting. In privacy law, the conditions for meaningful consent mainly exist in a fairy tale.

There are generally two approaches to consent in privacy law, and both fail to work effectively. In the United States, the notice-and-choice approach predominates, in which organizations post a notice about their privacy practices and then people are deemed to have consented to these practices if they fail to opt out. In the European Union ("EU"), the General Data Protection Regulation

---

[1] By data "processing," I am using the term broadly to encompass the use, storage, and transfer of personal data—essentially, everything that is done with it after collection.

[2] DERYCK BEYLEVELD & ROGER BROWNSWORD, CONSENT IN THE LAW 4 (2007).

[3] Heidi M. Hurd, *The Moral Magic of Consent*, 2 LEGAL THEORY 121, 121 (1996); *see also* GEORGE P. FLETCHER, BASIC CONCEPTS OF LEGAL THOUGHT 109 (1996) ("When individuals consent to undergo medical operations, to engage in sexual intercourse, to open their homes to police searches, or to testify against themselves in court, they convert what otherwise would be an invasion of their person or their rights into a harmless or justified activity.").

[4] Hurd, *supra* note 3, at 123.

("GDPR") uses the express consent approach, in which people must voluntarily and affirmatively consent (opt in).[5]

The notice-and-choice approach creates a fiction of consent too fanciful even for magical realism. Inaction is not an indication of consent; it signifies nothing. The overwhelming consensus of studies and scholarship has shown that people do not read privacy policies, cannot possibly read them all, and do not understand them in the rare circumstances they review them.[6]

Although better than notice-and-choice, the express consent approach is also deeply flawed. Even when opting in, people often struggle to understand the potential risks of consenting to various ways their data might be processed. People are often unable to consent meaningfully to many instances of the collection or processing of their data.[7] The express consent approach also is highly impractical: it inundates individuals with consent requests from thousands of organizations, giving people "consent fatigue" and making people less likely to consider each request. Moreover, the GDPR requires consent to each different type of data processing endeavor, which means that organizations must obtain multiple consents from individuals.[8] Express consent doesn't scale.

No matter how it is obtained, consent is not meaningful if made without adequate understanding. The amount of information and time needed to properly inform individuals to decide is far too extensive to be practical.

Attempts to fix privacy consent are futile. Several privacy laws seek to make privacy notices more conspicuous, but people still fail to read them. Privacy laws try to simplify and shorten privacy notices so that people can understand them, but simplistic and short privacy notices fail to accurately describe the practices and implications. Privacy is very complex, and attempts to simplify it are distorting and end up as vague generalities that are not informative. The harsh truth is that meaningful consent is rarely possible for most instances of data collection and processing.

When consent exists, it confers legitimacy. But as most privacy consent is fictitious, the legitimacy it provides is unwarranted, creating a dangerous situation because it confers power where power ought not to be given. Playing on Hurd's analogy, fictitious consent works like dark magic; it is a mischievous sorcery that dupes and distorts.

An alternative is to abandon consent and have government regulation predetermine when personal data can be collected, used, or disclosed. But this approach would be problematic as it would involve extensive government control and micromanagement as well as impinge on people's autonomy. There are people who want to trade their personal data for discounts. There are people

[5] *See infra* Section I.B.

[6] *See infra* Section II.A, C.

[7] *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881-82 (2013) [hereinafter Solove, *Privacy Self-Management*].

[8] EUROPEAN DATA PROT. BD., GUIDELINES 5/2020 ON CONSENT UNDER REGULATION 2016/679, ¶ 64 (2020).

who want their location tracked for certain benefits. There are people who gladly accept the prevailing business model of many websites, which is to offer free information and services in exchange for monetizing personal data. Autonomy demands at least some freedom to choose even when people's choices are not in their best interest or are made under imperfect circumstances.

Consent is troubling yet also necessary—a situation that I term the "consent dilemma."[9] Privacy law has not solved the consent dilemma, and this issue continues to plague attempts to regulate privacy.

In this Article, I propose a way out of the consent dilemma—a new approach to consent in privacy law that I call "murky consent." This approach begins by leaning in the opposite direction of the law and most attempts to address privacy consent. Instead of trying in vain to turn consent from fiction to fact—to make it genuine, informed, and meaningful—the law should instead lean into the fiction. The law should embrace privacy consent in its murkiness.

Currently, privacy law has a binary view of consent—either there is consent or there isn't. Recognizing murky consent creates a middle position between the binary poles of consent and nonconsent. Most privacy consent is fraught with ambiguity, beset with problems, deeply problematic, and unreliable. Rather than deny these deficiencies as some approaches do, or try to repair them as other approaches do, the best approach is to accept and acknowledge them.

Because it conceptualizes consent as mostly fictional, murky consent recognizes its lack of legitimacy. To return to Hurd's analogy, murky consent is consent without magic. Rather than provide extensive legitimacy and power, murky consent should authorize only a very restricted and weak license to use data. This would allow for a degree of individual autonomy but with powerful guardrails to limit exploitative and harmful behavior by the organizations collecting and using personal data.

In this Article, I argue most privacy consent should be considered to be murky consent, and that this is the ideal form of consent for the law to recognize in most circumstances. Because murky consent lacks legitimacy, the law should reduce its power. The law can do so by making murky consent subject to extensive regulatory oversight with an ever-present risk that it could be deemed invalid. Murky consent should rest on shaky ground. Because the law pretends people are consenting, the law's goal should be to ensure what people are consenting to is good. Doing so promotes the integrity of the fictions of consent.

I propose four duties to achieve this end: (1) duty to obtain consent appropriately; (2) duty to avoid thwarting reasonable expectations; (3) duty of loyalty; and (4) duty to avoid unreasonable risk. The law can't make the tale of privacy consent less fictional, but with these duties, the law can ensure the story ends well.

In Part I, I discuss consent in privacy law. I discuss the two general approaches to consent in privacy law, the notice-and-choice approach

[9] Solove, *Privacy Self-Management*, *supra* note 7, at 1894.

(commonly used in the United States) and the express consent approach (used in the EU).

In Part II, I discuss why both approaches to consent fail. There are many problems with consent—it is often highly ambiguous, subject to undue influence, rarely fully informed, and twisted by pre-existing notions and expectations. An even deeper set of problems exists—people are incapable or ill-equipped to make many consent decisions. Making all relevant choices regarding one's privacy does not scale and becomes too burdensome.

In Part III, I discuss the murky consent approach, why it is preferable to the other approaches to privacy consent, and the specific guardrails that should be applied to murky consent.

I. CONSENT IN PRIVACY LAW

Consent in privacy laws takes several forms, but broadly, there are two approaches: (1) the notice-and-choice approach; and (2) the express consent approach.

Common in the United States, the notice-and-choice approach involves a dubious form of implied consent. Organizations provide a notice of privacy practices, and consent is implied if people fail to opt out of certain forms of data collection and use, or if people continue to do business with the organization. Consent is thus presumed from inaction.[10]

In contrast, the EU's GDPR takes an express consent approach, which requires affirmative and unambiguous consent and rejects implied consent through inaction.[11] An express consent approach requires that people opt in to the collection and processing of their data by taking an affirmative action to indicate consent, such as checking a box or clicking an accept button.[12]

In this Part, I discuss both approaches and their underlying philosophies.

A. *The Notice-and-Choice Approach*

In the United States, a common approach to collecting and processing data is the "notice-and-choice" approach.[13] Organizations create a privacy notice (also

[10] *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (7th ed. 2021).

[11] Commission Regulation 2016/679, pmbl. ¶ 32, 2016 O.J. (L 119) (providing consent must be "freely given, specific, informed and unambiguous").

[12] *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (8th ed. 2024).

[13] U.S. privacy law frequently uses the notice-and-choice approach. *See, e.g.*, CAN-SPAM Act, 15 U.S.C. § 7704(a)(3) (allowing organizations to send unsolicited commercial emails to people, who must unsubscribe to make unwanted e-mails stop); Telephone Consumer Protection Act, 47 U.S.C. § 227 (permitting telemarketers to call people unless they affirmatively ask to be placed on National Do Not Call Registry or tell each particular caller to cease). Other laws require express consent. *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. § 6502(b) (requiring parents to provide express consent for collection and processing of

called a "privacy policy" or "privacy statement") to inform people about the collection and processing of personal data. Individuals are given a "choice" to opt out of certain uses and disclosures, such as sharing or selling personal data to third parties. At its most basic, the choice is take-it-or-leave-it—either do business with an organization or do not. In other instances, organizations present ways to opt out of certain data uses; if people fail to opt out, then they are deemed to consent.

Under the notice-and-choice approach, transparency is the key imperative—the onus is on individuals to review the privacy notice and then decide if they want to proceed. People's inaction (failure to opt out) is interpreted as implied consent to whatever collection and processing of personal data a company discloses in its privacy notice.

The notice-and-choice approach developed in the late 1990s as primarily a form of self-regulation. Many organizations began voluntarily posting privacy notices on their websites. These notices described the site's privacy practices, and users could then decide whether to continue using the site.[14]

In the late 1990s, the Federal Trade Commission ("FTC") endorsed the notice-and-choice approach, aiming to strengthen it by bringing enforcement actions against companies that violated the promises made in privacy notices.[15] The FTC interpreted the FTC Act's prohibition on deceptive trade practices to encompass broken promises in privacy notices.[16] In a 1998 report, the FTC declared that "[i]n the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web" and that "choice easily can be exercised by simply clicking a box on the computer screen."[17] The FTC noted "the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness)."[18] Yet the FTC only called for federal legislation to protect children's privacy.[19] The FTC issued a

children's data); Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.508(a) (requiring affirmative consent for certain uses and disclosures of protected health information). Some laws use a mix of the two approaches to consent. *See, e.g.*, Video Privacy Protection Act, 18 U.S.C. § 2710(2)(B) (opt in); 18 U.S.C. § 2710(2)(d) (opt out); Cable Communications Policy Act, 47 U.S.C. § 551(c)(1) (opt in); 47 U.S.C. § 551(c)(2) (opt out).

[14] Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even if Consent Frameworks Aren't*, 9 J. INFO. POL'Y 148, 153 (2019) ("[Under the notice-and-choice approach,] businesses can do what they want with user information, provided (1) they tell users that they are going to do it and (2) users choose to proceed.").

[15] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585-86 (2014).

[16] *Id.* at 628-30.

[17] FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 8-9 (1998), https://www.ftc.gov/reports/privacy-online-report-congress [https://perma.cc/EF5J-PB8Z].

[18] *Id.* at 41.

[19] *Id.* at 42.

follow-up report in 1999 reaching essentially the same conclusions.[20] Thus, during this period, the FTC focused mostly on spurring companies to follow the notice-and-choice approach and did not delve into its shortcomings.

Without the FTC's intervention, the posting of privacy notices would have lacked much meaning because there would have been no effective enforcement mechanism to ensure the promises in the notices would be kept. Only in a handful of cases did plaintiffs seek to challenge breaches of privacy notices in court via contract law actions, and most of these cases faltered.[21] Although privacy notices look similar to a contract, courts have still not consistently held that they are contracts, and to this day, it is notable how few cases have directly addressed the issue.[22] The FTC thus supplied teeth to the notice-and-choice approach, giving it a thin veneer of legitimacy.

Originally a voluntary business practice, privacy notices began to be codified into laws. For example, an early law to adopt the notice-and-choice approach was the Gramm-Leach-Bliley Act ("GLBA") in 1999.[23] The law requires financial institutions to provide people with a privacy notice and gives them the right to opt out of some data sharing.[24]

The notice-and-choice approach has been savaged in academic literature.[25] Hardly anyone reads privacy notices, those who try to read them struggle to

[20] FTC, SELF-REGULATION AND PRIVACY ONLINE: REPORT TO CONGRESS 5-6 (1999) (confirming challenges related to protection of children's privacy online and proposing steps for FTC to address issues).

[21] Solove & Hartzog, *supra* note 15, at 588-89 (noting nearly all privacy regulation cases end in settlement).

[22] There has been debate about the extent to which courts recognize privacy policies as contracts. The reporters to the American Law Institute's Restatement of Consumer Contracts concluded that most courts have recognized privacy policies as contracts. *See generally* Oren Bar-Gill, Omri Ben-Shahar & Florencia Marotta-Wurgler, *Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts*, 84 U. CHI. L. REV. 7 (2017). *But see* Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REGUL. 45, 51 (2019) ("[T]he Reporters' data regarding the judicial treatment of privacy policies do not adequately support the conclusions they draw . . . ."). Cases reach differing conclusions on whether privacy policies or notices are contracts. For example, in *Dyer v. Northwest Airlines*, the court held that "broad statements of company policy do not generally give rise to contract claims." 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004). In *Calhoun v. Google*, the court held that because Google's Chrome browser contract was incorporated by reference in the terms of service, "rather than being an informational resource, the Chrome Privacy Notice is part of the contract between Plaintiffs and Google." 526 F. Supp. 3d 605, 633 (N.D. Cal. 2021). The law does not yet appear to be conclusive on the question of whether privacy policies are contracts.

[23] 15 U.S.C. § 6802(a)-(b).

[24] *Id.*

[25] Meg Leta Jones & Jenny Lee, *Comparing Consent To Cookies: A Case for Protecting Non-Use*, 53 CORNELL INT'L L.J. 97, 124-127 (2020) (discussing critiques of attempts to give people "control" over their data through notice-and-choice); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019)

understand them, the statements in privacy notices are often vague and ambiguous, and the effort to read privacy notices does not scale because there are too many to read.[26] As a result, a remarkably low percentage of people opt out, which allows organizations to use personal data with only the vague self-imposed limits stated in the privacy notices.[27]

Even though few can defend the notice-and-choice approach, it has persisted in U.S. privacy law. A recent breed of state consumer privacy laws has embraced the notice-and-choice approach. As of 2023, about a dozen states have enacted consumer privacy laws. All primarily involve posting a notice about the sale of personal data to third parties or the sharing of personal data for targeted advertising and then providing people with a right to opt out.[28]

B. *The Express Consent Approach*

An alternative to the notice-and-choice approach is the express consent approach. Also known as "affirmative" consent,[29] express consent requires a clear voluntary indication of consent. Express consent is central to the EU's GDPR as well as privacy laws in many countries. Some privacy laws in the United States also take an express consent approach, though a majority use the notice-and-choice approach.

Express consent under the GDPR is part of its "lawful basis"[30] approach to regulating the collection and processing of personal data.[31] A "lawful basis" is a

(challenging notice-and-choice by listing examples of everyday privacy agreements with digital platforms and describing fatigue users feel from deluge of privacy agreements); Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 371 (2014) (establishing many articles and books criticize notice-and-choice without viable solution); Susser, *supra* note 14, at 149 (arguing notice-and-choice does not adequately protect people's privacy and listing complaints from academic community on matter); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 34 (2011) (noting consensus that notice-and-choice is a failure).

[26] Solove, *Privacy Self-Management*, *supra* note 7, at 1888; 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) (concluding if people were to read all relevant privacy notices, it would take more than 200 hours per year).

[27] Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230 (2002) (noting one survey found "only 0.5% of banking customers had exercised their opt-out rights").

[28] Mallory Acheson, Brianna Kelly & Jack Pringle, *2023: The Year of New Privacy Laws*, JD SUPRA (July 25, 2023), https://www.jdsupra.com/legalnews/2023-the-year-of-new-privacy-laws-7706078 [https://perma.cc/4PRF-LTQC].

[29] *What Is Valid Consent?*, U.K. INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ [https://perma.cc/86F9-XPJE] (last visited Feb. 15, 2024).

[30] EUROPEAN DATA PROT. BD., GUIDELINES 05/2020 ON CONSENT UNDER REGULATION 2016/679, ¶ 17 (2020).

[31] Commission Regulation 2016/679, art. 6(1), 2016 O.J. (L 119).

permissible reason to collect and process personal data. The GDPR recognizes six lawful bases: (1) consent of the data subject; (2) processing is necessary to the performance of a contract to which the data subject is a party; (3) processing is necessary to comply with a legal obligation; (4) processing is necessary to protect the vital interests of the data subject or another person; (5) processing is necessary to perform a task carried out in the public interest; and (6) processing is necessary for the controller's legitimate interests or those of a third party.[32]

Consent is thus just one of the six recognized lawful bases under the GDPR. It is also a lawful basis in the laws of most countries that use the lawful basis approach.[33] Many countries that do not use the lawful basis approach rely even more heavily on consent—they require consent as the primary basis to process personal data, though there are exceptions.[34]

Express consent is one of the strictest forms of consent in privacy laws. The GDPR requires that consent be a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[35] Consent under the GDPR is restrictive and not as unlimited as it is in many U.S. privacy laws.[36] Additionally, under the GDPR, the organizations obtaining consent must be able to produce proof of it.[37]

The GDPR provides individuals with the right to withdraw their consent for the future processing of personal data.[38] The right to withdraw consent is typically prospective rather than retroactive. Withdrawal of consent is linked to a right to have companies stop processing data or to delete it.

The express consent approach is far superior to the notice-and-choice approach. Unfortunately, express consent still has similar problems to the notice-and-choice approach, as well as other problems. I discuss these difficulties in the next part.

---

[32] *Id.*

[33] *See, e.g.*, Lei No. 13.709, de Agosto de 2018, incluído pela Lei n° 13.853 de 2019, Lei Geral de Proteção de Dados Pessoais, de 18 de Septembro de 2020 (Braz.); Data Protection Act, 2020 (Jam.); Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm [https://perma.cc/QGZ3-ZXJB] (China).

[34] *See* SOLOVE & SCHWARTZ, *supra* note 10, at 1296-99. There are exceptions to consent, which often are similar to the GDPR lawful bases. In practice, many organizations rely heavily on the exceptions to consent enumerated under the laws to process data. Consent-based laws thus turn into the functional equivalent of lawful basis laws.

[35] Council Regulation 2016/679, art. 4(11), 2016 O.J. (L 119).

[36] Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 144 (2017).

[37] *Id.*

[38] Council Regulation 2016/679, art. 7(3), 2016 O.J. (L 119).

II. CONSENT'S FICTIONS AND FALSE LEGITIMACY

Many privacy laws rely heavily on consent as a means to legitimize data collection and processing because consent carries such significant "moral force."[39] In modern Western philosophy, Thomas Hobbes, Adam Smith, and John Stuart Mill developed a lasting foundation for consent based on respect for individuals as autonomous beings.[40] Mill's concept of permitting individuals to make self-regarding choices has been enshrined as a central pillar of a free society. In the words of Mill, there is "a sphere of action in which society, as distinguished from the individual, has, if any, only an indirect interest; comprehending all that portion of a person's life and conduct which affects only himself, or if it also affects others, only with their free, voluntary, and undeceived consent and participation."[41]

Privacy law is caught in a battle between its two general approaches to consent—the notice-and-choice approach and the express consent approach. Both approaches, however, are fatally flawed. Although the notice-and-choice approach is especially problematic, many problems with consent also apply to express consent.

Consent is not meaningful unless people are truly informed, have appropriate choices, and are able to make a good risk assessment in exercising their choices. Even if a person freely chooses an option without any degree of coercion or manipulation, if the person lacks a reasonable understanding of the consequences of choosing the option, the consent is hollow.[42]

In theory, valid privacy consent should entail a clear indication that individuals are making an informed and voluntary decision. Unfortunately, consent falls far short of this ideal, so much so that it is hard to deem it as consent at all. Many problems beset privacy consent, and they are devastating. But the law generally ignores them and blithely continues to recognize much collection and processing of personal data as consensual. Severe deficiencies in consent are papered over with one fiction after another. What makes these fictions of consent so problematic is that consent bestows legitimacy that underpins the

---

[39] *Preface to* THE ETHICS OF CONSENT, at ix (Franklin G. Miller & Alan Wertheimer eds., 2010); *see also* John Kleinig, *The Nature of Consent*, *in id.* at 4 ("[C]onsent plays an important moral role . . . [and] transform[s] the normative expectations that hold between people and groups . . . .").

[40] David Johnston, *A History of Consent in Western Thought*, *in* THE ETHICS OF CONSENT, *supra* note 39 at 25, 45-49 (summarizing three philosophers' theories of individualism).

[41] JOHN STUART MILL, ON LIBERTY 13 (David Spitz ed., 1975) (1859).

[42] Emma C. Bullock, *Valid Consent*, *in* THE ROUTLEDGE HANDBOOK OF THE ETHICS OF CONSENT 85, 86 (Andreas Müller & Peter Schaber eds., 2018) ("The three procedural requirements for valid consent are that the consent is voluntary, informed and that the consenting party is decisionally competent."); Peter Schaber, *Consent and Wronging a Person*, *in* THE ROUTLEDGE HANDBOOK OF THE ETHICS OF CONSENT, *supra* 55, 55 ("[C]onsent does change the moral property of acts if and only if it meets certain procedural requirements for valid consent: that consent was voluntary, informed, and competently given.").

power to collect, use, and transfer personal data.[43] Privacy consent thus provides false legitimacy—power without moral authority.

In this Part, I discuss the various fictions of privacy consent. In most situations, privacy consent is scant, incomplete, unreliable, nonexistent, or impossible.

A. *Lack of Indications of Consent*

Indications of privacy consent are rarely clear; they are often highly ambiguous. Laws vary in how valiantly they try to obtain clear consent, from laws that recognize consent based on zero evidence to laws that look for various indicia of consent. Unfortunately, all of them fail.

Under the notice-and-choice approach, many U.S. laws accept silence or inaction constituting implied consent. When a privacy notice provides people with a right to opt out, people are deemed to have consented if they do not. This still holds true even if people never visited the privacy notice page, which is often a tiny link at the footer of a website that requires extensive scrolling to reach.

Another way that consent is implied under the notice-and-choice approach involves inaction based on a preticked box. Failing to untick the box is deemed to be consent. Under the GDPR, preticked boxes are explicitly called out as inadequate to indicate consent.[44]

Under either scenario—inaction based on a privacy notice or submitting a form without unchecking a box—there is no meaningful indication of consent. Failing to opt out doesn't reflect consent; it just demonstrates people's inertia and inattention. With the privacy notice, the odds are overwhelmingly against the person ever having visited the page, let alone read it. Paul Schwartz calls this situation the "consent trap"—people are deemed to have consented to the processing of their data merely by visiting a website.[45] Implying consent in such a situation is completely unjustified, especially given that most people do not read privacy notices.[46]

U.S. privacy law, however, blatantly allows these fictions to masquerade as consent. Although websites can readily determine whether a particular person visited the privacy notice page—and even how long a person stayed on that

[43] Hubert Schnüriger, *What Is Consent?*, THE ROUTLEDGE HANDBOOK OF THE ETHICS OF CONSENT, *supra* note 42 at 21, 21 ("Consent works as a criterion of legitimacy, deeply pervading social life, making actions and practices permitted that would otherwise be forbidden.").

[44] Council Regulation 2016/679, ¶ 32, 2016 O.J. (L 119).

[45] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1662 (1999).

[46] *See* Omri Ben-Shahar & Adam Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, 45 J. LEGAL STUD. S41, S42 (2016) ("According to one estimate, the average person encounters so many privacy disclosures every year that it would take 76 days to read them . . . .").

page—the law does not require finding out this information. Instead, the law blesses the strategy of setting up a poor and unreliable way to ascertain if people consented and then burying one's head in the sand by further evading any available methods to learn more.

In practice, the notice-and-choice approach does not involve much notice or choice. The law fails to require that people read or understand notices—and in the vast majority of cases, notices are ignored. In many circumstances, the choices presented are not meaningful ones.

Although clearly better than the notice-and-choice approach, the express consent approach also fails to provide clear evidence of consent. Express consent can be manifested by people taking some kind of action, such as signing a document, filling out an online form, or clicking a button on a website.

Express consent, however, only provides a superficial indication of consent. It fails to capture how informed people are and whether people really understand contractual terms. Most people do not read the terms of the contracts to which they agree.[47] A study by Florencia Marotta-Wurgler revealed that requiring people to click an "I agree" box next to terms only increased readership by 1%.[48]

One of the most superficial approaches to obtaining express consent involves allowing people to click the *accept* button without reading the details about what they are accepting.

Another approach involves requiring a person to scroll down a long regurgitation of legalese and then click accept, something that might strike many consumers as annoying and cumbersome. In willful ignorance, these mechanisms do not measure how fast a person scrolls down, avoiding the gathering of evidence that most people race to the bottom too quickly to read the text.

---

[47] Eric Goldman, *The Crisis of Online Contracts (as Told in 10 Memes)*, 2 NOTRE DAME J. ON EMERGING TECH. 1, 5 (2021) (noting "few consumers actually read online contract terms"); David A. Hoffman, *Relational Contracts of Adhesion*, 85 U. CHI. L. REV. 1395, 1396 (2018) ("[C]onsumers don't read their contracts . . . ."); Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 546 (2014); 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) ("[O]nly 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."); Florencia Marotta-Wurgler & Daniel L. Chen, *Does Contract Disclosure Matter?*, 168 J. INSTITUTIONAL & THEORETICAL ECON. 94, 113-14 (2012) (finding terms in contracts have no effect on purchasing decisions); Richard A. Epstein, *Contract, Not Regulation: UCITA and High-Tech Consumers Meet Their Consumer Protection Critics*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 226, 227 (Jane K. Winn ed., 2006) ("[I]t seems clear that most consumers—of whom I am proudly one—never bother to read these terms anyhow: we . . . adopt a strategy of 'rational ignorance' to economize on the use of our time.").

[48] Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts*," 78 U. CHI. L. REV. 165, 168 (2011).

Suppose an approach were devised to not allow a person to accept until they scrolled down and had sufficient time to read the terms. The accept button would be grayed out until enough time elapsed, and then it could be clicked. Users would find such a system to be annoying, and the time to read the text would likely be outrageously long. A system that waited fifteen to thirty minutes before a user could accept would be a nonstarter. Even if a system were to wait the proper amount of time, there is no guarantee that people would spend the time actually reading the text.

Nobody really believes that people take the time to read privacy policies. Such a belief would be more absurd than believing in unicorns and fairies. The truth is that people don't read privacy policies and any "consent" to them is a complete lie, but the law accepts the fiction that people are actually consenting.[49]

B. *Lack of Voluntariness*

Voluntariness is at the very foundation of the concept of consent, yet in practice, U.S. privacy law tolerates many situations in which people do not freely agree. Realistically, few decisions are free of all constraints or influence, but far too many choices about privacy are so highly constrained and manipulated that they can hardly be considered voluntary.

1. Unilateral Imposition of Terms

Especially in the digital economy, U.S. courts enforce contracts that are often one-sided impositions of terms on consumers.[50] David Hoffman observes that in the modern digital age, people must agree to a vastly greater number of contracts, increasing steadily in length and duration, and "firms have seized new opportunities to shift risks to consumers by imposing unread terms."[51]

Standardized contracts, loaded with boilerplate language, are now common for consumer contracts. These boilerplate contracts, called "contracts of adhesion," are take-it-or-leave it, as there is no opportunity to negotiate over the terms. The problem with such contracts, as Margaret Jane Radin argues, is that they often force people to waive their rights to sue in the event of being harmed, they force people into mandatory arbitration, they prevent people from joining class action lawsuits, and they select inconvenient locations for people to exercise their rights.[52] These contracts allow businesses to "construct their own

[49] Other areas of law attempt the same futile alchemy to try to turn the fiction into fact. Consider a mortgage signing, in which people must sign countless disclosure forms at a meeting in which it is completely impossible to read everything during the meeting. Document upon document is signed in an absurd ritual.

[50] Mark A. Lemley, *The Benefit of the Bargain*, 2023 WIS. L. REV. 237, 238-39 (2023).

[51] David A. Hoffman, *From Promise to Form: How Contracting Online Changes Consumers*, 91 N.Y.U. L. REV. 1595, 1596 (2016).

[52] MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 3-9 (2013).

legal universe" that deletes "rights structures enacted and guaranteed by the state."[53]

With the Internet of Things—the burgeoning number of smart products and devices connected online—the fiction of meaningful consent is even further strained. Often, there is no readily available display or link to a host of documents that people purportedly agree to. As Stacy-Ann Elvy notes, "[b]y entering into a single [Internet of Things] transaction, consumers are frequently required to assent to multiple different documents, including different terms of use, privacy policies, warranty agreements, end user licensing agreements ("EULAs") and possibly service agreements, even when they contract with a single provider."[54] Courts have accepted the weakest indications of consent to validate a wide array of important issues such as "rights to use, process, and share consumer-generated data and content; disclaimers for cybersecurity failures and data loss; mandatory arbitration and class action waivers; and provisions that restrict consumers' property rights in the physical devices they purchase."[55]

Of course, with take-it-or-leave-it terms, people are purportedly free to leave it—at least in theory. But in many cases, there are not adequate alternatives, and individuals must essentially unplug from the modern world to protect their privacy and their rights. As for agreeing to the collection and use of personal data, Helen Nissenbaum argues that people often do not have much of a choice: "While it may seem that individuals freely choose to pay the informational price, the price of not engaging socially, commercially, and financially may in fact be exacting enough to call into question how freely these choices are made."[56]

The doctrines of duress and unconscionability merely patrol the outer boundaries.[57] Duress involves using threats of economic or physical harm to obtain consent.[58] Unconscionability involves contracts with one-sided terms that are unfair.[59] These cases are hard for people to win—as Mark Lemley observes, "[c]ourts rarely apply unconscionability."[60] Additionally, the U.S. Supreme

[53] *Id.* at 15, 33.

[54] STACY-ANN ELVY, A COMMERCIAL LAW OF PRIVACY AND SECURITY FOR THE INTERNET OF THINGS 120 (2021).

[55] *Id.* at 142.

[56] Nissenbaum, *supra* note 25, at 35.

[57] RESTATEMENT (SECOND) OF CONTRACTS § 208 (AM. L. INST. 1981) ("If a contract or term thereof is unconscionable at the time the contract is made a court may refuse to enforce the contract, or may enforce the remainder of the contract without the unconscionable term, or may so limit the application of any unconscionable term as to avoid any unconscionable result."); *id.* § 175(1) ("If a party's manifestation of assent is induced by an improper threat by the other party that leaves the victim no reasonable alternative, the contract is voidable by the victim.").

[58] Brian H. Bix, *Contracts*, *in* THE ETHICS OF CONSENT, *supra* note 39, at 251, 257.

[59] *Id.* at 259.

[60] Lemley, *supra* note 50, at 244-45 (discussing limits of unconscionability as tool to battle unfair standard form contracts).

Court has weakened unconscionability protections in a series of decisions expanding the Federal Arbitration Act ("FAA") to preempt state law.[61]

In rhetoric, contract law seemingly requires meaningful consent, but in practice, this is a fiction. According to the standard dogma, contracts "must result from a meeting of the minds of the parties in mutual assent to the terms, must be based upon a sufficient consideration, free from fraud or undue influence, not against public policy and sufficiently definite to be enforced."[62] Many contracts are not meetings of the minds but are unilateral terms offered by contract-makers and accepted by contract-takers. For consumers, these contracts are often not even read or understood. In the context of privacy notices, courts have not even issued clear caselaw about whether such notices are even contracts at all.[63]

Additionally, most privacy notices state that organizations can change the terms at any point in time.[64] People are thus ostensibly agreeing to a blank check—to nearly anything that an organization wants to do in the future.[65] When changes are made, often no effort is taken to notify people of them.[66]

Charlotte Tschider aptly notes privacy notices are often a "one-sided communication of an organization's behaviors with respect to data."[67] She asks: "[H]ow can consent to unfair, one-sided, readily changeable terms actually represent real choice?"[68]

As Brian Bix states, consent is "absent in the vast majority of the contracts we enter into these days, but its absence does little to affect the enforceability of those contracts."[69] Bix argues that accepting a lack of consent in contract law is practical because "making too many commercial transactions subject to serious challenge on consent/voluntariness grounds would undermine the predictability of enforcement that is needed for vibrant economic activity."[70] However, even

[61] RADIN, *supra* note 52, at 130-31 (noting how Supreme Court expanded Federal Arbitration Act's reach to cover noncommercial parties and state cases).

[62] Doe v. HCA Health Servs. of Tenn., Inc., 46 S.W.3d 191, 196 (Tenn. 2001).

[63] SOLOVE & SCHWARTZ, *supra* note 10, at 856-64.

[64] Thomas D. Haley, *Illusory Privacy*, 98 IND. L.J. 75, 100 (2022) ("Analysis of the 122 top websites reveals that every one includes in its platform terms a unilateral modification provision."); Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617, 637 (2021) ("[M]any privacy notices also contain some language giving the organization the right to change the terms at any time.").

[65] In some cases, the FTC has concluded retroactive changes in privacy notices applied to previously-gathered personal data can violate the FTC Act Section 5. *See* Solove & Hartzog, *supra* note 15, at 640-41.

[66] Haley, *supra* note 64, at 101-02 (explaining how many platforms disclaim any obligation to inform users of policy changes).

[67] Tschider, *supra* note 64, at 636.

[68] *Id.* at 639.

[69] Bix, *supra* note 58, at 251.

[70] *Id.* at 252.

if there are practical reasons to allow contracts without consent, the fiction that these contracts involve consent provides unwarranted legitimacy.

The GDPR takes a stricter approach by requiring that consent be "freely given."[71] But the question remains: *What does "freely given" mean?* The GDPR provides at Recital 42 that "[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."[72] Guidance by the European Union Data Protection Board ("EDPB") explains that consent is invalid if a person "feels compelled to consent or will endure negative consequences if they do not consent."[73]

Under the GDPR, consent is viewed more skeptically for certain "vulnerable" categories of people (such as children) or people in power relationships (such as employees and patients).[74] At Recital 43, the GDPR states that "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller."[75] In other words, the GDPR rarely accepts consent by employees to employer demands to process personal data due to the power imbalance in the employer-employee relationship.[76] Unfortunately, the GDPR does not apply this skepticism beyond these vulnerable populations. In the vast majority of situations, the GDPR thus turns a blind eye to the fact that consent is nothing more than an illusion.

2. Manipulation

Decisions about privacy are often unduly influenced to a degree that casts doubt on their voluntariness. Of course, rarely are decisions free of any influence. On the one side, persuasion is an acceptable influence whereas coercion is not. With privacy consent, there is rampant manipulation—which exists in the menacing middle ground between persuasion and coercion. Often, manipulation shares some of the darker features of coercion and ends up closer to that side of the spectrum. As Daniel Susser, Beate Roessler, and Helen Nissenbaum note, coercion "robs" people of choices whereas manipulation works more subtly; it "infiltrates [a person's] decision-making process."[77] Ido

[71] Commission 2016/679, ¶ 42, 2016 O.J. (L 119).

[72] *Id.*

[73] EUROPEAN DATA PROT. BD., GUIDELINES 5/2020 ON CONSENT UNDER REGULATION 2016/679, ¶ 13 (2020).

[74] *See* Commission Regulation 2016/679, ¶ 43, 2016 O.J. (L 119).

[75] *Id.*

[76] EUROPEAN DATA PROT. BD., GUIDELINES 5/2020 ON CONSENT UNDER REGULATION 2016/679, ¶ 21 (2020) ("For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.").

[77] Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 15-17 (2019) (describing how manipulation functions in more "subtle and sneaky" way than coercion).

Kilovaty argues manipulation "deprives individuals of their agency by distorting and perverting the way in which individuals typically make decisions."[78]

The lines between persuasion, manipulation, and coercion are gray, and privacy law struggles to develop a coherent approach, especially to manipulation. As Robert Gellman notes, "[t]hose who want to exploit consumer data will cajole, pressure, threaten, mystify, obscure, entice or otherwise coax consumers to agree."[79] According to Cass Sunstein, manipulation is so pervasive that "the legal system usually does not attempt to prevent it."[80] Shaun Spencer surveys different definitions of manipulation and concludes "they all contain the notion of circumventing the subject's rational decision-making process" and most require intent to manipulate.[81]

Although privacy law responds to a limited extent to some of the more abusive forms of manipulation, an enormous amount of manipulation persists. In response to manipulation, the FTC has used "unfairness" under the FTC Act to address "behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[82] The FTC can be more protective of consumers than contract law. Recent U.S. state privacy laws are adding restrictions on "dark patterns"—manipulative and deceptive interfaces and attempts to obtain consent.[83] Privacy law is trying to address manipulation, but practically, it can only address the worst schemes.

---

[78] Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 469 (2019); *see also* Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 174 (2019) ("Manipulative practices impair the process of choosing, subjecting it to the preferences and influences of a third party, as opposed to those of the individuals themselves."); Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MKTG. BEHAV. 213, 216 (2015) (arguing "effort to influence people's choices counts as manipulative to the extent that it does not sufficiently engage or appeal to their capacity for reflection and deliberation"); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1029 (2014).

[79] Robert Gellman, *Is There a Role for Consent in Privacy?*, IAPP (June 30, 2021), https://iapp.org/news/a/is-there-a-role-for-consent-in-privacy/ [https://perma.cc/U286-XBU].

[80] Sunstein, *supra* note 78, at 219.

[81] Shaun B. Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959, 989 (2020) (comparing different authors' definitions of manipulation).

[82] FTC, COMMISSION STATEMENT OF POLICY ON THE SCOPE OF THE CONSUMER UNFAIRNESS JURISDICTION (1980), *reprinted in* Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984) (discussing Commission's approach to unfairness matters).

[83] California Consumer Privacy Act of 2018, 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, decisionmaking, or choice, as further defined by regulation."); Colorado Privacy Act, COLO. REV. STAT. § 6-1-1303(9) (similarly defining "dark pattern"); *see also* Harry Brignull, *Dark Patterns: Dirty Tricks Designers Use To Make People Do Stuff*, 90 PERCENT OF EVERYTHING (July 8, 2010), https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/index.html [https://perma.cc/DE4E-J53Z] (coining term "dark patterns").

What makes manipulation so difficult to combat is that people are gullible and manipulable. Human decision-making is fraught with irrationality and systematic biases and heuristics that can readily be exploited.[84] As Ryan Calo notes, "the digitization of commerce dramatically alters the capacity of firms to influence consumers at a personal level."[85] Organizations can increasingly exploit "irrationality or vulnerability in consumers."[86] As Neil Richards and Woodrow Hartzog note, "[b]ecause companies have strong incentives to obtain consent, it is no surprise many . . . malicious interfaces are used to coerce, wheedle, and manipulate people to grant it."[87]

Ultimately, the law cannot stamp out all manipulation, which is so rampant that only certain kinds can be addressed. But the fact that manipulative techniques for obtaining consent are so legion means that we should be far less confident in any determination that people are truly consenting. Realistically, we will never reach a utopia where we have cleansed all troubling forms of manipulation from privacy consent. The effort to do so is noble, but in the meantime, the law's acceptance of consent in our highly manipulated world is a fiction.

3. Requiring Consent as a Condition

Another problem with determining whether privacy consent is truly consensual involves the extent to which consent can be required as a condition to receive products, services, or other benefits. People are often cajoled into consenting because they must pay or forgo something if they refuse.

Some privacy laws try to curtail requiring consent as a condition. For example, in the United States, regulations promulgated under the Health Insurance Portability and Accountability Act ("HIPAA") restrict conditioning healthcare services on consent to the use of personal data for marketing or other purposes.[88] Other laws have less bold restrictions. For example, the California Consumer Privacy Act ("CCPA") provides that businesses "shall not discriminate against a consumer because the consumer exercised any of the consumer's rights."[89] Forms of such discrimination include denying goods or services, charging different prices, or providing a different level of quality.[90] The Virginia Consumer Data Protection Act has a similar provision.[91]

[84] *See generally* DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011) (outlining modes of decisionmaking); DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS (2008).

[85] Calo, *supra* note 78, at 999.

[86] *Id.*

[87] Richards & Hartzog, *supra* note 25, at 1489.

[88] 45 C.F.R. § 164.508.

[89] California Consumer Privacy Act § 1798.125.

[90] *Id.* (listing types of discrimination prohibited by statute).

[91] VA. CODE ANN. § 59.1-574(A)(4) (listing ways in which data controller cannot discriminate against consumers).

But these laws have large loopholes because data is often the price of a particular product or service. The internet presents a grand bargain to people—free goods and services in exchange for personal data.[92] A saying often uttered about the internet is: "If you're not paying for the product, you are the product."[93] Those giving out "free" products or services are not doing so out of charity; they are monetizing based on the personal data they gather.

Organizations can readily structure transactions to make data collection and processing appear more necessary, thus evading the restrictions on conditions that many laws make. For example, under the CCPA, a business may charge more when their consumers refuse to allow the transfer of their personal data "if that difference is reasonably related to the value provided to the business by the consumer's data."[94] Businesses are allowed to offer financial incentives to consumers for collecting and selling their personal information.[95] The result is that people can be enticed to surrender their data with a cornucopia of treats—technologies that glimmer and gleam, dazzling entertainment, fascinating information, and enormous conveniences. Are they really consenting? Or are they responding like lab rats addicted to opium? People experience the internet as Hansel and Gretel, their mouths watering as they explore a world built of candy houses; they often don't realize they are being fattened up to be part of a feast.

Unlike the approach in the United States, the GDPR has much stricter restrictions on data controllers' abilities to make providing services conditional on consumer consent to process personal data that isn't necessary for the performance of that contract.[96] According to the EDPB, "[i]f consent is given in this situation, it is presumed to be not freely given."[97]

The GDPR is stronger at restricting conditioned consent, but it has limits. Ultimately, the organizations that aim to collect and process personal data have

[92] Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 606 (2014) (discussing internet users' exchange of personal information for purportedly free internet services).

[93] This quote is often attributed to the 2020 Netflix documentary, *The Social Dilemma*. *See* Daniel Hövermann, *If You Are Not Paying for the Product, You Are the Product!*, MEDIUM (Sept. 24, 2020), https://medium.com/change-your-mind/if-you-are-not-paying-for-the-product-you-are-the-product-4dbc15b9a3f2. But it was in use a long time prior to the documentary. *See* Scott Goodson, *If You're Not Paying for It, You Become the Product*, FORBES (Mar. 5, 2012, 12:34 PM), https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product.

[94] § 1798.125(a)(2).

[95] *Id.* § 1798.125(b) ("A business may offer financial incentives . . . for the collection of personal information, the sale or sharing of personal information, or the retention of personal information.").

[96] Commission Regulation 2016/679, art. 7(4), 2016 O.J. (L 119).

[97] EUROPEAN DATA PROT. BD., GUIDELINES 5/2020 ON CONSENT UNDER REGULATION 2016/679, ¶ 26 (2020).

control over how they frame transactions and contracts. This power can allow them to evade restrictions.

C. *The Difficulties of Being Informed*

Privacy consent is not meaningful if it is not informed.[98] If people lack an understanding of what they are agreeing to, they are not really consenting; they are just making decisions in the dark. As Joseph Raz writes:

> The ideal of personal autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives . . . . [O]ne must be aware of one's options . . . [and] be capable of understanding how various choices will have considerable and lasting impact on his life.[99]

Unfortunately, privacy consent often falls far short of any reasonable indication of the one giving consent actually being informed.

1. Lack of Reading and Understanding

Under both the notice-and-choice and express consent approaches, people rarely understand what they are consenting to; in most cases, they don't even read about the decisions they are making.

Reading privacy notices is an exercise in torturous tedium that hardly anybody undertakes. Most privacy notices are ignored. Laws often mandate disclosures and warnings to individuals, but individuals skim through them or do not read them all.[100] For the few brave souls who try to read privacy notices, they are submerged in a suffocating bog of vague and confusing prose. Privacy notices are often long and complex. They are often written at a very high reading level.[101]

---

[98] In the law, the concept of informed consent has been recognized in the healthcare and research contexts. Originating in the common law, the requirement for informed consent for healthcare emerged in the United States in the late 1950s and early 1960s. *See* RUTH R. FADEN & TOM L. BEAUCHAMP, A HISTORY AND THEORY OF INFORMED CONSENT 24, 86 (1986) (discussing how informed consent first emerged in American medicine). For healthcare, U.S. states began to enact informed consent statutes throughout the 1970s, with thirty states having enacted such laws by 1982. *Id.* at 256. For human subject research, regulations for informed consent require that subjects "must be provided with the information that a reasonable person would want to have in order to make an informed decision about whether to participate, and an opportunity to discuss that information." Protection of Human Subjects, 16 C.F.R. § 1028.116.

[99] JOSEPH RAZ, THE MORALITY OF FREEDOM 369, 369-71 (1986).

[100] OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 10 (2014) (noting people "overlook, skip, or skim disclosures").

[101] Solove, *Privacy Self-Management*, *supra* note 7, at 1885 (citing length and complexity of privacy notices as reason why people do not read them).

Some privacy laws make weak efforts to improve this woeful situation, such as by requiring the privacy notice to be more conspicuous or written more simply. Under the GLBA, which regulates the collection and use of data by financial institutions, notice must be "clear and conspicuous."[102] The California Online Privacy Protection Act ("CalOPPA") requires that a privacy notice be posted conspicuously on an organization's website.[103] The CCPA goes a step further by mandating a conspicuous button for people to opt out of selling or sharing personal data.[104]

But these efforts fail to guarantee that privacy notices are read. In a related situation, Florencia Marotta-Wurgler's research reveals that "no matter how prominently [end user license agreements] are disclosed, they are almost always ignored."[105] Beyond requiring that privacy notices be clear and conspicuous, the laws do not require any indication that people understand them.[106] In the United States, the law clings to the fiction that people actually read disclosures, warnings, and contract terms. David Hoffman observes that courts enforce waivers of rights in contracts consumers do not read, blaming consumers for agreeing to such terms even though it is clear they were not even aware of them.[107]

For U.S. laws requiring opt out options and for laws requiring express consent such as the GDPR, hardly any measures ensure that consent is informed. The GDPR states consent must be "freely given, specific, informed and unambiguous," but in practice, it is hard to determine the degree to which consent is informed. One can present more conspicuous terms, write them in simpler words, or require people to affirmatively check a box or click a button, but these things do not mean that people actually read and understand the terms.

Informed consent goes far beyond merely posting privacy notices, lengthy terms and conditions, or some other documents, which is typical of most instances of consent in privacy law. Merely making information available does not ensure that people have even seen or read the information. A step beyond is to ensure that people have been exposed to the information, but being given information is not equivalent to having genuine understanding. To be informed, people must truly understand the choices they are making. But neither the notice-and-choice approach nor the express consent approach provide much indicia of such understanding.

---

[102] 17 C.F.R. § 248.4(a) (setting requirements for initial notice).

[103] The Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE § 22575 (West 2023) (requiring commercial website operators to post privacy policies "conspicuously").

[104] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.185 (requiring development and use of recognizable opt-out button for consumers).

[105] Marotta-Wurgler, *supra* note 48, at 182.

[106] *See* Solove, *Privacy Self-Management*, *supra* note 7, at 1888 (noting most people do not read privacy notices, and if they do, they likely do not understand them).

[107] Hoffman, *supra* note 47, at 1396-97 (explaining how judges hold consumers to their deals despite fact consumers do not read adhesive contracts).

2. The Dilemma of Complexity and Simplicity

Privacy laws face a difficult dilemma with notice—either notice can be long and complex or short and simple. A long notice can explain meaningfully how personal data is collected and used, but such a notice will be more daunting for people to read and harder for them to understand.

Privacy laws often declare that notice should be simple and written in an understandable and accessible way. For example, the GDPR requires that privacy notices be "concise, easily accessible and easy to understand" and written in "clear and plain language."[108] Other privacy laws also require clear and understandable language. Virginia's Consumer Data Protection Act requires that privacy notices be "reasonably accessible, clear, and meaningful."[109] Beyond the law, commentators have proposed more simplified forms of notice, such as using privacy nutrition labels, icons, pithy pop-up boxes, and similar techniques of concision.[110]

Despite these legal requirements, privacy notices have not become more readable. One study comparing privacy notices before and after the GDPR went into effect in 2018 found "scant" improvement in readability.[111] Post-GDPR, "privacy policies are still very often unreadable."[112]

Even if notices were more readable, simpler notice does not seem to lead to better understanding. In an empirical study by Omri Ben-Shahar, where he and his team presented subjects with privacy notices at varying degrees of simplicity, they found that in all circumstances, "results were consistent: altering the formal properties of the privacy disclosures had essentially no effect on respondents' comprehension of our disclosure, willingness to disclose information, or expectations about their privacy rights."[113] A study led by Aleecia McDonald compared several formats of a privacy policy, including a "short form with standardized components in addition to a full policy," and found that

[108] Commission Regulation 2016/679, ¶ 58, 2016 O.J. (L 119). The EDPB guidance states that a "message should be easily understandable for the average person." EUROPEAN DATA PROT. BD., GUIDELINES 5/2020 ON CONSENT UNDER REGULATION 2016/679, ¶ 67 (2020).

[109] Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-574(C) (2021).

[110] Mike Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044, 1066-77 (2017) (critiquing shorter privacy notice proposals for reducing transparency and eliminating meaningful information).

[111] Shmuel I. Becher & Uri Benoliel, *Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR*, *in* CONSUMER LAW & ECONOMICS 179, 197 (Klaus Mathis & Avishalom Tor eds., 2021) (discussing findings of study examining GDPR impact on privacy statement readability).

[112] *Id.*

[113] Ben-Sharhar & Chilton, *supra* note 46, at S44.

"participants were not able to reliably understand company's privacy practices with any of the formats."[114]

A very simple notice can't accurately describe many of the intricate ways that personal data is processed. Simple notices end up being vague and cursory. As Mike Hintze notes, "short-form approaches inevitably leave out important details, gloss over critical nuances, and simplify technical information in a way that dramatically *reduces* transparency and accountability."[115]

It is not clear that people could be fully educated about making certain privacy decisions because the matter is too complicated and too contingent upon future conditions. As Salon Barocas and Helen Nissenbaum observe, if privacy notices truly explained everything people needed to make informed decisions, "[t]he detail that would allow for this would overwhelm even savvy users because the practices themselves are volatile and indeterminate."[116]

The GDPR demands granular and specific consent to each particular purpose of data processing, yet also wants a simple and concise way to obtain consent—akin to wanting its cake and eating it too. The EDPB states that the GDPR requires that, at a minimum, the following information must be provided in order to adequately inform individuals: (1) the identity of the data controller, (2) the purpose of the data processing, (3) the type of data to be processed, (4) the existence of the right to withdraw consent, and (5) information about automated decision-making where relevant.[117] But this information is rather rudimentary. Knowing the types of data and the purposes of processing might not inform people of the issue they most need to know: *What is the risk that the processing of the data will cause harm?* Simplifying privacy notices will fail to be truly informative; making them more complex will create confusion. There is no way out.

3. Incorrect Pre-existing Notions

Informing people is difficult enough, as the amount of information to educate them about is enormous. But the task is made harder because people are not a tabula rasa, but have a tangle of pre-existing notions and expectations that are often wrong. This jungle of incorrect beliefs must be cleared to effectively inform individuals.

---

[114] Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley & Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats*, *in* PRIVACY ENHANCING TECHNOLOGIES 37, 37-38 (Ian Goldberg & Mikhail Atallah eds., 2009).

[115] Hintze, *supra* note 110, at 1044.

[116] 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, 58-59 (Julia Lane, Victoria Stodden, Stefan Bender & Helen Nissenbaum eds., 2014) (describing "transparency paradox" with short-form privacy notices).

[117] EUROPEAN DATA PROT. BD., *supra* note 30, ¶ 64 (May 4, 2020) (outlining minimum content requirements for informed consent under GDPR).

Several studies show that people harbor significantly incorrect notions about how their personal data is being collected and processed. Chris Hoofnagle and Jennifer Urban found that many people wrongly thought that their personal data was protected by stronger legal protections.[118] In a study by Kristen Martin, people read a privacy notice and then were asked about it, and they wrongly believed that their data would be more protected than what the notice said.[119] In another study led by Joseph Turow, a majority of people falsely believed that if a website has a privacy policy, then it can't share personal data with other companies without permission.[120] A study by Pew Research revealed that 52% of people surveyed wrongly believed that a privacy policy "ensures that the company keeps confidential all the information it collects on users."[121]

Consent that is not informed is already quite flawed, but it is further tainted when it is based on false beliefs. The task of correcting false notions and educating people would be a mammoth, and nearly impossible, project.

4. Lack of Expertise

Assessing privacy risk is immensely complicated and requires considerable expertise that most people lack. One might hope that people could be taught what they need to know in some kind of quick crash course, but the issues are simply too many and too complex to be taught in a slapdash manner. Even the most basic decisions are difficult for people to assess. Suppose a person is asked whether to share personal data with an organization. Part of the assessment of cost-benefit analysis turns on how secure and confidential the data will be. The organization promises "reasonable" security and that the data will be kept confidential. But to fully assess the risks, a person must know a lot more about the organization's data security program. Does the organization use good encryption? Does it have all the appropriate policies and procedures? Does it train its workforce? Does it adequately vet any vendor that handles personal data or has access to it? To assess confidentiality, the person needs to know about the privacy program. How well-resourced is it? What are the rules for when different parties can subpoena the data? How readily and likely will the government

[118] Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 305 (2014).

[119] Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. PUB. POL'Y & MKTG. 210, 219 (2015) (summarizing study findings).

[120] JOSEPH TUROW, JENNIFER KING, CHRIS JAY HOOFNAGLE, AMY BLEAKLEY & MICHAEL HENNESSEY, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT 21 tbl.9 (2009).

[121] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RSCH. CTR. (Dec. 4, 2014), https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ [https://perma.cc/ST38-GZ83] (summarizing study findings).

access the data? Is the workforce trained about privacy? How are access controls managed?

The list can go on and on. Most people end up consenting based on bald statements that data is being protected, but these statements are often boilerplate written by lawyers to sound reassuring without promising very much. People simply do not know enough to meaningfully consent. In most cases, consent means taking a leap of faith in the dark.

People would also have to be taught about the intricacies of modern data analytics, which reveals surprising inferences.[122] Indeed, the very point of data analytics is to reveal inferences that are not obvious. As Dennis Hirsch correctly contends, "individuals cannot understand what information they are really disclosing and, as a consequence, cannot make a meaningful choice about whether or not to share the information in the first place."[123]

Additionally, people are often unaware of the metadata embedded with various digital files and documents they provide. For example, a photo can be saturated with metadata such as date, location, and other information.

So many activities are swarming in a mist of data, much like the invisible virus particles expelled when people talk and breathe. People are often unaware of the extent of this phenomenon, as well as precisely what data they are exposing, let alone all the inferences that can be made when the data is aggregated and analyzed. Short of training everyone to become expert data scientists, people will not comprehend what their data is revealing about themselves.

5. Too Many Unknowns

In many cases, even extensive learning about privacy will still not be enough. For example, I consider myself a privacy expert, having studied and written about privacy for more than twenty-five years, and I do not know enough to confidently determine whether I should share information about my life on Facebook, whether I should use a smart doorbell, whether I should use a home assistant device, or whether I should reveal my location to many apps.

To accurately assess the privacy risks for providing data to most organizations, I would need to speak at length with their chief privacy officer or

[122] *See generally* Hideyuki Matsumi, *Predictions and Privacy: Should There Be Rules About Using Personal Data To Forecast the Future?*, 48 CUMB. L. REV. 149 (2018) (discussing data privacy law's treatment of "predictive information"); Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357 (2022) ("Contemporary information privacy protections do not grapple with the way that machine learning facilitates an *inference economy* in which organizations use available data collected from individuals to generate further information about both those individuals and about other people."); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494 (2019) (arguing GDPR protections are insufficient to address inference data).

[123] Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 444 (2020).

data protection officer, review their data transfer agreements, review their privacy impact assessments, question the engineers about their technology, see a data map and understand how data is stored, combined, and transferred, review any algorithms that are making decisions about me as well as the data that the algorithms are being trained on, review their specific data security safeguards and how well they are being implemented, examine any internal privacy assessments, see how effective their training is on privacy and data security, and on and on.

Even if I could obtain all this information, I lack the time to review it all for one organization, let alone thousands. In my own privacy decisions, my expertise has taught me that my decisions are based on a wild guess. I lack sufficient information about how these organizations protect my privacy; what I know is how much I don't know.

D. *Cognitive Limitations*

As I have explored elsewhere, people lack the cognitive ability to engage in good cost-benefit analysis of future uses and sharing of their data.[124] When people are presented with a choice about whether to allow the collection or use of their personal data, the benefits are often immediate and concrete. If people consent, they gain access to information, services, products, games, discounts, fun activities, videos, and other dopamine-generating wonders. People gain time-saving conveniences and magical new technologies that dazzle and delight. The costs are harder to determine because they are in the future and are highly uncertain. It is difficult for people to turn down instant bliss for some vague and abstract potential harm in the distant future. People struggle to evaluate risks of harm in the future.[125] People have a "human tendency to favor short-term over long-term consequences."[126] People also have an optimism bias, where they "overestimate the likelihood of positive events, and underestimate the likelihood of negative events."[127]

For example, suppose a person is asked to consent to allowing an online retailer to track her activity on its website to deliver personalized advertisements. For this, the person is offered a 10% discount at the store. The benefit is immediate. The costs are unclear. How is the person to assess the costs? When making the decision, the person does not think she is shopping for anything embarrassing that she wants to conceal. But the decision is not one that people spend months ruminating on; it is made quickly. The person often can't readily conceive of all the potential items she will look at on the website. Nor will the person be able to know how various algorithms might analyze the data. That analysis might yield unexpected and unwanted revelations about the person; or

[124] Solove, *Privacy Self-Management*, *supra* note 7, at 1891-93.

[125] Richards & Hartzog, *supra* note 25, at 1484 (noting people are "far too optimistic" and "discount future costs too much" when assessing possible future risk).

[126] NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 60 (2019).

[127] Tali Sharot, *The Optimism Bias*, 21 CURRENT BIOLOGY R941, R941 (2011).

it might make predictions about the person's future behavior that the person does not agree with and finds troubling or offensive. To make a cost-benefit calculation, the person would need to know the algorithm and how it works. But the algorithm is far too complex for most lay people to understand.

Additionally, to truly understand how the algorithm will work, a person will need to know not only the logic of the algorithm, but also all the other data fed into the algorithm, as many algorithms look for patterns across an entire data set of many people.

In short, there really is no way to make a good cost-benefit analysis. Individuals consent based on wildly speculative hunches, uninformed gut feelings, or immediate impulses. People often can't imagine what could go wrong. As Cameron Kerry argues, "individual choice becomes utterly meaningless as increasingly automated data collection leaves no opportunity for any real notice, much less individual consent."[128]

Even more generally—and quite depressingly—many people are simply not up to the task of making privacy decisions, no matter how high the stakes. People are ill-informed and do not want to take the time to become more educated. Even when educated, people fail to retain enough information to make wise decisions. People lack clear goals and clear thinking.[129] They are unable to escape cognitive biases. They "often make decisions with little information or deliberation."[130]

E. *Structural Limitations*

Several structural limitations plague people's ability to provide meaningful privacy consent. These problems stem from how consent choices are structured. Many situations involving consent involve inadequate choices. Other situations involve too many choices, which overwhelm people with complexity. Although in some circumstances a middle ground can be found that will satisfy Goldilocks, in many cases there is no satisfactory porridge.

1. Inadequate Choices

Many consent choices presented to individuals involve an inadequate set of choices. In U.S. privacy law, often the choices are binary—either opt in/out or not. In many cases, the choice is to either do business with a company and accept all of its privacy practices or not do business with the company at all. There is no option to opt out of each particular practice. The same holds true for opt in. Under many circumstances, the choice is all or nothing.

---

[128] Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How To Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/U5MV-CXSJ].

[129] BEN-SHAHAR & SCHNEIDER, *supra* note 100, at 109 ("People have poorly defined goals about most problems, and no plausible amount of thinking will define them sharply.").

[130] *Id.* at 64.

With privacy, people are often presented with take-it-or-leave it choices; they cannot negotiate. Julie Cohen critiques such consent mechanisms as hollow because "[u]sers remain unable to demand or specify changes in the basic conditions of information processing or the design of networked services."[131]

For people to meaningfully consent to the collection and processing of their personal data, they should know how their data will be protected. What people are told in privacy notices are vague meaningless statements such as "your privacy is important to us," that personal data is shared only with "trusted third parties," that the data is protected by "reasonable security safeguards," and so on. But what it means to protect privacy is intricate and wide-ranging. Privacy involves the quality of the internal governance program and how well privacy is integrated into the design of products and services, among many other things. Rarely is much information provided about these matters in privacy policies. Privacy depends significantly on the quality of the contractual relationships with third parties that process data on behalf of an organization, but people do not see these contracts before consenting. People know little about how third parties are vetted or monitored for compliance. As for data security, people know hardly anything about the quality or type of security measures, or the security of all the third parties that receive the data.

It is hard to imagine privacy law demanding that organizations lay bare their privacy programs, vendor contracts, privacy impact assessments, and other things. People would be swamped with information. Instead, the law settles for the fiction that providing vague generalities that people must either take or leave is somehow presenting them with a meaningful choice.

2. Too Many Choices

The flip side of not enough choices is too many choices. Too granular an approach is overwhelming. Yet the GDPR requires consent to be quite granular and specific. According to the EDPB, "[c]onsent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'."[132] Specificity means that consent for various purposes requires "a separate opt-in for each purpose."[133]

Organizations can process various types of personal data for a multitude of different purposes. If people are asked to consent at a high degree of granularity and specificity, then they will drown in a sea of endless consent requests.

Privacy choices at many companies have become more granular. Social media settings, for example, used to have a few choices, but now they have more settings than an airplane cockpit. A cost of this trend is that privacy choices are

[131] 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/3G59-GJZQ].

[132] EUROPEAN DATA PROT. BD., *supra* note 30, ¶ 60.

[133] *Id.*

overwhelming and perplexing. For example, as Luiza Jarovsky observed regarding a social media app's privacy settings:

> I have been studying privacy for years, I consider myself a tech savvy person, I use this app since it was launched, I am a millennial and . . . I have difficulty navigating these settings. I do not know where I should click to get to what I need. I get lost with the amount of choices I must make and they seem confusing and misplaced.[134]

Presenting people with so many choices might be appropriate because privacy is complex and does involve many choices. But it can make consent more onerous and lead to mistakes. In one study, participants who had to choose among "a larger amount of privacy options" reported "more negative feelings, experience[d] more regret, and [were] less satisfied with the choices made."[135] Studies in other contexts generally show that people with a moderate number of choices rather than a large number "are likelier to make a choice and to be more confident and happier about it."[136] As Nancy Kim observes, "[m]ore information may fail to improve and may even impair decision-making ability. Psychological studies show that for humans, attention is a scarce resource, and complex information may escape a decision-maker's notice."[137]

Navigating the Scylla of too few choices and Charybdis of too many is a tremendously challenging task. And if a particular organization somehow manages to get it right, another problem remains—none of this scales. I address this issue in the next Section.

F. *The Problem of Scale and Consent Fatigue*

Obtaining informed consent for every activity involving privacy is impractical. Too much effort must go into educating people, and there are so many decisions that the effort would put people into a permanent privacy school (with no summer recess).

Using the express consent approach is doomed because obtaining such consent does not scale. Thousands of organizations collect, use, and transfer an individual's personal data, so individuals would be deluged with countless requests for consent. In addition, each organization might engage in a wide array of different activities involving personal data at different times, so they would

---

[134] Luiza Jarovsky, *Privacy Settings Are Too Complicated. Here Are Some Ideas on How To Change Them*, MEDIUM (July 11, 2022), https://luiza.medium.com/privacy-settings-are-too-complicated-here-are-some-ideas-on-how-to-change-them-1b1267e7523c [https://perma.cc/NH99-ZP9E].

[135] Stefan Korff & Rainer Böhme, *Too Much Choice: End-User Privacy Decisions in the Context of Choice Proliferation*, *in* USENIX SOUPS 2014: PROCEEDINGS OF THE TENTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 69 (2014).

[136] BEN-SHAHAR & SCHNEIDER, *supra* note 100, at 104-05 (summarizing study findings regarding how people feel about "choice overloading" in general).

[137] KIM, *supra* note 126, at 13.

be issuing a stream of consent requests. The result is a tremendous and unwanted burden hoisted upon the individual.[138]

In 2008, Aleecia McDonald and Lorrie Cranor studied privacy notices and noted that the average length was 2,514 words.[139] More recent studies have indicated that the lengths of privacy policies have grown. The average length of the privacy policies of the twenty most-used apps in 2018 was 3,964 words—58% longer than those examined a decade earlier by McDonald and Cranor.[140] Consider the trend in Google's privacy policy. According to *The New York Times*, "Google's privacy policy evolved over two decades—along with its increasingly complicated data collection practices—from a two-minute read in 1999 to a peak of 30 minutes by 2018."[141] In 2022, an analysis of 50,000 privacy policies revealed that during the past twenty-five years, they grew by more than 4,000 words on average.[142] This trend is unsurprising—data collection and use has become more extensive and complicated, so it can't readily be explained simply and concisely.

The EDPB notes that under the GDPR, data subjects may encounter a "certain degree of click fatigue" if they "receive multiple consent requests that need answers through clicks and swipes every day."[143] The negative consequences of click fatigue are that the "warning effect" of consent mechanisms diminishes and that "consent questions are no longer read."[144] Although noting the problem, the EDPB provides no solution beyond stating: "The GDPR places upon controllers the obligation to develop ways to tackle the issue."[145]

Privacy laws can become too formalistic in requiring consent, creating a meaningless and often annoying chore for people in responding. For example, the GDPR's consent rules require websites to display cookie notices, known as

---

[138] Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551, 561-62 (2023).

[139] McDonald & Cranor, *supra* note 26, at 554. The study also noted that reading privacy notices "carries costs in time of approximately 201 hours a year." *Id.* at 565.

[140] Pierre-Nicolas Schwab, *Reading Privacy Policies of the 20 Most-Used Mobile Apps Takes 6h40*, INTOTHEMINDS CONSULTING BLOG (May 28, 2018), https://www.intothe-minds.com/blog/en/reading-privacy-policies-of-the-20-most-used-mobile-apps-takes-6h40/ [https://perma.cc/RB3A-9T97] (summarizing study findings).

[141] Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*., N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[142] Chris Stokel-Walker, *Privacy Policies Are Four Times as Long as They Were 25 Years Ago*, NEW SCIENTIST (Feb. 3, 2022), https://www.newscientist.com/article/2307117-privacy-policies-are-four-times-as-long-as-they-were-25-years-ago/ (summarizing study findings).

[143] EUROPEAN DATA PROT. BD., *supra* note 30, ¶ 87.

[144] *Id.* ¶¶ 87-88.

[145] *Id.* ¶ 88.

"cookie banners."[146] These notices end up creating aggravation and annoyance. They rarely provide any meaningful protection; people just click "accept cookies" to make the cookie banners go away. Excessive consent requests can become obnoxious and unhelpful; they give privacy regulation a bad reputation, as many people start to think of privacy laws as interrupting nags.

The timing of consent requests is often inopportune. Consent is requested at times when people are often not interested in thinking about privacy. People are eager to use new technologies, read information on websites, play games, watch videos, and so on. At these times, they often don't want to take a long detour to mull over privacy. People will even consent just to make annoying consent requests go away so they can proceed to what they want to do or see.

One oft-touted solution to the problem of scale when it comes to privacy self-management is to automate consent. Various failed attempts have been made at automating privacy consent, such as P3P and the Do Not Track ("DNT") option on browsers,[147] which started off with fanfare but later fizzled into irrelevance.[148] A reboot is being attempted through "Global Privacy Controls" ("GPC") via the CCPA.[149] It remains to be seen if this will prove successful.

Privacy is likely too contextual and nuanced to be readily automated. Of course, if one's choice is not to consent to anything, it can be easy to carry out that choice broadly. But if a person truly wants to understand and weigh the risks and benefits of consenting to various types of data collection and processing, it is hard to imagine how these decisions could readily be automated. Decisions about data sharing are contextual and risk based. They cannot be determined in a vacuum or in a one-sided manner. Risk decisions require estimates of likelihood and involve a balancing between risk and reward. High risks can be outweighed by significant benefits. Risk also involves likelihood and gravity of harm, so there are situations of high likelihood and low gravity and ones of low likelihood and higher gravity. How a person decides for each risk turns on the circumstances. It remains unclear how an automated global system can make these determinations well; most likely, a simplistic one-size-fits-all decision will be made.

Obtaining consent often is impractical for many instances of data collection, processing, and disclosures. There are too many such instances that data subjects would be overwhelmed by consent requests. Pinging people constantly for consent becomes an annoyance. With hundreds or thousands of organizations

---

[146] *See, e.g.*, *10 Effective GDPR Cookie Consent Examples*, COOKIEYES (Sept. 1, 2023), https://www.cookieyes.com/blog/gdpr-cookie-consent-banner-examples/ [https://perma.cc/F9QX-H6JJ].

[147] Goldman, *supra* note 47, at 12-13 (discussing pros and cons of "delegating the work of reviewing online terms to digital agents").

[148] Jones & Lee, *supra* note 25, at 102 ("[T]he U.S. and the EU have both failed to legally enforce a DNT signal.").

[149] California Consumer Privacy Act Regulations, CAL. CODE REGS. tit. 11, § 999.315(c)(2) (2023).

pestering people repeatedly, consent requests can become overwhelming to the point of being abusive. Faced with so many requests for consent, people will be unable to give each request the time and thought needed to make wise decisions. As people become overwhelmed by a tsunami of consent requests, their deliberation on it likely diminishes, and the consent loses any meaning—if it ever had any. Ironically, the more that privacy law relies on consent, the less reliable consent becomes.

Ultimately, trying to make consent more rigorous leads to "consent fatigue."[150] When inundated with consent requests, people tune them out or quickly consent just to make them go away. Ella Corren aptly describes responding to consent requests as a "burden."[151] Cameron Kerry argues: "In a constant stream of online interactions, especially on the small screens that now account for the majority of usage, it is unrealistic to read through privacy policies. And people simply don't."[152]

One way to address consent fatigue might be to increase the scope of consent so that it covers a wider range of processing activities and lasts for a longer duration. But as William McGeveran notes, making consent more "frictionless" carries significant risks—people might share more personal data and take on risks that they do not want to take on.[153] For example, the U.S. Video Privacy Protection Act ("VPPA") required people to consent for disclosing data about each video that they watched.[154] Netflix wanted to make it easier to share data about people's video watching on social media sites, so Netflix lobbied Congress to amend the VPPA.[155] Congress rushed to Netflix's aid, allowing a blanket consent that can include all of the videos a person watches for two years.[156] McGeveran argues that this frictionless sharing can lead to instances in which people end up disclosing more information than they expect.[157] When deciding to consent for each particular video, people are more inclined to think about the implications for consenting to each one. With the blanket consent, people might not consider that there are some videos they might not want to disclose. The

[150] Rishab Bailey, Smriti Parsheera, Faiza Rahman & Renuka Sanea, *Disclosures in Privacy Policies: Does "Notice and Consent" Work?*, 33 LOY. CONSUMER L. REV. 1, 3 (2021) (noting "structural issues such as the presence of too many entities processing personal data impose a burden" on users).

[151] *See generally* Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551 (2023) (coining and examining "consent burden" phenomenon).

[152] Kerry, *supra* note 128.

[153] William McGeveran, *The Law of Friction*, 3 U. CHI. L.F. 15, 39-46 (2013) (arguing "frictionless" disclosures "can harm [user] dignity, autonomy, and serenity" through "loss of individual control").

[154] 18 U.S.C. § 2710(b)(2) (2006) (amended by Pub. L. 112-258) (requiring "informed, written consent of the consumer given at the time the disclosure is sought").

[155] *See* McGeveran, *supra* note 153, at 26-27.

[156] Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (2013), codified at 18 USC § 2710(b)(2)(B).

[157] McGeveran, *supra* note 153, at 39-43.

result can be disclosures that people ultimately regret. Thus, McGeveran argues, "friction" can be good, as it involves "forces that impede individuals from disclosing personal information when they use online services."[158] Consent that has a wide span or that is relatively frictionless can be less reflective of a person's desires. People also might end up allowing more data collection and processing than is in their self-interest.

But there is a challenging tension because friction leads to consent fatigue. Many people might not want to be bothered by constant consent requests. Many people might not want to think about privacy constantly or even for a little time.

Some commentators argue that the fact that many people do not want to think about privacy means they do not care about privacy. They invoke what is called the "privacy paradox" to contend that people's consent validly reflects their lack of concern about privacy. But as I have argued elsewhere, the privacy paradox is a myth.[159] That people fail to think about privacy does not indicate they do not care. People often do not want to think about things they care deeply about at a particular moment in time. More generally, as Omri Ben-Shahar and Carl Schneider note, "[p]eople are, loosely and broadly, decision averse."[160] People find many decisions to be unpleasant and laborious. Many people do not want to be educated or informed; they simply do not want to decide. And perhaps people are not wrong in evading decisions they are often too ill-equipped to make.

III. MURKY CONSENT: A NEW APPROACH

Despite the intractable problems with privacy consent, there is a push to have more laws require express consent and opt in. Reforms involve more transparency, more individual privacy rights, and more attempts to give individuals control over their data. These approaches are doomed.[161] Even under the gold standard of informed consent, privacy consent will fail—there are just too many circumstances requiring consent for it to scale and it is becoming too difficult to understand how personal data will be used. There is no good solution because people just cannot understand enough to meaningfully consent.

Should privacy law abandon consent? One approach might be to have the government determine how people can share their personal data and how that data can be processed. But this approach can readily become too controlling. If the law were to forbid or override consent whenever consent was tainted with difficulties, then people would rarely be free to make their own decisions. People often make bad decisions; they rarely know enough; they rarely deliberate enough; they decide based on a litany of cognitive biases that can readily be

[158] *Id.* at 15.

[159] *See generally* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1 (2021) [hereinafter Solove, *The Myth of the Privacy Paradox*].

[160] BEN-SHAHAR & SCHNEIDER, *supra* note 100, at 61.

[161] Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 984-93 [hereinafter Solove, *The Limitations of Privacy Rights*].

exploited; and they are often coerced or manipulated. Because of these ugly truths, the law would need to micromanage nearly every instance of collection, use, and disclosure of personal data. The law would become overly controlling.[162] It would also be nearly impossible to develop a legal framework to govern the countless situations involving privacy, especially with such dynamic and evolving practices.

Respect for people's autonomy gives them space to make informed choices based on their determination of what is in their own self-interest. The problem is that for privacy, people's decisions are often highly manipulated and ill-informed. People frequently make choices that are unhealthy, risky, unwise, and not in their own interest. In many cases, people poorly assess what effect things will have on their future happiness.[163]

Even accepting that these problems can never be surmounted, respect for autonomy involves preserving space for individual choice, as unsound and compromised as it often is. As Nancy Kim aptly notes: "Humans are flawed, and our optimism bias, myopia and other cognitive and emotional limitations cause us to mispredict and misjudge future events . . . . These human limitations should not be used, however, as a justification to deprive individuals of decision-making authority."[164]

Many times, the law validly curtails people's choices, such as banning dangerous drugs or products. But in most cases, the law provides people with a large zone in which they can decide for themselves, even when their decisions may be foolish and wrong—and even when undue influence and manipulation can't be fully prevented. The law's respect for autonomy has a potent and durable moral foundation, which is why consent plays such a powerful role in the law.

But how can the law protect what is in an individual's self-interest and respect an individual's freedom to choose when we know individuals can't make many privacy choices in their own self-interest?

We are thus left with the consent dilemma. Consent doesn't work, but not having consent also doesn't work. The law copes by manufacturing fictions of consent of various degrees of absurdity. We are trapped in a Kafka story. Is there any way out?

---

[162] Perhaps the law would not be more controlling than the current status quo, as people currently lack sufficient autonomy in making decisions about their personal data. Promoting autonomy might be an illusory goal. Nevertheless, the law might still work best by preserving space for autonomy, even if autonomy is in grave doubt. Law without space for autonomous decisions presents concerns for free will. Even if free will were fictional, there might still be value in embracing this fiction.

[163] *See generally* DANIEL GILBERT, STUMBLING UPON HAPPINESS (2006). *See also* Douglas Husak, *Paternalism and Consent*, *in* THE ETHICS OF CONSENT, *supra* note 39, at 107, 115 (Franklin G. Miller & Alan Wertheimer eds., 2010) ("Economists have come to appreciate that few of us are very proficient at maximizing our own happiness or utility.").

[164] KIM, *supra* note 126, at 64.

In this Part, I contend that there is a way out. But the path is in a counterintuitive direction. Rather than try to make consent less fictional, we should embrace its fictions. I propose a new approach to privacy consent that I call "murky consent."

A. *Leaning into the Fictions*

For a long time, making consent more express, affirmative, and clear has been the ideal. The goal has been to turn consent from fiction to fact, to make consent live up to the myth. Unfortunately, the cruel irony is that efforts to improve consent frequently make it worse. For example, the editors of *The New York Times* wrote an op-ed critiquing opt-out approaches and declaring that "[u]sing an opt-in approach will help curb the excesses of Big Tech."[165]

But opt-in has a downside that is often overlooked—it emboldens organizations to collect and process personal data because it is perceived as a clearer form of consent than opt out, which is more dubious. Similarly, if the barter of personal data for free products and services were more explicit, this would be better in some ways but far worse in others. It would certainly be more transparent. People would realize that many apps and websites are not free; they would learn that they are in essence selling their data for all the free products and services they enjoy. But such an approach could give organizations a greater sense of entitlement to use data more aggressively because they purchased it. In contrast, with a cloudier consent method, such as the notice-and-choice approach, organizations might be more cautious in using data because of the greater ambiguity of consent.

Could contract law come to the rescue and make privacy consent meaningful? As Brian Bix notes, "consent, in terms of voluntary choice, is—or at least appears to be or purports to be—at the essence of contract law."[166]

Perhaps aggressive application of contract law to privacy notices might add formalities and protections that are now lacking. But as Allyson Haynes aptly argues, privacy policies often do not provide consumers with protections "they would not have had absent the policy," and some even create "greater leeway to use personal information."[167] Companies can readily include terms in privacy policies that are unfavorable to consumers.[168] She concludes: "Rather than providing consumers the protection they expect, privacy policies have become one more online contract of adhesion for consumers to avoid."[169] The more formal the situation involving consent becomes, the more legitimacy and legal

---

[165] Opinion, *America, Your Privacy Settings Are All Wrong*, N.Y. TIMES (Mar. 6, 2021), https://www.nytimes.com/2021/03/06/opinion/data-tech-privacy-opt-in.html.

[166] Bix, *supra* note 58, at 251.

[167] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information*, 111 PENN. ST. L. REV. 587, 609 (2007).

[168] *Id.* at 612 (suggesting website operators will respond to lack of substantive privacy protection with unfavorable consumer terms in policies).

[169] *Id.* at 624.

power is conferred to organizations seeking consent to collect and process personal data. Formalities such as contract law or express consent mechanisms will not turn privacy consent's fictions to fact, but they will add power to the fictions.

Contract law, however, also struggles with consent.[170] As Brian Bix points out, there is a debate in contract law between whether a subjective or objective approach to consent should be taken. Under the "internal" or "subjective" approach, the law should look to whether a person consented by focusing on "state of mind, preferences, [and] volition."[171] Under the "external" or "objective" approach, the law should focus on observable indicia of consent.[172] Randy Barnett, for example, takes the latter approach, contending that a contract should be enforced based on the voluntary performance of acts that convey an "intention to create a legally enforceable obligation."[173]

As David Hoffman observes, contract law has strained to adjust to a world where contracts have grown exponentially.[174] We have moved from a world where people made contracts in person to a digital realm where people agree by clicking buttons. As Eric Felten notes, "most of us make more legal agreements in a year than our grandparents made in a lifetime."[175]

With so many contracts, the subjective approach becomes more impractical compared to the objective approach. Bix sides with the objective approach because he views the subjective approach as too idealistic; it could send modern commercial activity into chaos. The subjective approach would open a Pandora's box of questions about the countless contracts underpinning commerce today, turning the ground to quicksand.

Even under the objective approach to contract formation, for consent to have any meaning, there must be valid objective indicia of consent. But such indicia are lacking with so many modern contracts, especially terms of service. These contracts are based on fictions, which allow for the legitimacy and moral force of consent without the existence of consent.

Ultimately, any legitimacy and moral force supplied by fictions are unwarranted.[176] Contract law thus lacks the answers; it just poses more questions. It does not present privacy law with a usable approach to consent.

---

[170] *See* RADIN, *supra* note 52, at 19-32; Bix, *supra* note 58, at 252.

[171] Bix, *supra* note 58, at 252.

[172] *Id.* at 252-53.

[173] Randy E. Barnett, *A Consent Theory of Contract*, 86 COLUM. L. REV. 269, 300 (1986).

[174] Hoffman, *supra* note 51, at 1604-05.

[175] Eric Felten, Opinion, *Are We All Online Criminals?*, WALL ST. J. (Nov. 18, 2011), https://www.wsj.com/articles/SB10001424052970203699404577044213438024248.

[176] For example, as Elettra Bietti writes, "the ideal of autonomous consent cannot be reached in practice in the platform economy because the conditions which constitute consent as a morally transformative device are absent." Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE L. REV. 308, 313 (2020).

Attempts to improve privacy consent will fail to make it less fictional. Instead, these efforts just dress up the fictions and give them more legitimacy. Privacy consent already has far too much unwarranted legitimacy; it does not need more.

B. *Murky Consent*

Rather than try to fix privacy consent to make it live up to its fictions, the law should take a different approach—one that might seem radical at first because it points in the opposite direction of most proposed solutions. Privacy law should accept that privacy consent is fictional and embrace this reality. The law should thus *lean into the fictions* by stopping pretending that they are true. Privacy consent is inescapably fictional, and it works best as a set of fictions. The problem is not the fictionality of consent; it is the desperate attempt to deny and repudiate this reality.

I propose that privacy law should recognize a new form of consent that exists in the gray middle ground between full consent and nonconsent. I call the consent in this zone "murky consent" because it is highly ambiguous and dubious. This form of consent would lack the legitimacy of full consent. Murky consent would operate as a limited and weak license to use personal data.

Stripping legitimacy from consent should correspondingly limit the power of consent and the scope of the collection, use, and disclosure of personal data that it authorizes. Rather than try to peddle fiction as fact, the law should openly acknowledge that murky consent is fictitious, yet accept it as a necessary lie because the machinery of the digital economy must be lubricated by lies.

1. Lessening Consent's Legitimacy: Beyond the Binary

The law often treats consent as a simple binary—either people consent, and this opens up a license to use personal data in a myriad of ways, or people don't consent. This is far too simplistic a set of options. Consent is far more complicated than the simplistic binary in the law. Of course, law is by necessity a simplification of the vast complexities of life. Rules can't capture life in all its multifarious nuances. But the law must also avoid being so crude that it operates like a caveperson with a club.

Consent is often ambiguous and should be treated as such. Consent exists in many shades of gray. As Nancy Kim argues, the "nature of consent itself is not fixed, but complex and dynamic," and should be understood as "less a threshold to be crossed than a sliding scale which can be (and should be) adjusted depending upon the context."[177] Kim also correctly notes that "[p]erfect consent is rare, perhaps even unattainable," and that law's approach to consent "must reflect realistic assumptions about human intent and behaviors, not idealized ones."[178]

Consider cookie consent and the GDPR. On the surface, a happy story can be told about the GDPR and cookies. After the GDPR, more people were informed

[177] KIM, *supra* note 126, at 74, 81.

[178] *Id.* at 117-18.

about cookies and more people accepted them. But below the surface, there is a more sinister story; people are not suddenly consenting more to cookies. They are clicking to make the cookie pop-up go away. This illusory consent is worse than the canard behind the notice-and-choice approach. Nobody really accepts the lie that failing to opt out indicates consent whereas opt in appears more legitimate. The opt-in consent for cookies is still a fiction, but it has an attitude—perhaps even a swagger. Organizations now have the cover of documented express consent, a potent instrument that might embolden them to do more with the data.

In contrast, with the notice-and-choice approach, cookies exist in a gray zone. They are not legitimate because they are not consented to, yet they still are used. The status of cookie data is uneasy, a no man's land where every step is treacherous, where caution is best used when processing data. This kind of murky world is a feature, not a bug.

In most situations involving technology and personal data, consent can never truly be meaningful, and the law is making things worse by pretending that it is. There is a wide spectrum between full informed consent and nonconsent, and most situations involving privacy fall somewhere in the middle. Murky consent should not confer the same legitimacy as full consent. Rather than provide wide-ranging freedom to gather and use data, murky consent should provide a limited and highly restricted license. This approach to consent would be far more consistent with the world we live in. Ironically, embracing privacy consent's fictionality is the most realistic thing the law can do.

Consent will be murky in most situations involving the collection and use of personal data by private and public sector organizations. Although situations involving clear consent are possible in some circumstances, the vast majority of cases will involve murky consent.

2. Weakening Consent's Power

Because murky consent lacks much legitimacy, it should not bestow the same degree of power that consent currently grants. Many privacy laws already require limits on the scope and duration of data collection and retention to what is necessary for the purposes of use. Consent is revocable under many laws, such as the GDPR. These components are essential; any law that lacks them is deficient. For example, revocability ensures that there always is a backstop; consent may be quite dubious, even almost nonexistent, but revocability at least guarantees that there is always a way out, that people always have a choice.

Beyond these restrictions on scope and duration, the law must significantly weaken murky consent's power. To do this, the law must impose a series of duties to promote the integrity of privacy consent's fictions. If the law is pretending that people consent, then the pretense should be plausible. Murky consent should be invalid if it is a bad deal for people. If the law is imagining that people are consenting, then the law should require that what they are consenting to is actually good. To put it another way, we can't escape the fact

that privacy consent is a fictional story, but we can demand that the story end happily ever after.

For murky consent, the law should impose the following duties:

- *Duty to Obtain Consent Appropriately.* The method for obtaining murky consent must vary proportionately with the risk. Murky consent cannot be obtained fraudulently or unethically.
- *Duty to Avoid Thwarting Reasonable Expectations.* Murky consent shall be invalid whenever it thwarts people's reasonable expectations about how their data will be collected, used, or disclosed.
- *Duty of Loyalty*. The entity seeking murky consent must put the interests of individuals before its own interests.
- *Duty to Avoid Unreasonable Risk*. Murky consent shall be invalid if it involves an unreasonable risk of harm to individuals, their rights, interests, or welfare. Murky consent shall also be invalid if it creates an unreasonable risk of harm to society.

a. *Duty To Obtain Consent Appropriately*

In the fictional story of consent, the law must ensure that the beginning is credible. Although nearly all mechanisms to obtain privacy consent are highly flawed, this does not mean that stronger mechanisms to obtain consent lack any benefit. The *Duty to Obtain Consent Appropriately* recognizes that although most means of obtaining consent are deeply flawed, they are not all equal. The law should require more rigorous ways of obtaining consent when the risks are higher. For low-risk situations, notice-and-choice might be appropriate. Many people do not want to be bothered by opting in, and if the risks are low, forcing cumbersome means to obtain consent is counterproductive. Making people consent to everything trivializes consent and makes people less likely to take consent seriously when it really matters.

As the risk increases, the means to obtain consent should strengthen. Opt in consent should be required when there are greater risks. In situations of high risk, even more stringent methods should be used, such as pop-up warnings and measures to slow people down so they do not make snap decisions. Of course, as I argued earlier, even these stronger means of obtaining consent do not turn consent from fiction to fact. But these requirements add useful resistance to the ability to collect and use personal data, and this resistance increases the cost of riskier uses of data. Even with this resistance, consent would still be murky.

Although murky consent is dubious and ambiguous, it should not be fraudulent. Murky consent must not be obtained through manipulation, bad faith, trickery, or other problematic methods. Consent is a fiction, but there are different degrees of plausibility in fiction, from poetic license to outright charade. Murky consent is fictional but it should not be farcical.

b. *Duty To Avoid Thwarting Reasonable Expectations*

The *Duty to Avoid Thwarting Reasonable Expectations* aims to ensure that people's data is used consistently with what they might reasonably expect. If consent is a fiction, it should be a *plausible* fiction, one that strives to reflect realistically what people would actually consent to if they were able to do so.

Organizations should have a duty to avoid thwarting *reasonable* expectations, not actual expectations, which could be nearly anything. Reasonableness is itself a fiction—it is a standard of care based on an idealized account of common social norms and practices. The gathering and use of personal data must be consistent with these norms. Deviations from reasonable expectations fall outside the scope of murky consent. If organizations want to deviate, they must either find a way to obtain actual consent, which will be quite difficult, or find another basis to collect and use personal data other than consent.

Ensuring that people's reasonable expectations are respected aims to prevent situations where people unwittingly consent to things they wouldn't want if they were truly informed. According to a study led by Nathan Good, when people were informed about the online contract terms to which they purportedly agreed, they often regretted their decision to accept the terms.[179]

If enforced rigorously, this duty can serve as a significant constraint on the collection, use, and transfer of personal data. For example, under many privacy laws, if an organization wants to use people's data in new ways (such as to train AI algorithms), it can just insert a statement about it into its privacy notice or create some form of disclosure that people must accept. With either notice-and-choice (opt out) or express consent (opt in), many people would consent to it. If this use is not reasonably expected, then putting it in the privacy notice would be insufficient for murky consent no matter which approach to consent were used.

c. *Duty of Loyalty*

The *Duty of Loyalty* aims to prevent organizations from putting their own interests ahead of the interests of individuals.[180] As I have argued elsewhere, the law should hold that organizations that collect and process personal data about individuals stand in a fiduciary relationship to them.[181] Fiduciary relationships are ones where there is a significant power difference between parties in a relationship, and this power differential justifies imposing special duties on the party with the greater power. The general concept of the fiduciary relationship is that there is a responsibility of the powerful party to look out for the interests

[179] Nathaniel S. Good et al., *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, *in* ACM, SOUPS '05: PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY 43, 50 (2005).

[180] For more background and a theory of a duty of loyalty, see Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021).

[181] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 102-03 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON].

of the other party and not capitalize on its position of heightened power.[182] The use of fiduciary duties to govern the relationships between powerful organizations and individuals has been embraced by many scholars, including Jack Balkin, Neil Richards, Woodrow Hartzog, Lauren Scholz, Ifeoma Ajunwa, and others.[183]

Under this approach, for example, requirements that people waive rights to sue or agree to arbitration would be invalid unless arbitration could be carried out in ways that do not diminish consumer rights and power.[184] As Margaret Jane Radin aptly argues, these are coercive attempts to eliminate rights guaranteed to people by the state for the sole benefit of companies.[185]

d. *Duty To Avoid Unreasonable Risk*

The last component, the *Duty to Avoid Unreasonable Risk,* is framed around the reasonableness of a risk rather than more abstractly on how high a risk might be. The law should not try to protect against all risk; there is risk in everything. Nor is there an ideal level of risk. Risk is relational. Society accepts different risk tolerances for different activities. A high risk might be reasonable if undertaken for a high reward that is socially beneficial. A lower risk might be unreasonable if there is no corresponding benefit.

The law routinely allows certain risk taking and disallows other risk taking. A person can consent to be a firefighter but cannot consent to be put at risk by flammable products. In a supermarket, people consent to buying food that might be unhealthy, but they cannot consent to tainted food. The law must strike a balance between autonomy and protecting people's welfare. When the risks become unreasonable, consent becomes even more dubious and should not be recognized even as murky consent. The law must be careful to avoid spurning autonomy in a zeal to protect individuals. Unreasonable risks are not situations that are merely disadvantageous to individuals. Even reasonable people take such risks, as evidenced by the popularity of lotteries. The goal of murky consent is not to invoke the nanny state through the backdoor. Instead, the goal is to

[182] *Id.*

[183] *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016) (reconciling opposed interests of need for regulation and First Amendment freedoms); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 144 (2020) (arguing consumer interactions should create fiduciary relationship between consumers and companies); Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 987 (2022) (discussing scholarly proposed duties of loyalty, partially in form of information fiduciaries); Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 CARDOZO L. REV. 1671, 1720-26 (2020) (critiquing fiduciary relationship analogy and arguing hiring platforms should be considered fiduciaries).

[184] Although I am skeptical of arbitration, I am not ready to claim that litigation would always be preferable to arbitration.

[185] RADIN, *supra* note 52, at 33.

respect autonomy but impose limits on how much individual foibles, gullibility, shortsightedness, and poor decisionmaking can unduly harm them.

Murky consent should also be invalid when it could cause unwarranted societal harm.[186] The law tolerates a widescale freedom in contracting, but it does not allow all transactions, even if consensual. Certain rights are inalienable. Contracts can be void for public policy when they involve certain immoral, troublesome, or dangerous acts—even if desired by individuals.[187] Privacy is not solely an individual interest; it has a social value and is vital to a free and democratic society. This fact does not mean that privacy should be inalienable; but when one person's choices affect others or cause damage to society, there is a societal interest that must be considered.

Contract terms such as requiring individuals to waive rights to litigate in the event of wrongdoing not only hurt individuals but also undermine the rule of law, a larger societal harm. As Radin argues, "[i]f enough cases come to be subject to binding, secret, ad hoc, nonprecedential arbitration, the common-law legal system of precedent would, at least as regards consumers, cease to exist in practice."[188] Beyond the fact these rights waivers are solely benefitting organizations and not individuals, the societal harm these provisions cause should be another reason to reject them as a basis for murky consent.

*****

The murky consent approach aims for a fictional story with integrity. If the law allows for the fiction that people consent, then the law should also ensure that people's consent is actually good for them. The duties discussed above would restrict common practices such as burying problematic data uses in lengthy privacy notices, having vaguely defined uses that allow organizations to do nearly anything they want, or enticing people to consent to uses that are beyond what is reasonably expected or that create an unreasonable risk of harm.

The duties I have sketched out aim to limit the power of murky consent and ensure that people are protected from harmful practices. In essence, leaning into the fictions of consent means imagining a world where people could really provide meaningful consent, then asking: *If such an imaginary world existed, what would people actually consent to?*

These duties are a start, not a guarantee of sufficient protection for all situations involving murky consent. This disclaimer aside, these duties provide basic guardrails that should provide strong protection in many circumstances.

---

[186] In her approach to what she calls "consentability," Nancy Kim argues that a key determination should involve whether "social harms caused by the proposed activity [are] outweighed by its social benefits." KIM, *supra* note 126, at 49 (2019).

[187] For background about when the law does and should recognize contracts that involve severe bodily injury or killing, see Vera Bergelson, *The Right To Be Hurt: Testing the Boundaries of Consent*, 75 GEO. WASH. L. REV. 165, 169 (2007).

[188] RADIN, BOILERPLATE, *supra* note 52, at 135.

Some of the duties discussed above are already embodied in some privacy laws. But they are often not all included, and most laws lack most of these duties in any meaningful instantiation. When similar duties are included in laws, they are often weakly enforced. For the murky consent approach to work, the duties must be enforced rigorously. Weak enforcement can undermine even the best of laws. It is essential that the enforcers of the laws, whether courts or regulators, avoid deferring to organizations about what is reasonable. Although organizations will make these determinations in the first instance, they can't be trusted to do this without careful oversight. Determinations about reasonableness must be examined by regulators. Organizations must be accountable for their decisions and penalized if they make bad ones. Without rigorous enforcement, organizations can make any rule or duty hollow by complying in a mechanical and perfunctory way.[189]

Organizations will likely clamor for clarity and simplicity; they will want to have specific rules about what is unreasonable. But these issues are difficult to define in advance; they are best worked out case by case. Ultimately, murky consent is a grand bargain: the law should allow for a highly fictional form of consent and avoid bogging organizations and individuals down with a tsunami of express consent requests. In exchange, seekers of consent must be especially careful and circumscribed about how they collect and process personal data. Murky consent is a very limited and delicate license—it can be readily transgressed.

Murky consent's uncertain validity is a feature, not a bug. The tremulous status of murky consent—always at risk of being found to contravene one of the duties discussed above—makes it appropriately weak, as it is of dubious legitimacy. The resulting power to collect, use, and transfer personal data should be precarious, uncertain, and fragile.

Using data with the limited license murky consent provides should be uneasy, like walking a minefield. Organizations should always be uncertain and cautious in their activities. This is a key virtue of the murky consent approach—organizations should never feel entitled to collect and use personal data or emboldened in how they use it. Data collection and use puts individuals at risk; it should put organizations at risk too.

C. *Beyond Consent*

In some cases, privacy law should move beyond relying so heavily on consent. In other areas, the law doesn't allow people to consent to taking

[189] *See* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER xv (2021) (discussing corporate decisions routinizing antiprivacy work to make privacy law just an act); Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 776 (2020) ("Privacy law is failing to deliver its promised protections in part because the corporate practice of privacy reconceptualizes adherence to privacy law as a compliance, rather than a substantive, task."); Cohen, *supra* note 131 ("[D]ata protection in practice can reduce to an exercise in managerial box-checking.").

dangerous and ineffective medications. The law doesn't make people figure out for themselves whether the food they buy will poison them. The law doesn't allow people to buy unsafe products. But with digital technology, the law often tolerates hazardous products and leaves it to consumers to determine what is safe and what is treacherous. Consumers are hardly able to do this.

Privacy law should focus primarily on issues of structure and power.[190] But a regime of privacy regulation can't exclude consent without becoming too paternalistic. Murky consent adds guardrails and oversight; it strives to be more honest about consent rather than the duplicity that pervades today. Although consent should be part of a privacy regulatory regime, consent must have limits. Privacy law must still do significant work in the background to ensure safety.

Other regulatory areas can lend helpful ideas. When it comes to pharmaceuticals, the Food and Drug Administration ("FDA") weighs the safety and effectiveness of drugs. FDA review is "independent and unbiased" and involves establishing that "a drug's health benefits outweigh its known risks."[191] Even drugs that carry a risk of serious side effects can be approved if they have a corresponding benefit. Individuals can choose which drugs they want to use, including riskier ones, but the FDA has limited the choices and excluded drugs that are not effective enough to counterbalance the risks.

A similar yet distinct approach exists for motor vehicles. The National Highway Traffic Safety Administration ("NHTSA") enforces the Federal Motor Vehicle Safety Standards, which establish a minimum baseline of safety for vehicles.[192] There are a wide array of choices in cars, with varying levels of safety. People can even ride motorcycles, which are much riskier than cars. But there are still many rules for vehicle safety that must be followed. Consumers have choices, but many protections are not a matter of individual choice.

Ultimately, the best regulatory regimes preserve space for individual choice, yet also recognize that consent must be carefully constrained.

CONCLUSION

Privacy law has long been ensnared in an intractable dilemma: allow consent, which is a fiction in most cases, or abandon consent. Neither choice is satisfying.

---

[190] SOLOVE, THE DIGITAL PERSON, *supra* note 181, at 226-27 (advocating for addressing architecture of data economy); Solove, *The Myth of the Privacy Paradox*, *supra* note 159, at 1; Solove, *Privacy Self-Management*, *supra* note 7, at 1181 (suggesting individuals cannot self-manage own privacy due to structural problems); Solove, *The Limitations of Privacy Rights*, *supra* note 161, at 976 (proposing broader structural measures over common individual privacy rights framework); KIM, *supra* note 126, at 117 (discussing overarching questions guiding normative discussion of how society views consent).

[191] *Development & Approval Process | Drugs*, FDA (Aug. 8, 2022), https://www.fda.gov/drugs/development-approval-process-drugs [https://perma.cc/RUR8-Z7CF].

[192] 49 C.F.R. §§ 571-171.5 (setting out Federal Motor Vehicle Safety Standards for motor vehicles and motor vehicle equipment).

A battle rages between the notice-and-choice approach and the express consent approach, but neither turns the fictions of consent into facts. The notice-and-choice approach is farcical; the express consent approach is impractical.

The law should stop trying to improve privacy consent in the futile hope of making it meaningful. Instead, the law should accept it for the fiction that it is. The goal is to create a happy fictional story of consent. Murky consent must always be a good deal for people.

Recognizing murky consent is the way out of a seemingly intractable dilemma between consent and paternalism. Murky consent reduces the legitimacy that consent provides and creates a zone for collecting and processing personal data that is safer, restricted, and more responsible and accountable. Murky consent is imperfect, but it is practical. It is a way to move forward, past the consent dilemma that has stymied privacy law for decades.