2023

Murky Consent: An Approach to the Fictions of Consent in Privacy Law

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

Recommended Citation
104 Boston University Law Review (Forthcoming)

Murky Consent:

An Approach to the Fictions of Consent in Privacy Law

by

Daniel J. Solove

104 BOSTON UNIVERSITY LAW REVIEW (forthcoming 2024)

Draft: February 24, 2023

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. Regarding 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, where organizations post a notice of their privacy practices and then people are deemed to have consented 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 non-existent 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 make decisions 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 in most circumstances, 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 consent embraces the fact that consent in privacy is largely a set of fictions and is at best highly dubious.

Abandoning consent entirely in most situations involving privacy would involve the government making most decisions regarding personal data. But this approach would be problematic, as it would involve extensive government control and micromanaging, and it would curtail people's autonomy. The law should allow space for people's autonomy over their decisions, even when those decisions are deeply flawed. The law should thus strive to reach a middle ground, providing a sandbox for free play but with strong guardrails to protect against harms.

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. Instead of providing 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 the Article, I propose some key guardrails to use with murky consent.

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

by Daniel J. Solove[1]

[1] 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 excellent work. Thanks to Brian Bix, Danielle Citron, Ella Corren, David Hoffman, Oscar Gandy, Mike Hintze, Chris Hoofnagle, Nancy Kim, Florencia Marotta-Wurgler, Omri Ben-Shahar, and Allyson Haynes Stuart for helpful feedback.

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.[2]

Consent is an issue that 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.[3] 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 refer to as "privacy consent" for shorthand. In particular, I will concentrate on the collection, use, and disclosure of personal data involved with the multitude of 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. Heidi Hurd refers to consent as a form of "moral magic."[4] 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."[5] 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 fall short of requiring *meaningful* consent. By "meaningful" consent, I am referring to a 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

[2] 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.
[3] DERYCK BEYLEVELD & ROGER BROWNSWORD, CONSENT IN THE LAW 4 (2007).
[4] Heidi M. Hurd, *The Moral Magic of Consent*, 2 Legal Theory 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.").
[5] *Id.* at 123.

predominates, where 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 (GDPR) uses the express consent approach, where people must voluntarily and affirmatively consent (opt in).[6]

The reality is that under either approach to consent, two general problems remain. First, the *evidence of consent* is non-existent under the notice-and-choice approach and at best highly ambiguous under the express consent approach. Privacy law has thus far failed to establish a reliable way to determine whether a person has actually consented. Second, people lack the *capacity to consent* under many circumstances. People are often unable to consent meaningfully to many instances of the collection or processing of their data.[7]

The notice-and-choice approach creates a fiction of consent that is too fanciful even for magical realism. Inaction is not an indication of consent; it signifies nothing. The overwhelming consensus of studies and scholarship has demonstrated that people do not read privacy policies, cannot possibly read them all, and do not understand them in the rare circumstances they review them.[8]

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 and consequences of consenting to various ways their data might be processed. 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 pay attention to 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.[9]

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. Additionally, express consent does not scale. Too many organizations would need to require consent. Each company would also likely need to make multiple and continuous requests for consent given the multifarious ways they collect, use, and transfer personal data.

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 attempt to simplify and shorten privacy notices so that people can understand them, but simplistic and short privacy notices fail to accurately

[6] *See infra* at notes __ - __.
[7] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV 1879 (2013).
[8] *See infra* at notes __ - __.
[9] European Data Protection Board, *Guidelines 5/2020 on Consent Under Regulation 2016-679,* at ¶ 64 (May 4, 2020).

describe the practices and implications. Privacy is very complex, and attempts to simplify are distorting and end up being vague generalities that are not informative. Privacy laws have attempted to shift more to express consent, but that model also fails. The harsh truth is that meaningful consent is rarely possible for the vast number of transactions where people are asked about the collection and processing of their personal data.

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 distorts and disrupts.

An alternative is to abandon consent entirely in most instances and having government regulation specify when personal data can be collected, used, or disclosed. But this approach would be problematic, as it would involve extensive government control and micromanaging as well as impinge upon people's autonomy. There are people who want to trade their personal data for discounts. There are people who want their location tracked for certain reasons. 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 troublesome circumstances.

Consent is so troubling yet also so necessary – a situation that I term the "consent dilemma."[10] 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 offers up a middle position that exists in the large gray zone between the binary poles of consent and non-consent. Most privacy consent is fraught with ambiguity and beset with problems; it is deeply problematic and unreliable. Instead of denying these deficiencies as some approaches do or trying 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. Instead of providing extensive legitimacy

[10] Solove, *Privacy Self-Management, supra* note _, at X.

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 that most privacy consent should be considered to be murky consent and that this is actually the ideal form of consent for the law to recognize in many circumstances. Because murky consent is not binary, there is no one-size-fits-all approach to what should constitute valid consent in all circumstances or to how much power consent should confer. As a starting point, I flesh out guardrails that should limit the power of consent in most situations. These guardrails include: (1) limited scope (limited data retention, data minimization), (2) duties to protect individuals (duty of loyalty, avoidance of unreasonable risk), (3) appropriate obtaining and revoking of consent (proportionality, clean hands, and revocability), and (4) avoidance of societal harm.

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 (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, is rarely fully informed, and is twisted by pre-existing notions and expectations. An even deeper set of problems exists – people are incapable and unequipped 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 general approaches: (1) the notice-and-choice approach; and (2) the express consent approach.

Common in the U.S., 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.[11]

In contrast, the EU's GDPR takes an express consent approach, which requires affirmative and unambiguous consent and rejects implied consent

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

through inaction.[12] 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.[13]

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 processing data is what has become known as the "notice-and-choice" approach.[14] Organizations create a privacy notice (also referred to as a "privacy policy" or "privacy statement") to inform people about they collect and process 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. Or, the choice could be take-it-or-leave-it – either do business with an organization or not. If people do not opt out, then they are deemed to have consented.

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 noticed described the site's privacy practices, and users could then decide whether or not to continue using the site.[15]

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.[16] The FTC interpreted the FTC Act's prohibition on deceptive trade practices to encompass broken promises in privacy notices.[17] In a 1998 report, the FTC declared that "In 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

[12] GDPR art. 4(11) (consent must be "freely given, specific, informed and unambiguous").
[13] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (7th ed. 2021).
[14] Unlike in the EU, which rejects notice-and-choice, privacy law in the United States frequently uses this approach. *See e.g.,* CAN-SPAM Act, 15 U.S.C. §7704(a)(3) (organizations can send unsolicited commercial emails to people, who must unsubscribe to make them stop); Telephone Consumer Protection Act, 47 U.S.C. §227 (telemarketers can call people unless they affirmatively ask to be placed on the 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 the collection and processing of children's data); HIPAA, 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).
[15] Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't,* J. Info. Policy 37, 41-42 (2019) (describing the notice-and-choice approach as: "[B]usinesses 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.").
[16] Solove & Hartzog, *FTC Common Law, supra.*
[17] Solove & Hartzog, *FTC Common Law, supra.*

box on the computer screen."[18] The Commission noted that "despite the Commission's three-year privacy initiative supporting a self-regulatory response to consumers' privacy concerns, the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness)." Nevertheless, the Commission only called for federal legislation to protect children's privacy.[19] The FTC issued a follow-up report in 1999 reaching essentially the same conclusions.[20] The FTC focused mostly on spurring companies to follow the notice-and-choice approach and did not delve into its shortcomings.

An early law to adopt the notice-and-choice approach was the Gramm-Leach-Bliley Act (GLBA) in 1999.[21] The law requires financial institutions to provide people with a privacy notice and gives people the right to opt out of certain types of data sharing. Privacy notices were originally sent to customers in the mail. The GLBA helped to spark the spread of the notice-and-choice approach beyond sites. Primarily focused on the privacy practices of websites, privacy notices began to cover general privacy practices offline as well.

Without the FTC's intervention, the posting of privacy notices would lack much meaning because there would have been no effective enforcement mechanism to ensure that the promises made in the notices would be followed. 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.[22] The FTC thus supplied teeth to the notice-and-choice approach, giving it a thin veneer of legitimacy.

A key component of the notice-and-choice approach is that 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.

Privacy notices exist in a weird twilight in contract law. They are typically separate from other contracts, such as terms of service (TOS) and end user license agreements (EULAs). Although privacy notices look similar to a contract, courts have not held consistently that they are contracts, and it is notable how few cases directly address the issue.[23]

---

[18] FTC, *Privacy Online: A Report to Congress* 8-9 (June 1998), https://www.ftc.gov/reports/privacy-online-report-congress.

[19] *Id.* at 41.

[20] FTC, *Self-Regulation and Privacy Online: Report to Congress* 6 (July, 1999), https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf.

[21] 15 U.S.C. § 6802(a)–(b) (2006).

[22] Solove & Hartzog, *FTC Common Law, supra.*

[23] 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. 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 Reg. 45, 51 (2019) ("[T]he Reporters' data regarding

The notice-and-choice approach has been savaged in the academic literature.[24] Hardly anyone reads privacy notices, those who try to read them struggle to understand them, the statements in privacy notices are often vague and lack much meaning, and the effort to read privacy notices does not scale because there are too many to read.[25] The result is that 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.[26]

Despite the fact that 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, including the California Consumer Privacy Act (CCPA).[27]

The notice-and-choice approach reflects a philosophy that the government should be relatively "hands off." Transparency is the key imperative – as long as information about privacy practices is available, the onus is on individuals to review it and then decide if they want to proceed.

B. THE EXPRESS CONSENT APPROACH

An alternative to the notice-and-choice approach is the express consent approach. Also known as "affirmative" consent,[28] express consent requires a clear voluntary indication of consent. Express consent is central to the

---

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,* 334 F. Supp. 2d 1196 (D.N.D. 2004), the court held that "broad statements of company policy do not generally give rise to contract claims." In Calhoun v. Google, 526 F.Supp.3d 605 (N.D. Cal. 2021), 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." The law does not yet appear to be conclusive on the question of whether privacy policies are contracts.

[24] Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461, 1463 (2019); Richard Warner & Robert Sloan, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. High Tech. L. 370 (2014); Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't*, 9 J. of Info. Pol'y 37-62 (2019); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 Daedalus 32, 34 (2011) (nothing that there is a consensus that notice-and-choice is a failure); Meg Leta Jones & Jenny Lee, *Comparing Consent to Cookies: A Case for Protecting Non-Use*, 53 Cornell In'l L.J. 97, 124-127 (2020) (discussing critiques of attempts to give people "control" over their data through notice and choice).

[25] Solove, *Privacy Self-Management, supra;* Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S 540, 565 (2008) (if people were to read all relevant privacy notices, it would take more than 200 hours a year).

[26] 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) (stating that according to one survey, "only 0.5% of banking customers had exercised their opt-out rights").

[27] California Consumer Privacy Act (requiring a prominent opt out button for selling and sharing of personal data).

[28] United Kingdom Information Commissioner's Office, *What Is Valid Consent?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

EU's GDPR as well as privacy laws in many countries. Some privacy laws in the U.S. 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" approach to regulating the collection and processing of personal data.[29] A "lawful basis" is a 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.[30]

Consent is 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.[31] In fact, consent is the primary lawful basis to process personal data in many countries' privacy laws, especially Latin American countries.[32]

Express consent is one of the strictest forms of consent in privacy laws. The GDPR requires that consent must 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 data relating to him or her."[33] Consent under the GDPR is quite restrictive and not as unlimited as it is in many U.S. privacy laws.[34] Additionally, under the GDPR, the organizations obtaining consent must be able to produce proof of it.[35]

The GDPR provides individuals with the right to withdraw their consent for the future processing of personal data.[36] 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 definitely 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 too. I discuss these difficulties in the next part.

---

[29] GDPR art. 6.
[30] GDPR art. 6.
[31] *See* LGPD; Jamaica; China's PIPL.
[32] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1296-99 (7th ed. 2021). 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 in order to process data. Consent-based laws thus turn into the functional equivalent of lawful basis laws.
[33] General Data Protection Regulation, art. 4(11).
[34] Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 Geo. L.J. 115, 144 (2017)
[35] *Id.*
[36] GDPR art. 7.3.

II. CONSENT'S FICTIONS AND FALSE LEGITIMACY

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 transcend this approach and also apply to express consent.

Consent is not meaningful unless people are truly informed, have appropriate choices, and are capable of making 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.[37]

In this Part, I argue that in most circumstances, privacy consent is fictitious. There are various fictions in privacy consent that cover up severe problems. What makes these fictions of consent so problematic is that consent confers legitimacy on the collection, use, and transfer of personal data. This legitimacy is a potent form of power, a broad license to engage in certain activities involving personal data. [38]

A. DEGREES OF LEGITIMACY

There are different ways that organizations can be justified in engaging in the collection and processing of personal data: (1) there is an absence of any legal restriction; (2) the law provides permission; or (3) individuals provide consent. Of these ways, consent is king.

First, organizations can be justified in collecting and processing personal data when there are no legal restrictions on these activities. In the United States, the default rule in privacy is generally that if something is not prohibited, then it is permitted.[39] This approach only confers a limited legitimacy based on the general norms in the United States that there is freedom to act in the absence of a legal restriction. Such action might be

[37] 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 id* at 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.").

[38] Hubert Schnüriger, *What Is Consent? in id.* at 21,21 ("Consent works as a criterion of legitimacy, deeply pervading social life, making actions and practices permitted that would otherwise be forbidden.").

[39] Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 Geo. L.J. 115, 135 (2017) ("Unlike EU law, U.S. law starts with a principle of free information flow and permits the processing of any personal data unless a law limits this action.").

considered unethical or troubling, as well as undesired by individuals, so its legitimacy is tainted by these possibilities. We do not know if individuals really want these activities to be done with their data; all we know is that they are not forbidden.

A second way that organizations can be justified in collecting and processing personal data is with legal permission. Laws can authorize (or even require) the collection and processing of personal data. For example, under the GDPR's lawful basis approach, data must be processed according to a justified reason under the law. Unlike in the United States, the default is not that in the absence of the law, personal data may be collected and processed as an organization desires. Instead, the default is the opposite; the law authorizes the collection and processing of personal data. With the blessing of the law, the processing of personal data has a significant legitimacy. Society, through its laws, has determined that certain uses of personal data are allowable and even desirable. This form of legitimacy is akin to a societal license to collect and process personal data.

When the law authorizes data processing without consent, legitimacy is based on the society's determination that these activities are in the best interests of society. Such an instance might include when data processing is for legal proceedings or when necessary to protect people's health or safety. But in many cases, the law permits data collection and processing where it is unclear how much society or the individual benefits. For example, although the GDPR protects against processing that would be harmful to individuals, it still permits instances where the processing has zero benefit to individuals as well as instances where individuals do not desire the processing. Under the GDPR, personal data may be processed if "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third part, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject."[40]

Legitimacy based on legal authorization has its limits, as there may be cases where society might permit data processing but individuals may not desire it. Whenever society overrides people's decisions regarding their personal lives, there is an incursion on autonomy. Overriding the individual can certainly be justified and legitimate, but the legitimacy is stronger when not in tension with autonomy.

The third major way to justify the collection and processing of personal data is the individual's consent. Many privacy laws rely partially, heavily, or even primarily on consent as a means to legitimize data collection and processing because consent carries such significant "moral force."[41] In modern Western philosophy, Thomas Hobbes, Adam Smith, and John

[40] GDPR art. 6.1(f)

[41] Preface, *A History of Consent in Western Thought, in* THE ETHICS OF CONSENT ix (Franklin G. Miller & Alan Wertheimer eds. 2010); *see also* John Kleinig, *The Nature of Consent, in id.* at 3, 4 ("consent plays an important moral role . . . [and] transforms the normative expectations that hold between people and groups").

Stuart Mill developed a lasting foundation for consent based on respect for individuals as autonomous beings.[42] Mill's concept of permitting individuals to make self-regarding choices has proven to be a central principle 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."[43]

Consent's legitimacy flows from this underpinning of autonomy. Consent permits things that otherwise would be quite harmful or risky that the law would generally forbid without consent. Respecting autonomy means respecting individuals in making choices regarding their own self-interest. The challenge is that people often do so abysmally. People often make choices that are unhealthy, risky, unwise, and not in their own interest. In many cases, research and study has shown that people are bad about making choices that maximize their happiness, as people struggle to assess what effect things will have on their future happiness.[44]

Even though people make many decisions poorly, a nanny state that micromanages people's lives would likely be quite undesirable as well as immoral under many theories of morality. Respect for autonomy involves allowing individuals to choose for themselves what is in their own best interest even when they are likely to make wrong choices. Certainly, in many circumstances, the law validly curtails people's choices. People cannot choose to use certain dangerous drugs or products. But in most cases, the law provides people with large zone where they can decide for themselves, even when their decisions may be foolish and wrong. 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.

B. FICTIONS OF CONSENT

In theory, privacy consent should mean a clear indication that individuals truly agree to the collection and processing of their data. To truly agree to something, people must make an informed and voluntary decision. Unfortunately, for decisions about privacy, consent falls far short of this ideal, so much so that it is difficult 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 to be consensual. What passes as consent in privacy law is essentially a bundle of fictions, each one a different fantasy that has no plausible basis in fact. The law accepts this collection of fairy

[42] David Johnson, *A History of Consent in Western Thought, in* THE ETHICS OF CONSENT 25, 45-49 (Franklin G. Miller & Alan Wertheimer eds. 2010).
[43] JOHN STUART MILL, ON LIBERTY 13 (Norton ed. 1975).
[44] DANIEL GILBERT, STUMBLING UPON HAPPINESS (2006); *see also* Douglas Husak, *Paternalism and Consent, in* THE ETHICS OF CONSENT, *supra* note __, at 107, 115 ("Economists have come to appreciate that few of us are very proficient at maximizing our own happiness or utility.").

tales and proceeds as if everything is happily ever after. What is most striking is how fanciful some of these fictions are; nobody can plausibly believe they are true.

In the sections that follow, I discuss several problems with privacy consent that are often ignored by the law. Two themes are intertwined in many of the problems. First, in most situations, evidence of privacy consent is scant, incomplete, unreliable, or totally nonexistent. Obtaining a clear and convincing indication of privacy consent is a hopelessly difficult task, but it is conceivably possible. Some privacy laws try valiantly to achieve this goal, but it remains elusive. Most often, the best we have is highly speculative evidence of consent. Privacy laws, however, refuse to accept this truth, no matter how apparent it may be, and they instead cover up the evidentiary gaps with fictions.

A second theme involves the capacity to consent. Even if there were a way to obtain reliable evidence of whether a person is consenting, people are unable to consent meaningfully to the collection and processing of their personal data in many situations.

The problems discussed below involve evidentiary or capacity issues or both. Collectively, these problems demonstrate that to a substantial extent, there is no privacy consent, and even if there were, the existence of consent would be nearly impossible to establish.

1. Ambiguity 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.

Many U.S. laws recognize accept silence or inaction constituting implied consent. When a privacy notice is available that provides people with a right to opt out, people are deemed to have consented if they do not opt out. 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 pre-ticked box. For example, suppose people sign up for an account on a website and are presented with a pre-ticked box for the use of their data for a marketing newsletter. They fail to untick the box. Under the GDPR, pre-ticked boxes are explicitly called out as inadequate to indicate consent.[45] Under many U.S. privacy laws, pre-ticked boxes are acceptable. At least such boxes are often on forms and check out carts, so it is more likely that people will see them. But it still remains unclear whether, in fact, they were seen.

[45] GDPR Recital 32.

Under either scenario—inaction based on a privacy notice or submitting a form without unchecking a box—there is no meaningful indication of consent. Opt out does not 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 reading 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.[46] Implying consent in this situation is completely unjustified, especially given that most people do not read privacy notices.[47]

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 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, or 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 they agree to.[48] A study by Florencia Marotta-Wurgler revealed

[46] Paul M. Schwartz, *Privacy and Autonomy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).
[47] Omri Ben-Shahar & Adam Chilton, *Simplification of Privacy Disclosures: An Experimental Test,* 45 J. Legal Stud. S41, S42 (2016).
[48] 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 (2014); Florencia Marotta-Wurgler, *Does Contract Disclosure Matter?,* 168 J. Inst. & Theoretical Econ. 94, 113-14 (2012) (finding that 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" 205, 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."); Eric Goldman, *The Crisis of Online Contracts (as Told in 10 Memes)*, 2 Notre Dame Journal on Emerging Technologies (2021) (noting that "few consumers actually read online contract terms'); 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 (2014) ("only one or two of every 1,000 retail software shoppers access the license agreement and that most of those who do access it read no more than a small portion.").

that requiring people to click an "I agree" box next to terms only increased readership by 1%.[49]

Some of the most superficial approaches to obtaining express consent involve screens that allow people to click the accept button without reading the details about what they are accepting. In most case, the consent mechanisms are programmed to allow people to accept even before they have scrolled or clicked to review the details of 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. These mechanisms do not measure how quickly a person scrolls down, even though it is possible to do so. In willful ignorance, organizations fail to measure this information to avoid generating evidence that most people are just zooming to the bottom too fast to actually read the text.

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 quite annoying, and the time to read the text would likely be outrageously long. A system that waited 15 to 30 minutes before a user could accept would be a non-starter. 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 are taking the time to read privacy policies. Such a belief would be more absurd than believing in unicorns and fairies. The truth is that people do not read privacy policies and any "consent" to them is a complete lie, but the law accepts the fiction that people are actually consenting.[50]

2. Degree of Influence

Another key dimension of consent is the degree of influence that is tolerated for valid consent. It is rare for decisions to be made free of any influence. Persuasion is a form of acceptable influence. On the darker side are coercion and manipulation. As Daniel Susser, Beate Roessler, and Helen Nissenbaum note, coercion "robs" people of choices whereas manipulation works more subtly; it "infiltrates [a person's] decisionmaking process."[51] Ido Kilovaty argues that manipulation "deprives individuals of their agency by distorting and perverting the way in which individuals

[49] 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).

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

[51] Daniel Susser, Beate Roessler, and Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World,* 4 Geo. L. Tech. Rev. 1, 15 (2019).

typically make decisions."[52]

The lines between persuasion, manipulation, and coercion are quite gray, and the law must choose a coherent approach for when to deem consent to be valid. Unfortunately, privacy law in the United Sates lacks a coherent approach. 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."[53]

(a) Unilateral Imposition of Terms

Voluntariness is at very foundation of the concept of consent, yet in practice, U.S. privacy law tolerates many situations where people must agree to a unilateral imposition of terms and lack meaningful choices.

In the context of employment, an at-will employee can generally be terminated for failing to accept certain privacy-invasive employment practices. In a few instances, the law rejects demanding certain types of personal information, such as the Americans with Disability Act which prohibits gathering data about disabilities in some circumstances.[54] Some highly privacy-invasive practices by employers could be rejected by courts as a violation of public policy.[55] But there are countless forms of surveillance, questionnaires, and tests that employees must "consent" to avoid being terminated.[56] The Fair Credit Reporting Act (FCRA), the law requires that applicants for a job consent in order for employers to obtain a background check on them.[57] But the law does not forbid employers from not hiring people if they fail to provide consent, so essentially, people can be coerced into consenting if they want to obtain the job.

Beyond the employment context, U.S. courts enforce contracts that are often one-sided impositions of terms on consumers.[58] 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,

---

[52] Ido Kilovaty, *Legally Cognizable Manipulation,* 34 Berkeley Tech. L.J. 449, 469 (2019). *See also* Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. Marketing Behavior 213, 218 (2015) ("manipulation involves "an 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); Tal Zarsky, *Privacy and Manipulation in the Digital Age,* 20 THEORETICAL INQUIRIES IN LAW 157, 174 (2019) ("[m]anipulative 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.").

[53] Robert Gellman, *Is There a Role for Consent in Privacy*, IAPP (Apr. 15, 2022), https://iapp.org/news/a/is-there-a-role-for-consent-in-privacy/.

[54] Americans with Disabilities Act, 42 U.S.C. §§ 12112(d)(2)(B), 12112(d)(4)(A) (employers prohibited in inquiring about the "nature and severity" of a person's disability unless related to one's ability to do a job function or for business necessity).

[55] Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 Ohio St. L.J. 671 (1996).

[56] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1113-23 (7th ed. 2021).

[57] Fair Credit Reporting Act, 15 U.S.C. § 1681b(g).

[58] Mark A. Lemley, *The Benefit of the Bargain,* at 1(paper draft on file with author), available at https://ssrn.com/abstract=4184946.

and "firms have seized new opportunities to shift risks to consumers by imposing unread terms."[59]

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.[60] These contracts allow businesses to "construct their own legal universe" that deletes "rights enacted and guaranteed by the state."[61]

With the Internet of Things – the burgeoning number of smart products and devices connected online – the fiction of meaningful consent is even further strained. Oftentimes, there is no readily available display or link to a host of documents that people purportedly agree to. As Stacy-Ann Elvey notes, "By 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."[62] Courts have accepted the weakest indications of consent to encompass a wide array of important issue 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."[63]

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 in order to protect their privacy and their rights. When it comes to 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."[64]

The doctrines of duress and unconscionability merely patrol the outer

[59] David A. Hoffman, *From Promise to Form: How Contracting Online Changes Consumers,* 91 NYU L. Rev. 1595, 1596 (2016).
[60] MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 3-9 (2012).
[61] *Id.* at 15, 33.
[62] STACY-ANN ELVEY, A COMMERCIAL LAW OF PRIVACY AND SECURITY FOR THE INTERNET OF THINGS 120 (2021).
[63] STACY-ANN ELVEY, A COMMERCIAL LAW OF PRIVACY AND SECURITY FOR THE INTERNET OF THINGS 142 (2021).
[64] Helen Nissenbaum, *A Contextual Approach to Privacy Online,* 140 Daedalus 32, 35 (Sept. 29, 2011).

boundaries.[65] Duress involves using threats of economic or physical harm to obtain consent.[66] Unconscionability involves contracts with one-sided terms that are unfair.[67] Cases are hard for people to win. As Mark Lemley observes, "Courts rarely apply unconscionability."[68] Additionally, the U.S. Supreme Court has weakened unconscionability protections in a series of decisions expanding the Federal Arbitration Act (FAA) to preempt state law. The result is curtailing the ability to invalidate mandatory arbitration clauses unconscionable.[69] The Supreme Court also upheld a choice of forum clause that "render litigation almost impossible for claimants and thus deprive them of any viable opportunity to have their day in court."[70]

In rhetoric, contract law seemingly requires meaningful consent, but in practice, this is a fiction. According to the standard dogma, "[c]ontract must result from a meeting of the minds of the parties in mutual assent to the terms, and must be based upon sufficient consideration, free from fraud or undue influence, not against public policy, and sufficiently definite to be enforced."[71] 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.[72]

Additionally, most privacy notices state that organizations can change the terms at any point in time.[73] People are thus ostensibly agreeing to a blank check – to nearly anything that an organization wants to do in the future.[74] When changes are made, often no effort is taken to notify people of them.[75] Charlotte Tschider aptly notes that privacy notices are often a "one-sided communication of an organization's behaviors with respect to data."[76] She

[65] Restatement (Second) of Contracts § 208 ("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* at § 175 ("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.").
[66] Bix, *Contracts, supre* note X, at 257.
[67] Bix, *Contracts, supre* note X, at 259.
[68] Lemley, *Benefit of the Bargain, supra* note X, at 10.
[69] RADIN, BOILERPLATE, *supra* note __, at 130-31.
[70] *Id.*
[71] RICHARD A. LORD, WILLISTON ON CONTRACTS § 1:3 (4th ed. 2004) (citing *Doe v. HCA Health Services of Tennessee, Inc.,* 46 S.W.3d 191 (Tenn. 2001)).
[72] SOLOVE AND SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note _, at 856-864.
[73] Thomas 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.").
[74] In some cases, the U.S. Federal Trade Commission (FTC) has concluded that retroactive changes in privacy notices applied to previously-gathered personal data can violate the FTC Act Section 5. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 Colum. L. Rev. 583, 640-41 (2014).
[75] Haley, *Illusory Privacy, supra* note X, at 102.
[76] Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the*

aptly asks: "[H]ow can consent to unfair, one-sided, readily changeable terms actually represent real choice?"[77]

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 these contracts."[78] 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."[79]

Even if there are practical reasons to allow coercion in practice for certain contracts or other transactions, to call it "consent" is unjustifiable. Whether or when coercion should be tolerated might be a debatable issue, but the fiction that coerced consent is valid provides unwarranted legitimacy. The legitimacy of consent emerges in large part out of respect for the autonomy of the individuals who freely choose to consent. Coercion masquerading as consent is a wolf in sheep's clothing.

The GDPR takes a stricter approach to coercion. It requires that consent be "freely given." But the question remains: *What does "freely given" mean?* The GDPR provides at Recital 42 that "Consent 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."[80] Guidance by the European Union Data Protection Board (EDPB) explains that consent is invalid if a person "feels compelled to consent or will ensure negative consequences if they do not consent."[81]

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).[82] 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."[83] 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.[84]

Consent Myth, 22 N.C. J. L & Tech. 617, 636 (2021).
[77] *Id.* at 639.
[78] Brian Bix, *Contracts, in* THE ETHICS OF CONSENT 251, 252 (Franklin G. Miller & Alan Wertheimer eds. 2010).
[79] *Id.*
[80] GDPR Recital 42.
[81] European Data Protection Board, *Guidelines 5/2020 on Consent Under Regulation 2016-679,* at ¶ 13 (May 4, 2020).
[82] GDPR Recital 43.
[83] GDPR Recital 43.
[84] European Data Protection Board, *Guidelines 5/2020 on Consent Under Regulation 2016-679,* at ¶ 21 (May 4, 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(10(a)) due to the nature of the relationship between employer and employee.").

Nevertheless, the GDPR still must bend to the practicality argument Bix raises. Beyond vulnerable populations, the GDPR cannot fully cleanse away the fictions of consent. In countless transactions, there is a lack of compelling evidence that consent is anything more than an illusion.

(b) Manipulation

Manipulation is much less restricted by privacy laws than coercion. According to Cass Sunstein, manipulation is so pervasive that "the legal system usually does not attempt to prevent it."[85] Shaun Spencer surveys different definitions of manipulation and concludes that "they all contain the notion of circumventing the subject's rational decision-making process" and most require intent to manipulate.[86]

Privacy law attempts to address manipulation, and although the law is attempting to respond to a limited extent against some of the more abusive forms of manipulation, an extensive amount of manipulation continues to exist. 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."[87] 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.[88] Privacy law is trying to address manipulation, but practically, it can only address the worst schemes.

What makes manipulation so difficult to combat is that people are quite gullible and manipulable. Human decisionmaking is fraught with irrationality and systematic biases and heuristics that can readily be exploited.[89] As Ryan Calo notes, "the digitization of commerce dramatically alters the capacity of firms to influence consumers at a personal level." Organizations are increasingly capable of exploiting "irrationality or vulnerability in consumers."[90] As Neil Richards and Woodrow Hartzog note, "Because 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."[91]

---

[85] Sunstein, *Manipulation, supra* note _, at X.
[86] Shaun Spencer, *The Problem of Online Manipulation,* 2020 U. Ill. L. Rev. 959, 989 (2020).
[87] *Federal Trade Commission, Policy Statement on Unfairness* (1980), Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.
[88] California Consumer Privacy Act, Cal. Civ. Code § 1798.140(l); Colorado Privacy Act, Co. Rev. Stat. 6-1-1303(9). The term "dark patterns" was coined by Harry Bringnull, in *Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff*, 90 Percent of Everything (July 8, 2020).
[89] DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011); DAN ARIELY, PREDICTABLY IRRATIONAL (2008).
[90] Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995, 999 (2014).
[91] Neil M. Richards & Woodrow Hartzog, *The Pathologies of Digital Consent,* 96 Wash. U. L. Rev. 1461, 1489 (2019).

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 certainly noble and worth pursuing, but in the meantime, the law's acceptance of consent in our current highly-manipulated world is a fiction.

(c) Conditions on Consent

Another problem with determining whether privacy consent is truly consensual involves what type of conditions are placed on consent. People are often cajoled into consenting because they must pay or forgo something if they refuse.

Some privacy laws impose restrictions on imposing conditions on consent. For example, in the U.S., HIPAA restricts conditioning providing healthcare services on consenting to allowing the use of personal data for marketing or other purposes.[92] Other laws have less bold restrictions. For example, the CCPA provides that business "shall not discriminate against a consumer because the consumer exercised any of the consumer's rights."[93] Forms of such discrimination include denying goods or services, charging different prices, or providing a different level of quality unless these differences are "reasonably related to the value provided to the customer by the consumer's data."[94] The Virginia Consumer Data Protection Act has a similar provision.[95]

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.[96] A saying often uttered about the Internet is: "If you're not paying for the product, you are the product."[97] 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

[92] HIPAA, 45 C.F.R. 164.508.
[93] CCPA, 1798.125.
[94] CCPA, 1798.125.
[95] Virginia Consumer Data Protection Act, S.B. 1392 § 59.1-574(A)(4).
[96] Chris Jay Hoofnagle and Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 606 (2014).
[97] This quote is often attributed to the Netflix documentary, *The Social Dilemma* (2020), *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), https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/?sh=4fe233b5d6ee.

conditions that many laws make. For example, under the CCPA, a business may charge more for consumers who refuse to allow the transfer of their personal data "if that difference is reasonably related to the value provided to the consumer by the consumer's data."[98] Businesses are allowed to offer financial incentives to consumers for collecting and selling their personal information.[99] The result is that people can be presented with a cornucopia of treats – technologies that glimmer and gleam, dazzling entertainment, fascinating information, and enormous conveniences – and readily give away their data. Are they really consenting? Or are they responding like lab rats addicted to morphine? People experience the Internet as Hanzel and Gretel, their mouths watering as they explore a world built of candy houses; they often do not realize they are being fattened up to be part of a feast.

In contrast to the approach in the U.S., the GDPR has much stricter restrictions on making providing services conditional on consent to process personal data. The GDPR requires that "utmost account" must be taken when "the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[100] According to the EDPB, "If consent is given in this situation, it is presumed to be not freely given."[101]

The GDPR is certainly stronger at restricting conditioned consent, but it has limits. Ultimately, the organizations that aim to collect and process personal data have control over how they frame transactions and contracts. This power can allow them to evade restrictions.

3. The Difficulties of Being Informed

Privacy consent is not meaningful if it is not informed. 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 autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives. . . . To choose, one must be aware of one's options . . . [and] must be capable of understanding how various choices will have considerable and lasting impact on his life."[102]

Reading privacy notices is an exercise in torturous tedium that hardly anybody undertakes. 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 frequently written at a very high reading level.[103]

---

[98] CCPA, 1798.125(2).
[99] CCPA 1798.125.
[100] GDPR Article 7(4).
[101] European Data Protection Board, *Guidelines 5/2020 on Consent Under Regulation 2016-679,* at ¶ 26 (May 4, 2020).
[102] JOSEPH RAZ, THE MORALITY OF FREEDOM 369, 371 (1986).
[103] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV 1879 (2013).

In the law, one of the strongest forms of consent is "informed consent" in the healthcare and research contexts. Originating in the common law, the requirement for informed consent for healthcare emerged in U.S. in the late 1950s and early 1960s.[104] U.S. states began to enact informed consent statutes throughout the 1970s, with 30 states having enacted such laws by 1982.[105] The juridical underpinnings of informed consent trace back to Justice Cardozo's opinion in *Schloendorff v. Society for New York Hospitals,* where he declared: "Every human being of adult years and sound mind has the right to determine what shall be done with his own body; and a surgeon who performs an operation without his patient's consent commits an assault, for which he is liable in damages."[106] In *Salgo .v Leland Stanford Jr. University Board of Trustees,* the court held that not only consent is required for medical procedures, but also the consent must be informed.[107] As articulated in the pivotal case, *Canterbury v.* Spence, the U.S. Court of Appeals for the District of Columbia Circuit held that for healthcare, "[t]rue consent to what happens to one's self is the informed exercise of a choice."[108] Today, regulations for informed consent for human subject researched requires 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."[109] The information must be "understandable," there must be "sufficient detail," and the information must include a description of "reasonably foreseeable risks or discomforts," of the benefits, and of any appropriate alternatives.[110]

Privacy consent often falls far short of these requirements. The notice-and-choice approach fails to ensure that people are informed. Most privacy notices are ignored. Laws often mandate disclosures and warnings to individuals, but individuals skim through them or do not read them all. [111]

Some privacy laws take some weak efforts to improve this woeful situation, such as make the privacy notice more conspicuous or require that it be written more simply. Under the Gramm-Leach-Bliley Act (GLBA), which regulates the collection and use of data by financial institutions, notice must be "clear and conspicuous."[112] The California Online Privacy Protection Act (CalOPPA) requires that a privacy notice be posted conspicuously on an organization's website.[113] The California Consumer

[104] RUTH R. FADEN & TOM L. BEAUCHAMP, A HISTORY AND THEORY OF INFORMED CONSENT 24, 86 (1986).
[105] *Id.* at 256.
[106] Schleondorff v. Society of New York Hospitals, 105 N.E.92 (N.Y. 1914).
[107] Salgo v. Leland Stanford Jr. University Board of Trustees, 317 P.2d 170, 181 (1957) (doctors had to disclose "any facts which are necessary to form the basis of an intelligent consent by the patient to proposed treatment").
[108] Canterbury v. Spence, 464 F.2d 772 (D.C. Cir. 1972).
[109] Protection of Human Subjects, 16 CFR § 1028.116.
[110] *Id.*
[111] OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 10 (2014) (noting that people "overlook, skip, or skim disclosures").
[112] Gramm-Leach-Bliley Act Regulations, 17 CFR § 248.4.
[113] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579

Privacy Act (CCPA) goes a step further by mandating a conspicuous button for people to opt out of selling or sharing personal data.[114]

But these efforts fail to guarantee that privacy notices are actually read. In a related situation, reading end user license agreements (EULAs), Florencia Marotta-Wurgler's research reveals that "no matter how prominently EULAs are disclosed, they are almost always ignored.[115] Beyond requiring that privacy notices be clear and conspicuous, the laws do not require any indication that people understand them. In the U.S., 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.[116]

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

Even if privacy laws could reach the same standards of informed consent in healthcare, they are likely to fail. Professor Charles Lidz, an expert in bioethics, observed that "[t]here is very substantial empirical evidence that the large majority of both research subjects and patients do not carefully weigh the risks and benefits."[117] For example, in one study of cancer patients involved in clinical trials for experimental medications, "[f]ewer than half of patients correctly identified the safety and dosing objectives" of the medications in the experiment after providing informed consent.[118]

Informed consent goes far beyond merely making available 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 truly informed, there must be more

(2004).

[114] California Consumer Privacy Act, 1798.185.

[115] 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, 182 (2011).

[116] David A. Hoffman, *Relational Contracts of Adhesion,* 85 U. Chi. L. Rev. 1395, 1396-97 (2018).

[117] Charles W. Lidz, *Informed Consent: A Critical Part of Modern Medical Research,* 342 Amer. J. Med. Sci. 273 (2011).

[118] Katherine E. Reeder-Hayes, Megan C. Roberts, Gail E. Henderson, and Elizabeth C. Dees, *Informed Consent and Decision Making Among Participants in Novel-Design Phase I Oncology Trials*, DOI: 10.1200/JOP.2017.021303 Journal of Oncology Practice 13, no. 10 (October 1, 2017) e863-e873.

demonstrable methods used to ensure that people truly understand the choices they are making. Such methods do not exist under either the notice-and-choice approach or the express consent approach.

(a) The Dilemma of Complexity and Simplicity

Privacy laws face a difficult dilemma with notice – either notice can be lengthy and complex or short and simple. A lengthy notice can explain meaningfully how personal data is collected and used, but such a notice will be more daunting for people to read and more challenging 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."[119] Other privacy laws also require clear and understandable language. For example, Virginia's CDPA requires that privacy notices be "reasonably accessible, clear, and meaningful."[120] Beyond the law, various proposals have been made to create simple notices, such as using privacy nutrition labels, icons, pithy pop up boxes, and similar techniques of concision.[121]

Despite these legal requirements, privacy notices have not become more readable. One study of privacy notices compared them before and after the GDPR went into effect in 2018 and found "scant" improvement in readability.[122] Post-GDPR, "privacy policies are still very often unreadable."[123]

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 they presented subjects with privacy notices at varying degrees of simplicity, they found "In each of these three tests our 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."[124] A study led by Aleecia McDonald reached a similar result. The study compared several formats of a privacy policy, including a "short form with standardized components in addition to a full policy" and found that "participants were not able to reliably understand company's privacy

[119] GDPR Recital 58. The EDPB guidance states that a "message should be easily understandable for the average person." European Data Protection Board, *Guidelines 5/2020 on Consent Under Regulation 2016-679,* at ¶ 67 (May 4, 2020).
[120] Virginia Consumer Data Protection Act, S.B. 1392 § 59.1-574(C).
[121] Mike Hintze, *In Defense of the Long Privacy Statement*, 76 Md. L. Rev. 1044, 1066-77 (2017).
[122] 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).
[123] *Id.*
[124] Omri Ben-Shahar & Adam Chilton, *Simplification of Privacy Disclosures: An Experimental Test,* 45 J. Legal Stud. S41, S42 (2016).

practices with any of the formats."[125]

A very simple notice cannot accurately describe many of the highly complex ways that personal data is processed. Simple notices end up being vague and cursory. As Mike Hintze aptly 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."[126]

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 aptly note, if privacy notices truly explained everything people needed to make informed decisions, the "detail that would allow for this would overwhelm even savvy users because the practices themselves are volatile and indeterminate."[127]

The GDPR demands granular and specific consent to each specific purpose of 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: the identity of the data controller, the purpose of the data processing, the type of data that will be processed, the existence of the right to withdraw consent, and information about automated decisionmaking where relevant.[128] 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.

(b) Incorrect Pre-Existing Notions

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

Several studies show that people harbor significantly incorrect notions about how their personal data is being collected and processed. A study by

[125] Aleecia M. McDonald, Robert W. Reeder, Patrick Kelley, & Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats, in* PRIVACY ENHANCING TECHNOLOGIES 37, 38 (Ian Goldberg & Mikhail Atallah eds. 2009).
[126] Mike Hintze, *In Defense of the Long Privacy Statement*, 76 Md. L. Rev. 1044, 1064 (2017).
[127] 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.); *see also*
[128] European Data Protection Board, *Guidelines 5/2020 on Consent Under Regulation 2016-679,* at ¶ 64 (May 4, 2020).

Chris Hoofnagle and Jennifer Urban found that many people wrongly thought that their personal data was protected by stronger legal protections.[129] A survey by Kristen Martin revealed that people projected incorrect beliefs that their data would be more protected than the actual notice provided in the survey: "Privacy notices became a tabula rasa for users' privacy expectations."[130] In another study led by Joseph Turow, a majority of people falsely believed that if a website has a privacy policy, then it cannot share personal data with other companies without permission.[131] 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."[132]

Consent that is not informed is already quite flawed, but it is further tainted when it is based on false beliefs. Consenting based on mistaken information is generally worse than consenting based on ignorance. The task of correcting false notions and educating people would be a mammoth project that is unlikely achievable at the scale of all of society.

Beyond correcting false beliefs about privacy protection, people would also have to be taught about the intricacies of modern data analytics, which reveals surprising inferences, ones that are quite unexpected.[133] 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.[134]

Beyond inferences, people are often unaware of the metadata that is embedded with various digital files and documents they provide. For example, a photo of yesteryear is not the same as today's photo, which is saturated with data such as date, location, and other metadata.

So many activities are swarming in a mist of data, much like the invisible virus particles that are expelled when people talk and breathe. People are

---

[129] Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest L. Rev. 261, 283–84, 302 (2014).

[130] 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).

[131] Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* 21 table 9 (2009).

[132] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, Pew Research Center (Dec. 4, 2014), https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/

[133] Hideyuki Matsumi, *Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?*, 48 Cumb. L. Rev. 149 (2018); Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, https://ssrn.com/abstract=3921003 (Sept. 10, 2021); 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).

[134] 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).

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 understand much data collection and processing. They are not informed and cannot be informed.

Consent under these circumstances is fictitious. The law tries to combat this problem, but the game is an inevitable checkmate. Yet, the law continues to play on.

4. Inability to Decide

As I have explored in depth elsewhere, people lack the knowledge as well as cognitive ability to engage in good cost-benefit analysis regarding future uses and sharing of their data.[135] When people are presented with a choice about whether or not 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, and other dopamine-generating joyous 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.[136] People often have a "human tendency to favor short-term over long-term consequences."[137] People also have an optimism bias, where they "overestimate the likelihood of positive events, and underestimate the likelihood of negative events."[138]

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 or that she wants to conceal. But the decision is not one that people spend months ruminating on; it is made quickly. The person often cannot readily conceive of all the potential items she will look at on the website in the future. Nor will the person be able to know how various algorithms might analyze the data. That analysis might yield revelations of facts about the person that the person wants to conceal; or 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. Many algorithms use not just the data streams of each individual separately but instead look for patterns across an entire data set

[135] Solove, *Privacy Self-Management, supra* note _, at __.
[136] Neil M. Richards & Woodrow Hartzog, *The Pathologies of Digital Consent,* 96 Wash. U. L. Rev. 1461, 1484 (2019).
[137] NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 60 (2019).
[138] Tali Sharot, *The Optimism Bias,* 21 Current Biology R941 (Dec. 6, 2011).

of many people. Algorithms use these patterns to make conclusions about particular individuals. So, to truly understand how the algorithm will work, the person will need to know not only the logic of the algorithm, their own future stream of data that will be fed into the algorithm, but also all the other data fed into the algorithm. In short, there really is no way to make a good cost-benefit analysis. At best, individuals consent based on wildly speculative hunches or uninformed gut senses. People often cannot 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."[139]

Even more basic decisions are difficult for people to assess. Suppose a person is asked whether to share personal data with a company. Part of the assessment of cost-benefit analysis depends upon 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 security program that the organization has in place. 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 various types of parties can subpoena the data? How readily and likely will the government 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 dark.

To make a nearly impossible situation even worse, decisions on whether to consent to various forms of data collection, processing, or disclosure do not scale. There are too many companies that people interact with for people to make even one consent decision per organization. And, organizations often engage in many different instances of collecting, processing, and disclosing data, so there will be multiple decisions required for each organization. Moreover, over time, organizations will want to engage in different uses or disclosure of data as new opportunities and circumstances arise, so people could be asked to consent again even for the same data.

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 do not want to take a lot of time to mull over privacy.

---

[139] Cameron Kerry, *Why Protecting Privacy is a Losing Game Today – and How to Change the Game*, BROOKINGS (Apr. 15, 2022, 5:00 PM), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

Consent requests often entice people to consent just to make the annoying request go away so they can proceed to what they want to do or see. The benefits of technologies, products, and services are often instantaneous. A few people might forgo immediate gratification and take a long detour learning about privacy, studying the issues involved, carefully weighing the risks and benefits, and then reaching an informed decision. These people probably exist only in the pages of fiction.

5. Structural Limitations

Several structural limitations plague people's ability to provide meaningful consent to the collection and processing of their personal data. These problems stem from how consent choices are structured. Many situations involving consent involve inadequate choices. On the other side, 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 workable middle ground.

(a) 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. There is no an ability to opt out of each particular practice. The same holds true for opt in. Under many circumstances, the choice is all or nothing.

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."[140]

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 quite 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

[140] Julie E. Cohen, *How (Not) to Write a Privacy Law,* Knight First Amendment Institute, at p. 8 (2020).

third parties are vetted or monitored for compliance. Regarding 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.

Without these details, people really do not know much about how protected their data will be. In many cases, an organization can be like a restaurant, which appears clean and sparkling where people dine yet have a kitchen crawling with cockroaches. Privacy law rarely demands that people see what is going on in the kitchen before consenting. Yet, for privacy, the kitchen is highly relevant for meaningful consent.

It is difficult 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 they must either take or leave is somehow presenting people with a meaningful choice.

(b) Too Many Choices

The flip side of not enough choices is too many choices. Too granular an approach is overwhelming. Nevertheless, the GDPR requires consent to be quite granular and specific. According to the EDPB, "Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'."[141] Specificity means that consent for various purposes requires "a separate opt-in for each purpose."[142]

Organizations can process a multitude of 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 overwhelming and very complex. 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.[143]

[141] European Data Protection Board, *Guidelines 5/2020 on Consent Under Regulation 2016-679,* at ¶ 60 (May 4, 2020).
[142] European Data Protection Board, *Guidelines 5/2020 on Consent Under Regulation 2016-679,* at ¶ 60 (May 4, 2020).
[143] 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

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."[144] 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."[145] As Nancy Kim observes, "More 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."[146]

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 still remains – none of this scales. I will address this issue in the next section.

6. 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 be issuing a stream of consent requests. The result is a tremendous and unwanted burden hoisted upon the individual.[147]

In 2008, Aleecia McDonald and Lorrie Cranor studied privacy notices and noted that the average length was 2514 words.[148] More recent studies have indicated that the length of privacy policies have grown. The average length of the privacy policies of the twenty most-used apps in 2018 was 3964 words – 58% longer than those examined in a decade earlier by McDonald and Cranor.[149] Take, for example, the trend in Google's privacy policy.

---

[144] Stefan Korff and Rainer Böhme, *Too Much Choice: End-User Privacy Decisions in the Context of Choice Proliferation*, Symposium on Usable Privacy and Security (SOUPS) (2014), https://www.usenix.org/system/files/soups14-paper-korff.pdf.

[145] OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 104-05 (2014).

[146] NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 13 (2019).

[147] Ella Corren, *The Consent Burden: Between Privacy and Consumer Protection* (draft on file with author).

[148] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S, A Journal of Law and Policy for the Information Society 540, 565 (2008) (if people were to read all relevant privacy notices, it would take more than 200 hours a year).

[149] Pierre-Nicolas Schwab, "Reading Privacy Policies of the 20 Most-Used Mobile Apps Takes 6h40," Into the Minds Blog (May 28, 2018),

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."[150] In 2022, a machine learning analysis of 50,000 privacy policies revealed that during the past 25 years, they grew by more than 4,000 words on average.[151] This trend is not surprising – data collection and use has become more extensive and complicated, so it cannot 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."[152] The negative consequences of click fatigue are that the "warning effect" of consent mechanisms diminishes and that "consent questions are no longer read."[153] 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."[154]

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, often referred to as "cookie banners." 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.

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,[155] which started off with fanfare but later fizzled into irrelevance.[156] A rebooted attempt is through "Global Privacy Controls" (GPC) via the CCPA.[157] It remains to be seen if this will prove successful.

---

https://www.intotheminds.com/blog/en/reading-privacy-policies-of-the-20-most-used-mobile-apps-takes-6h40/.

[150] Kevin Litman-Navarro, "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.

[151] 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/.

[152] European Data Protection Board, *Guidelines 5/2020 on Consent Under Regulation 2016-679,* at ¶ 87 (May 4, 2020).

[153] *Id.* at ¶¶ 87-88.

[154] *Id.* at ¶ 88.

[155] Goldman, *Crisis of Online Contracts, supra* note __, at 8.

[156] Meg Leta Jones & Jenny Lee, *Comparing Consent to Cookies: A Case for Protecting Non-Use,* 53 Cornell In'l L.J. 97, 102 (2020) ("[T]he U.S. and the EU have both failed to legally enforce a DNT signal.").

[157] California Consumer Privacy Act Regulations § 999.315(c)(2).

Privacy is likely too contextual and nuanced to readily be 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 different types of data collection and processing, it is difficult 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 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 depends upon the circumstances. It remains unclear how an automated global system can make these determinations well; most likely, a simplistic one-size-fits 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 pestering people repeatedly, consent requests can become overwhelming to the point of being abusive. Faced with so many requests for consent, people will not be able 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 upon consent, the less reliable consent becomes.

Ultimately, trying to make consent more rigorous leads to what has become known as "consent fatigue."[158] 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."[159] 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."[160]

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

[158] Rishab Bailey, Smriti Parsheera, Faiza Rahman, Renuka Sanea, *Disclosures in Privacy Policies: Does "Notice and Consent" Work?*, 33 Loy. Consumer L. Rev. 189, 191 (2021).
[159] Ella Corren, *The Consent Burden: Between Privacy and Consumer Protection* (draft on file with author).
[160] Cameron Kerry, *Why Protecting Privacy is a Losing Game Today – and How to Change the Game*, BROOKINGS (Apr. 15, 2022, 5:00 PM), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

data and take on risks that they do not want to take on.[161] For example, the US Video Privacy Protection Act (VPPA) required people to consent for disclosing data about each video that they watched.[162] 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.[163] Congress rushed to Netflix's aid, allowing a blanket consent that can include all of the videos a person watches for a period of two years.[164] McGeveran argues that this frictionless sharing can lead to instances where people end up disclosing more information than they expect.[165] 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 that they might not want to disclose. The result can be disclosures that people ultimately regret. Thus, McGeveran argues, "friction" can be a good thing, as it involves "forces that impede individuals from disclosing personal information when they use online services."[166] 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 small amount of time.

Some commentators argue that the fact that many people do not want to think about privacy means that 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.[167] The fact 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 broadly, as Omri Ben-Shahar and Carl Schneider note, "People are, loosely and broadly, decision averse."[168] 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.

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.

---

[161] William McGeveran, *The Law of Friction*, U. Chicago Legal Forum Vol. (2013), Article 3, at 15, https://chicagounbound.uchicago.edu/uclf/vol2013/iss1/3.

[162] 18 U.S.C. 2710(b)(2) (2012) (prior to amendment by Pub. L. 112-258) (requiring "informed, written consent of the consumer given at the time the disclosure is sought).

[163] McGeveran, *Friction, supra* note _, at 26.

[164] 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).

[165] McGeveran, *Friction, supra* note _, at 39-43.

[166] William McGeveran, *The Law of Friction*, U. Chicago Legal Forum Vol. (2013), Article 3, at 15, https://chicagounbound.uchicago.edu/uclf/vol2013/iss1/3.

[167] Daniel J. Solove, *The Myth of the Privacy Paradox,* 89 Geo. Wash. L. Rev. 1 (2021).

[168] OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 61 (2014).

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.[169] They are unable to escape cognitive biases. They "often make decisions with little information or deliberation."[170]

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 25 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 have a lengthy conversation with their chief privacy officer or 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 do know is how much I don't know.

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, more attempts to give individuals control over their data. These approaches are doomed.[171] 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 and it will not scale.

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

[169] OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 109 (2014) ("People have poorly defined goals about most problems, and no plausible amount of thinking will define them sharply.").
[170] OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 64 (2014).
[171] Solove, *The Limitations of Privacy Rights, supra* note __, at __.

was tainted with difficulties, then people would rarely ever 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 exploited; and they are often coerced or manipulated. Because of these ugly truths, the law would need to micromanage every nearly every instance of collection, use, and disclosure of personal data. The law would become overly controlling.[172] It would be nearly impossible to develop a legal framework to govern the countless situations involving privacy, especially with such a 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. Even accepting that these problems can never be surmounted, there is value in preserving space for individual choice, as flawed and compromised as human decisionmaking 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."[173]

But how can the law protect what is actually in an individual's self-interest and respect an individual's freedom to choose when we know individuals are incapable of making 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. Reformers try to make the fictions a bit less absurd, but we still remain in a Kafka story. Is there any way out?

In this Part, I contend that there is a way out. But the path is in a counterintuitive direction. Instead of trying 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 IN TO THE FICTIONS

For a long time, finding ways to make 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 might make it worse. For example, the

[172] 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.

[173] NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 64 (2019).

editors of the New York Times wrote an op ed critiquing opt out approaches and declaring that "Using an opt-in approach will help curb the excesses of Big Tech."[174] But opt in has a downside that is often overlooked – it provides greater legitimacy when organizations use it to collect and process personal data. Opt out consent has a dubious legitimacy, enveloping the license to use the data in a fog. Opt in has greater legitimacy. But this also might encourage increased use of the data. If the law required opt in, organizations will find ways to manipulate users into opting in, and then use the data more aggressively because of the opt in's stronger claim to legitimacy.

Even if the law tried to cleanse away the manipulation, organizations could likely find ways to entice people to consent. People make decisions often for immediate gratification, and privacy involves rather abstract concerns and a vague risk of something happening in the distant future. People struggle to assess the risks when they consent. The privacy costs are quite hard to comprehend, as they often involve how personal data is aggregated over time, how algorithms analyze that data, and what decisions are made based on that data. These processes are highly complex. In contrast, the benefits of consenting to data collection and processing are often more immediate and concrete – people can use products and services, have access to news and information, or be entertained by video, games, music, and more. Therefore, if consent cannot be tricked, it can be bought.

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. Certainly, it would 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 greater transparency comes at a cost because it can further legitimize the trade of personal data. Generally, with greater legitimacy comes greater power to use data — or at least an emboldened sense of entitlement. Organizations would view the data as theirs because they bought it. They would become more entitled to use it because they paid for it and people sold it to them. Contrast this with the current situation, where it remains quite ambiguous that any real sale of data has occurred. Organizations might take data, assume uneasily that they can use it, but their license is fraught with uncertainty. In a more transparent world, the license becomes clearer and organizations become bolder about using personal data.

Could contract law come to the rescue and make privacy consent meaningful? As Brian Bix notes, "consent—in one form or another—is at the core of the modern understanding of contract law."[175]

Perhaps aggressive application of contract law to privacy notices might add formalities and protections that are currently 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

[174] Opinion, "America, Your Privacy Settings Are All Wrong," N. Y. Times (Mar. 6, 2021).
[175] Brian H. Bix, *Consent and Contract, in* ROUTLEDGE HANDBOOK, *supra* note X, at 222, 222.

create "greater leeway to use personal information."[176] Companies can readily include terms in privacy policies that are unfavorable to consumers.[177] She concludes: "Rather than providing consumers the protection they expect, privacy policies have become one more online contract of adhesion for consumers to avoid."[178] The more formal the situation involving consent becomes, the more legitimacy and legal 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 mainly serve to add power to the fictions.

Contract law, however, also struggles with consent.[179] 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 actually consented by focusing on "state of mind, preferences, volition."[180] Under the "external" or "objective" approach, the law should focus on observable indicia of consent.[181] 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."[182]

As David Hoffman observes, contract law has strained to adjust to a world where contracts have grown exponentially.[183] 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."[184]

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. Consent is based on fictions, which allow for the legitimacy and

[176] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information,* 111 Penn. St. L. Rev. 587, 609 (2007).
[177] *Id.* at 612.
[178] *Id.* at 624.
[179] *See* RADIN, BOILERPLATE, *supra* note X, at X; Bix, *Contracts*, *supra* note X, at 252.
[180] Bix, *Contracts*, *supra* note _, at 252.
[181] *Id.*
[182] Randy E. Barnett, *A Consent Theory of Contract,* 86 Colum. L. Rev. 269, 269 (1986).
[183] David A. Hoffman, *From Promise to Form: How Contracting Online Changes Consumers,* 91 N.Y.U. L. Rev. 1595, 1596 (2016).
[184] Eric Felten, *Postmodern Times: Are We All Online Criminals?* Wall St. J. Nov. 18, 2011, at D8.

moral force of consent without the existence of consent.

Ultimately, any legitimacy and moral force supplied by fictions are unwarranted.[185] Contract law thus lacks the answers; it just poses more questions. It does not present privacy law with a useable approach to consent.

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

Instead of trying 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 to pretend that they are true. Privacy consent is inescapably fictional, and it works best as a set of fictions in many circumstances. The problem is not the fictionality of consent; it is the desperate attempt to deny and repudiate this reality.

Most privacy consent is murky at best. I propose that privacy law should recognize a new form of consent that exists in the gray middle ground between full consent and non-consent. 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. Beyond the Binary

The law often treats consent as a simple binary – either people consent, and this opens upon 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 are unable to capture life in all its multifarious nuances. But the law must also avoid

[185] For example, as Elettra Bietti aptly notes, "the ideal of autonomous consent cannot be reached 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).

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."[186] 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."[187]

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 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 actually 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 non-consent, and most situations involving privacy fall somewhere in the middle. Murky consent should not confer the same legitimacy as full consent. Instead of providing nearly complete 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. Guardrails

Because murky consent is not binary, there is no one-size-fits-all set of

[186] KIM, CONSENTABILITY, *supra* note X, at 74, 81.
[187] *Id.*at 117-18.

rules to govern every situation. In most situations, however, there are some guardrails that can serve as an effective way to limit the power of murky consent and ensure that people are protected from the most harmful and troubling practices.

These guardrails involve government-imposed rules on the collection and processing of personal data, but they are designed not to completely override individual autonomy. The guardrails are designed to reflect reasonable expectations of individuals and embody principles of good faith and fair dealing. The guardrails aim to ensure what people would agree to and expect if they had the capacity to understand how their data will be used and the risks involved.

Ultimately, no set of guardrails can achieve perfection. People will consent to things that are less than ideal for them, and any approach that allows space for consent must accept this fact. Guardrails are not total controls; they define boundaries. They do not guarantee only the good or ideal; instead, they aim to prevent bad and treacherous situations.

The following guardrails are a starting point:

1. *Limited Scope.* Murky consent must have a limited scope in terms of data collected and how much data is used to achieve the purposes of collection.

    (a) *Limited Data Retention.* Personal data obtained via murky consent must have a reasonable retention period.

    (b) *Data Minimization*. Personal data obtained via murky consent must be the minimum necessary for the purposes.

2. *Duties to Protect Individuals.* Murky consent must be accompanied by robust duties to individuals.

    (a) *Duty of Loyalty*. At all times, the entity seeking murky consent must put the interests of individuals before its own interests.

    (b) *Avoidance of Unreasonable Risk*. Murky consent shall be invalid if it involves an unreasonable risk of harm to individuals, their rights, interests, and welfare.

3. *Appropriate Obtaining and Revoking.* Murky consent must be obtained in an appropriate manner, and individuals should always be able to revoke consent.

    (a) *Proportionality.* The method for obtaining murky consent must vary proportionately with the risk.

    (b) *Clean Hands.* Murky consent cannot be obtained through

improper means. It cannot be fraudulently or unethically obtained.

(c) *Revocability*. Murky consent must always be revokable.

4. *Avoidance of Societal Harm*. Murky consent must not cause unwarranted societal harm.

Rule 1, *Limited Scope,* reflects that murky consent grants only a restricted and narrow license to collect and process personal data. The more dubious the consent, the less powerful it should be. Limiting the scope of murky consent keeps it constrained and prevents the extent that personal data can be exploited. Acts of consent that extend for a significant duration of time are more troublesome. One reason why the law prohibits consent to slavery is because it is forever.[188] A broad consent to collect and process data eternally confers too much power on organizations. The goal of murky consent is to weaken the consent's power because of its dubious foundations.

Rule 2, *Duties to Protect Individuals,* addresses the importance of ensuring that individual interests are protected. 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.

The first component of this rule, *Duty of Loyalty,* aims to prevent organizations from putting their own interests ahead of the interests of individuals.[189] 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.[190] Fiduciary relationships are ones where there is a significant difference in the power of respective 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 of the other party and not take advantage of its position of heightened power.[191] The use of fiduciary duties to govern the relationships between powerful organizations and individuals has been embraced subsequently by many scholars, including Jack Balkin, Neil Richards, Woodrow Hartzog, Lauren Scholz, and others.[192]

---

[188] JOHN STUART MILL, ON LIBERTY (Norton ed. 1975) (noting that abdication of freedom by one "single act" undermines the "principle of freedom" which cannot be alienated). For other accounts about why one should not be able to consent to being enslaved, see KIM, CONSENTABILITY, *supra* note X, at 91-92.

[189] 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).

[190] SOLOVE, DIGITAL PERSON, *supra* note _, at 102-103.

[191] SOLOVE, DIGITAL PERSON, *supra* note _, at 102-103

[192] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183 (2016); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. Corp. L. 143 (2020); Neil M. Richards & Woodrow Hartzog, *The Surprising Virtues of Data Loyalty*, 71 Emory L.J. 985 (2022).

Under this approach, boilerplate contracts that waive rights to sue or force individuals into mandatory arbitration would be invalid, unless arbitration could be carried out in ways that do not diminish consumer rights and power.[193] 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.[194]

The second component of this rule, *Avoidance of 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 protection of 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 respect autonomy but impose limits to the extent to which individual foibles, gullibility, shortsightedness, and poor decisionmaking can unduly harm them.

Rule 3, *Appropriate Obtaining and Revoking,* addresses how murky consent is obtained and ensures that it can be revoked. Consent remains murky even if obtained via express consent mechanisms such as opt in, even if people are given special warnings. This is because these mechanisms do not ensure that consent is truly informed and meaningful. Although these mechanisms are highly imperfect and flawed, this does not mean that stronger mechanisms to obtain consent lack any benefit.

The *Proportionality* component of this rule 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 actually 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

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

[194] MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 33 (2012).

and makes people less likely to take consent seriously when it really matters.

As the risk increases, the means to obtain consent should strengthen as well. 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 a snap decision. 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 friction to the ability to collect and use personal data, and this friction increases the cost of using data in risky ways, which provides protection. This friction is not enough protection on its own, which is why consent obtained under heightened requirements would still be murky and would still require restrictions.

Note that high risk does not contradict the rule of avoiding an unreasonable risk. An unreasonable risk is different from a high risk because reasonableness examines both the cost and benefit. A high risk can be tolerated if the benefit is worth the risk. This rule requires judgment and cannot be reduced to a simplistic bright line rule. The law works out reasonableness case by case, over time, through countless situations. A clearer picture gradually develops, and norms emerge and evolve.

The *Clean Hands* component is a structural rule that prevents organizations from exploiting murky consent. Murky consent is dubious and ambiguous, but it is not fraudulent. Murky consent must not be obtained through fault. The law should restrict manipulation, bad faith, trickery, or other problematic methods of obtaining consent. Consent is a fiction, but there are different degrees of plausibility in fiction, from poetic license to an outright farce.

The *Revocability* component ensures that where individuals realize that the fiction of murky consent is not measuring up to what is in their best interest, they can revoke it. Although murky consent is designed to avoid swamping people with endless consent requests that they cannot handle, the goal is not to take control away from people when they actually want to exercise control. Revocability allows people to have some degree of control, even though individual control is fraught with difficulties.

Additionally, revocability creates a check on organizations from trying to get people to unwittingly consent to things they really do not want. 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 these terms.[195] People should be able to revoke their consent when they learn that they made a bad deal.

Revocability is essential. Although murky consent is fictional, it should not

[195] Nathan Good et al., *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, Proceedings of the 2005 Symposium on Usable Privacy and Security 43 (2005), http://law.berkeley.edu/files/Spyware_at_the_Gate.pdf.

be farcical. Revocability ensures that there always is a backstop; consent may be quite dubious, even almost non-existent, but revocability at least guarantees that there is always a way out, that people always have a choice. Revocability does not bless consent, but it prevents being trapped in hell with no escape.

Rule 4, *Avoidance of Societal Harm,* ensures that murky consent is invalid when it could cause unwarranted societal harm.[196] 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.[197] Privacy is not solely an individual interest; it has a social value and is an essential part of the fabric of 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, "If 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."[198] Beyond the fact these rights waivers are solely for the benefit of companies and not a benefit to individuals, the societal harm that these provisions cause should be another reason to reject them as a basis for murky consent.

* * *

These rules are a start, not a guarantee of sufficient protection for all situations involving murky consent. This disclaimer aside, these rules are basic guardrails that should provide strong protection in many circumstances. These rules allow for different forms of collection, use, and disclosure of personal information; the rules provide for flexible and proportionate limitations. Although these rules are proposed for murky consent, they can also be useful for other situations involving the collection, use, and disclosure of personal data without consent.

In setting forth these rules, I am not arguing that they are an inextricable part of murky consent. Other rules might work. In some circumstances, the rules I set forth might not be enough. These rules are just a way to flesh out what consent without magic might look like in practice. The key point is that murky consent comes with a small sandbox to play in, unlike regular

[196] 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." NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 49 (2019).

[197] 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 (2007).

[198] RADIN, BOILERPLATE, *supra* note __ at 135.

consent which can provide quite a large sandbox, and sometimes a gigantic one.

For these rules to work, there must be vigorous enforcement. Deferring to companies for their own judgment about risk is a recipe for disaster. Although companies should make these determinations in the first instance, they are too biased to be trusted to do this without careful monitoring, as there is a conflict of interest. Risk determinations must be examined by regulators. Companies must be accountable for their judgments and penalized if they make bad ones.

Organizations will want clarity and simplicity about what is low, medium, and high risk; they will want to have specific rules about what is unreasonable risk. But these issues are difficult to define in advance; they are best worked out case by case.

Regulators must scrutinize and audit the way organizations follow these rules. Rules are not self-executing, and they are meaningless unless they are followed rigorously in good faith. If organizations can follow these rules in a mechanical and perfunctory way, then the rules will turn hollow.[199] They will become like a rotten tree trunk, something that might appear fine on the outside but that will ultimately collapse in the long run. Regulators must be able to nullify murky consent whenever organizations fail to follow the rules.

Murky consent is a kind of grand bargain. The law will allow for a highly fictional form of consent and will 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 readily be transgressed. Using data with the limited license murky consent provides should be a bit uneasy, like walking a minefield. Organizations should always feel uncertain and humbled in their activities. This is a key virtue of the murky consent approach – organizations should not ever 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, the law should move beyond relying so heavily on consent to protect privacy. The law doesn't allow people to consent to taking dangerous and ineffective medications. The law doesn't make people figure out for themselves whether the food they buy will poison them. The law

[199] See ARI WALDMAN, INDUSTRY UNBOUND; Ari Ezra Waldman, *Privacy Law's False Promise,* 97 Wash. U. L. Rev. 773 (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."); Julie E. Cohen, *How (Not) to Write a Privacy Law,* Knight First Amendment Institute, at p.12 (2020) ("[D]ata protection in practice can reduce to an exercise in managerial box checking.").

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 in a position to do this.

Most privacy protections must exist beyond consent. Privacy law should focus primarily on issues of structure and power.[200] But a regime of privacy regulation cannot exclude consent without becoming too paternalistic. Murky consent adds guardrails and oversight; it is an attempt 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."[201] 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 sufficiently effective 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.[202] 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 still have choices, but there are many protections that are not a matter of individual choice.

Ultimately, the best regulatory regimes avoid excessive paternalism, preserve individual choice, yet also recognize that consent is quite impure and fraught with trouble. Allowing for consent is akin to playing with fire; if not done very carefully and thoughtfully, consent can readily become quite dangerous.

---

[200] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004); Daniel J. Solove, *The Myth of the Privacy Paradox,* 89 Geo. Wash. L. Rev. 1 (2021); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV 1879 (2013); Daniel J. Solove, *The Limitations of Privacy Rights,* 98 Notre Dame L. Rev. __ (forthcoming 2023).

[201] U.S. Food & Drug Administration, *Development and Approval Process | Drugs* (Aug. 8, 2022), https://www.fda.gov/drugs/development-approval-process-drugs.

[202] 49 C.F.R. 571 et seq.

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.

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

The law should stop trying to improve privacy consent in a futile hope of making it meaningful. Instead, the law should accept it for the fiction that it is. 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 realistic and practical. It is a way to move forward, past the consent dilemma that has stymied privacy law for decades.