2019

The Pathologies of Digital Consent

Neil M. Richards

Woodrow Hartzog

THE PATHOLOGIES OF DIGITAL CONSENT

NEIL RICHARDS[*] AND WOODROW HARTZOG[**]

ABSTRACT

Consent permeates both our law and our lives—particularly in the digital context. Consent is the foundation of the relationships we have with search engines, social networks, commercial web sites, and any one of the dozens of other digitally mediated businesses we interact with regularly. We are frequently asked to consent to terms of service, privacy notices, the use of cookies, and so many other commercial practices. Consent is important, but it's possible to have too much of a good thing. As scholars have documented, while consent models permeate the digital consumer landscape, the practical conditions of these agreements fall far short of the gold standard of knowing and voluntary consent. Yet as scholars, advocates, and consumers, we lack a common vocabulary for talking about the different ways in which digital consents can be flawed.

This article offers four contributions to improve our understanding of consent in the digital world. First, we offer a conceptual vocabulary of "the pathologies of consent"—a framework for talking about different kinds of defects that consent models can suffer, including unwitting consent, coerced consent, and incapacitated consent. Second, we offer three conditions for when consent will be most valid in the digital context: when choice is infrequent, when the potential harms resulting from that choice are vivid and easy to imagine, and where we have the correct incentives choose consciously and seriously. The further we fall from these conditions, we argue, the more a particular consent will be pathological and thus suspect. Third, we argue that our theory of consent pathologies sheds light on the so-called "privacy paradox"—the notion that there is a gap between what consumers say about wanting privacy and what they actually do in practice. Understanding the "privacy paradox" in terms of consent pathologies shows how consumers are not hypocrites who say one thing but do another. On the contrary, the pathologies of consent reveal how consumers can be nudged and manipulated by powerful companies against their actual interests, and that this process is easier when consumer protection law falls

* Koch Distinguished Professor of Law & Director, Cordell Institute, Washington University.

** Professor of Law and Computer Science, Northeastern University. For helpful comments on prior drafts and discussions on this topic, we would both like to thank Scott Baker, Danielle Citron, Jon Heusel, Jonathan King, and Katie Shilton. We would particularly like to thank Ari Waldman for his partnership in the conference that led to this paper, to Rachel Mance for her outstanding work in planning and running the conference, and to Luis Fernandez and Siri Nelson for their excellent research assistance.

far from the gold standard. In light of these findings, we offer a fourth contribution—the theory of consumer trust we have suggested in prior work and which we further elaborate here as an alternative to an over-reliance on increasingly pathological models of consent.

INTRODUCTION

Consent permeates our law. It is one of its most powerful and most important building blocks. This should be no wonder. We live in a society that lionizes individual choice in the many social roles we play every day, whether as consumers, citizens, family members, voters, lovers, or employees. Consent reinforces fundamental cultural notions of autonomy and choice. It transforms the moral landscape between people and makes the otherwise impossible possible.[1] It is essential to the exercise (and waiver) of fundamental constitutional rights, and it is at the essence of political freedom, whether we are talking broadly about a "social contract" or making political choices for individual candidates and referenda in the voting booth.

Consider the substantial amount of legal work that consent performs. It is the basis of contracts, whether for goods, services, real estate, or marriage. The consent of the governed is the basis for the rule of law in democratic societies and was an important basis for the American Revolution. Consent can also work magic. When consent is present, trespassers can become dinner guests, a battery can become a welcome pat on the back, and even what would otherwise be a sexual assault can become an act of intimacy.[2]

Consent's power, its usefulness, and its resonance with norms of autonomy and choice make it an easy legal tool to reach for when we want to regulate behavior. Just as activities that have no harm might warrant lesser (or no) regulation, what consenting adults choose to do together takes that activity presumptively beyond the law's regulatory power. This is true whether the activity happens in the open or behind the proverbial closed doors. Consent's power is particularly justified in cases of what we might

1. For a more developed history of consent for data practices and contemplation of its role, see NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019); Elizabeth Edenberg & Meg Leta Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, 21 NEW MEDIA & SOC'Y 1804 (2019); Meg Leta Jones, *The Development of Consent to Computing*, 2019 IEEE ANNALS OF THE HISTORY OF COMPUTING (forthcoming).

2. Edenberg & Jones, *supra* note 1, at 1804–05 ("Valid consent can render permissible an otherwise impermissible action. It transforms the specific relations between the consenter and consentee about a clearly defined action. We can consent to sexual relations, borrowing a car, surgery, and the use of personal information. Without consent, the same actions can become sexual assault, theft, battery, and an invasion of privacy.").

call "gold standard" consent—agreements between parties who have equal bargaining power, significant resources, and who *knowingly* and *voluntarily* agree to assume contractual or other legal obligations.

Perhaps nowhere has consent been deployed more frequently as a legal concept than in the context of digital goods and services. Consent is the foundation of the relationships we have with search engines, social networks, commercial web sites, and any one of the dozens of other digitally mediated businesses we interact with regularly. We are frequently asked to consent to terms of service, privacy notices, the use of tracking cookies, and so many other commercial practices. But it's possible to have too much of a good thing. As we and other privacy law scholars have documented elsewhere, while consent models permeate the digital consumer landscape, the practical conditions of these agreements fall far short of the gold standard.[3] Think about your own agreements with the social networks you use, the apps you install on your phone, or the Amazon Alexa that might sit, listening, in your kitchen or bedroom. Do you know what you agreed to? Have you read the agreements? Did you have a meaningful choice? While the answer to these questions is usually "no," the dominant legal regime that applies in the United States is that the terms and conditions of these services are valid as long as there is some kind of "notice and choice" to consumers.[4] In practice, and as enforced with occasional exception by the Federal Trade Commission (FTC), notice-and-choice models can be legally sufficient even if the notice is buried somewhere in a dense privacy policy, and the choice is take-it-or-leave-it—accept what a company wants to do with your data or not use the service at all.[5]

---

3. *See, e.g.*, NANCY KIM, WRAP CONTRACTS (2013) [hereinafter KIM, WRAP CONTRACTS]; MARGARET RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L.J. 1180 (2017) [hereinafter Richards & Hartzog, *Privacy's Trust Gap*]; Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*]; Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1880 (2013); Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529 (2007); Scott Peppet, *Unraveling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future*, 105 NW. L. REV. 1153 (2011); Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85 (2014).

4. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS iii (2010); Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405 (2010) [hereinafter Hartzog, *The New Price to Play*].

5. *See, e.g.*, Richards & Hartzog, *Privacy's Trust Gap*, *supra* note 3, at 1198; Richards & Hartzog, *Taking Trust Seriously*, *supra* note 3, at 444.

While criticism of the over-use of consent in the consumer privacy context is rising, critics lack a shared vocabulary with which to discuss when consent is legitimate, when it is flawed, and how to talk about and distinguish those flaws.[6] Our lack of the right words and concepts with which to talk about defects in consent models runs into the rhetorical, cultural, and legal power of consent. As a consequence, consent criticism can fail to gain traction in the minds of those who are undecided or who have taken consent's powerful "consenting adults" rhetoric at face value. This results in a projection of gold standard norms onto the deficient digital landscape in ways that we want to suggest are *pathological*. In this article, we offer a conceptual framework for *thinking* about when consent is valid and when it has pathologies, and a conceptual vocabulary for *talking* about different kinds of pathologies that consent models can suffer. Our analysis is focused on the consumer privacy context, but we believe that our model and the vocabulary of the pathologies of consent can be useful in many of the other areas of the law in which consent is frequently applied.

Let us be clear about our claim: We are not arguing for a wholesale rejection of consent. A legal system without consent would be so radically different from what we have that it would be almost unimaginable. More fundamentally, we believe that consent should retain its prominent place in our law generally. Our argument is more nuanced. Consent is undeniably powerful, and often very attractive. But we have relied upon it too much, and deployed it in ways and in contexts to do more harm than good, and in ways that have masked the effects of largely unchecked (and sometimes unconscionable) power.[7] The gold standard of consent to data practices has been articulated throughout our law as being "knowing and voluntary."[8] European law uses an analogous method to require consent that is "freely given, specific, informed," and voluntary.[9] But this ideal can only exist

6. *See* Solove, *supra* note 3, at 1880–81; *see also* Edenberg & Jones, *supra* note 1, at 1810–14 (arguing in favor of locating the normative core of consent for data practices).

7. *See* Solove, *supra* note 3, at 1894.

8. *See infra* Part I.

9. For example, the EU's new General Data Protection Regulation (GDPR) embodies this concept by defining "consent" to require "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Regulation 2016/679, art. 4(32), 2016 O.J. (L 119) 1, 34. Recital 32 of the GDPR explains further that "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement." Regulation 2016/679, pmbl. ¶ 32, 2016 O.J. (L 119) 1, 6.

under certain circumstances,[10] which is what we hope to illuminate in this essay. We argue that consent is most valid when we are asked to choose *infrequently*, when the potential harms that result from the consent are *easy to imagine*, and when we have the correct *incentives to consent* consciously and seriously. The further we fall from this gold standard, the more a particular consent is pathological and thus suspect.

Beyond the conceptual framework and vocabulary, we offer a third contribution to our understanding in this area. We believe that the theory of consent pathologies offered here complicates a seductive but simplistic story that has been offered in tech policy circles for over a decade. This is the notion of the "privacy paradox"—the idea that consumer anxiety about privacy is undermined by the fact that consumers act in privacy-diminishing ways in practice. Understanding this phenomenon in terms of consent pathologies reveals that consumers are not hypocrites who say one thing but do another that reveals their true preferences. On the contrary, the pathologies of consent show how consumers can be nudged and manipulated by powerful companies against their actual interests, and this phenomenon is easier when the legal regime that purports to protect consumers falls far from the gold standard. As a fourth contribution, we suggest that the solution is not to double down on our increasingly pathological models of consent, but to look to other mechanisms that are more sensitive to relationships and power differentials, such as those designed to inspire the social trust that makes consent less necessary.

Our argument has four parts. In Part I, "the Empire of Consent," we survey the many instances of consent in our law, illustrating both the varied work that consent performs and the varied tests for consent that courts and legislatures have produced. We show how different legal regimes produce different formulations on a continuum of how consent should be measured by the law, and how much consent is necessary in particular contexts. Toward the more restrictive end of the continuum, models of consent coalesce around the standard of "knowing and voluntary," for example in the relinquishment of a fundamental right such as the right to a jury trial. Yet in the digital context, the rhetorical practice of many technology companies is to talk like they are offering informed consent while offering something far inferior legal or practical matter.

10. *See* Edenberg & Jones, *supra* note 1, at 1805 ("Consent can be legally binding, as long as the transaction has met certain legal requirements or institutional standards defining the scope of consent. The legal notion of consent is built on the moral notion; however, problems arise when legally binding consent fails to capture the relevant morally legitimate transference of rights and obligations.").

The heart of our article is Part II, "the Pathologies of Consent," in which we offer a conceptual framework of the ways in which consent to data practices might fall short of the gold standard. We begin with a note on our methodology, adapted from the method by which the economist Richard Thaler developed a series of critiques of the dominant rational actor model in economics, thereby significantly contributing to the development of the field of behavioral economics.[11] We then offer three different sets of circumstances in which we suspect that consent may be less accurate, useful or legitimate. First, there is *unwitting consent*, which takes the "knowing" out of "knowing and voluntary." This can take at least three forms, including not understanding the legal agreement, not understanding the technology being agreed to, or not understanding the practical consequences or risks of agreement. Second, there is *coerced consent*, a consent that takes the "voluntary" out of "knowing and voluntary," for example in cases where a person is confronted with a choice between consent and the loss of an important asset such as their life or their job. Third, there is *incapacitated* consent, in which voluntariness is not available as a matter of law, such as with children and others who are categorically incapable of legally consenting.

In Part III, "Ideal Consent," we suggest a set of preconditions necessary for consent to achieve the ideal of being knowing and voluntary. Without these preconditions, we argue that consent models will not be particularly useful or legitimate. In fact, without these preconditions, consent models for data practices risk being harmful and corrosive to the very autonomy they seek to protect. First, the choice to be made must be *infrequent* (so as not to overload the capacity of our minds to make rational choices). Second, the *harms* which we might incur by granting consent must be *vivid* (i.e., they must be easy to imagine).[12] Third, the stakes of a decision to consent must be *significant* (i.e., there is ample incentive to take each decision seriously). Consent works well where these three criteria are satisfied. But where some or all of these criteria are not present, consent starts to lose both its usefulness and its very legitimacy. We call the presence of these three factors *gold standard consent*, and argue that it should be the benchmark against which the legal and ethical validity of consent are measured.

---

11. For Thaler's own description of his process, see RICHARD H. THALER, MISBEHAVING: THE MAKING OF BEHAVIORAL ECONOMICS (2016). For an application of this process in privacy law scholarship, see ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2010).

12. *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1027 (2013).

In Part IV, "Beyond Consent," we offer a roadmap for a world in which consent is cabined to the contexts in which it is most effective and most legitimate. As elsewhere in the paper, we use the example of the laws regulating consumer technologies powered by human information as our example. We argue that while consent will and should remain an important option in the legal toolbox, we should resist the easy but troublesome tendency of always going to consent in the first instance. In other words, we argue that consent should not be a common tool in modern data protection regimes. To use the parlance of Silicon Valley, consent does not scale. It is almost entirely incompatible with the modern realities of data and technology in all but the most limited of circumstances.

Instead, building on other work, we propose a privacy framework with a major focus on the concept of trust.[13] Trust-based protections would require parties in information relationships to protect the data placed in their care and to treat each other fairly and with deference. They would prohibit entrusted entities from asking for consent to practices that would make people unreasonably vulnerable. Lawmakers looking to embrace trust and minimize the pathologies of consent could leverage rules concerning the design of technologies and legal prohibitions on consent such as unconscionability to shift the policy conversation in a way that values both consent and privacy, and protects the millions and millions of human beings to whom these rules apply.

I. THE EMPIRE OF CONSENT

Consent flows through our legal system to such an extent that it would be almost impossible to imagine our law without it. Consent's importance in our law has been recognized for generations. Henry Sumner Maine famously observed in 1861 that "the movement of the progressive societies has hitherto been a movement *from Status to Contract*."[14] Maine's argument was that unlike the premodern societies characterized by social interactions structured by kinship and other forms of hierarchical ordering, modern societies were increasingly characterized by social interactions structured

13. *See generally* Richards & Hartzog, *Privacy's Trust Gap*, *supra* note 3; Richards & Hartzog, *Taking Trust Seriously*, *supra* note 3; ARI WALDMAN, PRIVACY AS TRUST (2018); Jack Balkin, *Information Fiduciaries and the First Amendment*, 46 U.C. DAVIS L. REV. 1183 (2016).

14. 1 HENRY MAINE, ANCIENT LAW 101 (J.H. Morgan ed., J.M. Dent & Sons 1917) (1861).

by contracts—private agreements whose chief hallmark was consent.[15] Consent thus became one of our basic social structures, and if we look for it, we can see it everywhere.

Let us take a moment to be precise about what we mean here. When we talk about "consent" in this article, we mean a legal relationship characterized in form or substance by agreement or a concurrence of wills.[16] In a moral sense, we mean to rely on Edenberg and Jones's definition of consent as "effective communication of an intentional transfer of rights and obligations between parties. Valid consent transforms the specific relation between the consenter and consentee about a clearly defined action."[17] In its strongest form, as Justice Story memorably put it in 1835, "[c]onsent is an act of reason, accompanied with deliberation, the mind weighing, as in a balance the good or evil on each side."[18] Yet as we will see below, the prevalence of consent in our law includes weaker forms, including presumed consent and even fictive consent. In this Part, we survey at a high level some of the ways in which Maine's observation about contractual ordering has proven correct by showing how our law can be viewed in a very real sense as an empire of consent.

Perhaps the easiest place to begin an appreciation of the role of consent in our law is the common law. As all lawyers are familiar, contract law's basic elements of offer and acceptance are predicated on the notion of consent. Contractual consent is objective, meaning it does not matter what you actually thought you were consenting to, only what you objectively manifested consent to.[19] Contract law also allows consent to alternative dispute resolution, via arbitration or mediation clauses, at least when such contracts are not adhesionary, and there is bargaining power between the contracting parties.[20]

Property law's hallmark is the right of alienation—the voluntary right to agree to transfer one's property, real or personal—to another.[21] This

15. Katharina Isabel Schmidt, *Henry Maine's "Modern Law": From Status to Contract and Back Again?*, 65 AM. J. COMP. L. 145, 154 (2017).

16. *Cf. Consent*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("A voluntary yielding to what another proposes or desires; agreement, approval, or permission regarding some act or purpose, esp. given voluntarily by a competent person; legally effective assent.").

17. Edenberg & Jones, *supra* note 1, at 1811.

18. 1 JOSEPH STORY, COMMENTARIES ON EQUITY JURISPRUDENCE § 222 (1835).

19. Hartzog, *The New Price to Play*, *supra* note 4.

20. *E.g.*, Sutton's Steel & Supply, Inc. v. Bellsouth Mobility, Inc., 776 So. 2d 589, 597 (La. Ct. App. 2000).

21. Thomas W. Merrill, *The Property Strategy*, 160 U. PA. L. REV. 2061, 2079 (2012).

principle runs throughout the law of property, but it is easiest to appreciate in the rules governing gifts, which require donative intent (a donor voluntarily intending (i.e., consenting) to give a gift to the donee), delivery (physical transfer of the gift to the donee), and acceptance (consent to the gift by the donee).[22] Similarly, consent allows exceptions to the right to exclude, whether by turning a trespasser into a dinner guest, or by allowing the creation of licenses, easements, and bailments.

Consent is less central in tort law, which imposes duties that flow to the general population or some subset thereof, like in the case of the duty to exercise reasonable care. But consent remains important, for it can work to assume the risks of someone else's actions. Thus, if you are my karate instructor, and you negligently (or even recklessly) injure me, I might be unable to recover if I sue you because I assumed the risk of engaging in the dangerous sport and consented to spar with you in the first place.[23] Or if you go to watch the Boston Red Sox and are injured by a foul ball, the Red Sox will probably be immune from suit because you are presumed to have accepted the risk of injury by consenting to watch them play at Fenway Park (or wherever).[24]

With respect to intentional torts like assault, battery, conversion, and trespass, consent is typically treated as an affirmative defense.[25] Consider a surgical procedure, which would be a legal battery without consent, and even where some consent is supplied can become a battery again when consent is exceeded.[26] Consider further the important role consent plays in the complex of "privacy torts," the subset of intentional torts dealing with the collection, dissemination, and use of sensitive personal information. The four torts recognized by William Prosser[27]—intrusion into seclusion, disclosure of private facts, false light publicity, and appropriation of likeness—are all negated by consent to the invasion of privacy.[28] Thus, for example, it violates the intrusion tort when a surgeon photographs a patient during cosmetic breast surgery, and the patient's consent form does not

22. Guardian State Bank & Tr. Co. v. Jacobson, 369 N.W.2d 80, 83–84 (Neb. 1985).
23. *E.g.*, Levine v. Gross, 704 N.E.2d 262, 263 (Ohio Ct. App. 1997).
24. Costa v. Boston Red Sox Baseball Club, 809 N.E.2d 1090 (Mass. App. Ct. 2004).
25. *Consent*, BLACK'S LAW DICTIONARY, *supra* note 16.
26. *E.g.*, Kaplan v. Mamelak, 75 Cal. Rptr. 3d 861 (Cal. Ct. App. 2008).
27. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960). For additional background about the privacy torts and Prosser's role in their creation, see G. EDWARD WHITE, TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY 176–179 (expanded ed. 2003); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).
28. RESTATEMENT (SECOND) OF TORTS § 652A(2) (1977).

cover such uses of the photographs.[29] Consent to have your image used for commercial purposes is also a defense to an action for appropriation of likeness for commercial gain.[30] Of course, there are more intentional torts governing the collection, use, and disclosure of information than the four recognized by Prosser. A full "expanded set" of privacy torts includes trespass, breach of confidence, defamation, and intentional infliction of emotional distress.[31] Yet even this broader group of torts can be negated by defense—a trespasser with permission becomes a licensee or even a guest,[32] permission to disclose eliminates a duty of confidentiality,[33] and you can permit (or pay) someone to say mean or false things about you. In all of these cases, if you consent, you cannot sue.

Beyond contracts, property, and tort, consent also plays an important role in the law regulating family and sexual relations. For over a century, courts have recognized that "[t]he fundamental principle of all marriage is mutual consent."[34] This principle was echoed in *Obergefell v. Hodges*, when the Supreme Court held that the Fourteenth Amendment protects the right of marital choice, a concept that runs throughout its analysis.[35] The foundation of the Court's analysis is thus its statement that the Fourteenth Amendment's liberty guarantee "extend[s] to certain personal choices central to individual dignity and autonomy, including intimate choices that define personal identity and beliefs."[36] The Court concluded that "[u]nder the Constitution, same-sex couples seek in marriage the same legal treatment as opposite-sex couples, and it would disparage their choices and diminish their personhood to deny them this right."[37] Consent runs broadly throughout the rest of family law as well; it can be the difference between a loving sexual act and sexual assault or rape. The age at which it becomes legal to engage in sexual activity is of course known as the "age of

29. Judge v. Saltz Plastic Surgery, 330 P.3d 126 (Utah Ct. App. 2014).

30. RESTATEMENT (SECOND) OF TORTS § 652C (1977).

31. NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES FOR THE DIGITAL AGE 158 (2015).

32. *E.g.*, State v. Pixley, 200 A.3d 174, 177 (Vt. 2018) (explaining that trespass requires a person to enter the land without legal authority or consent).

33. *E.g.*, Grimminger v. Maitra, 887 A.2d 276, 279 (Sup. Ct. Pa. 2005) (patient consent serves as an affirmative defense to a claim of a breach of physician-patient confidentiality).

34. *Recent Cases: Marriage — Validity — Common-Law Marriage — Mistake as to Existence of Prior Marriage Between the Parties*, 34 HARV. L. REV. 561, 561 (1921) (summarizing the holding of Great N. Ry. Co. v. Johnson, 254 F. 683 (8th Cir. 1918)).

35. 135 S. Ct. 2584, 2605 (2015).

36. *Id.* at 2597.

37. *Id.* at 2602.

consent."[38] Consent is also the key feature in the legality of some sexual activities in BDSM[39] and is also an issue when elderly married couples engage in sexual activity when one partner has lost the capacity to legally consent.[40]

Beyond the common law, consent also plays a critical role in the context of digital privacy regulation. In the United States, the dominant regime of privacy regulation is known as "notice and choice." As interpreted by the Federal Trade Commission under its Unfair and Deceptive Trade Practices authority, this has meant that consumers are presumed to have consented to data practices as long as there has been some kind of "notice" to the consumer about what is happening and some kind of "choice" about whether they want it to happen. A recent FTC report on company surveillance of consumers across digital devices (for example tracking laptop web browsing activity to deliver targeted ads to the same consumer on a cell phone) is illustrative of the FTC's approach:

> As with traditional forms of tracking, companies should offer consumers choices about how their cross-device activity is tracked. And, when companies offer such choices, the FTC Act requires that the companies respect them. To the extent opt-out tools are provided, any material limitations on how they apply or are implemented with respect to cross-device tracking must be clearly and conspicuously disclosed.[41]

In practice, however, such requirements are relatively easy to comply with, as all a company needs to do to avoid FTC liability for unfair or deceptive trade practices if challenged is show that their use of consent is neither deceptive nor unfair.[42] Thus "notice" can mean a vague but not false description of data practices buried deep within a long privacy policy and "choice" can mean no more than the choice to use the service in the first place (Apple, Android, or no phone at all, for example).[43] It is perhaps for

38. *E.g.*, State v. Holloway, 916 N.W.2d 338, 345 (Minn. 2018) ("What has been known as statutory rape—sexual conduct with a person not of the age of consent—has been a crime in Minnesota since it was first organized as a territory.").

39. *See* William Eskridge, *The Many Faces of Sexual Consent*, 37 WM. & MARY L. REV. 47, 49–50 (1995); Margo Kaplan, *Sex-Positive Law*, 89 N.Y.U. L. REV. 89, 117 (2014).

40. Alexander Boni-Saenz, *Sexual Advance Directives*, 68 ALA. L. REV. 1, 3–4 (2016).

41. FED. TRADE COMM'N, CROSS-DEVICE TRACKING: AN FTC REPORT 13 (Jan. 2017).

42. *Cf.* 15 U.S.C. § 45(a)(1) (prohibiting the use of "unfair" or "deceptive" trade practices in or affecting interstate commerce).

43. WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 58–72 (2017) [hereinafter HARTZOG, PRIVACY'S BLUEPRINT].

this reason that when Facebook CEO Mark Zuckerberg testified before Congress in response to a series of privacy scandals involving his company, his defense, first and foremost, was that Facebook puts its users in "control,"[44] a good sound bite, but one that can be all but meaningless as a legal requirement.

Consent within Europe's data protection frameworks is more rigorous than in parts of US privacy law. Indeed, unlike US law, the European Union (EU) treats privacy and the related but distinct concept of data protection as fundamental rights. Consent remains central to this fundamental rights-based approach, although Europe's modern data protection regime is skeptical of over-relying on the notion.[45] Recital Seven of the EU General Data Protection Regulation (GDPR explicitly states that "Natural persons should have control of their own personal data."[46] This control is effectuated significantly through the mechanism of "informed consent" as a basis for legitimizing data processing.[47] Beyond the GDPR, the reasoning behind the

---

44. Written Testimony from Facebook to House Energy and Commerce Committee for Record of April 11, 2018 Hearing (June 29, 2018), https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf [https://perma.cc/B7LR-L7XU] (note: the word 'control' is mentioned over 1,000 times). It goes on like this for a while. *See also* Dan Fletcher, *How Facebook is Redefining Privacy*, TIME (May 20, 2010), http://content.time.com/time/magazine/article/0,9171,1990798-4,00.html [https://perma.cc/D66L-4FG3] ("'The way that people think about privacy is changing a bit . . . . What people want isn't complete privacy. It isn't that they want secrecy. It's that they want control over what they share and what they don't.'"); Anita Balakrishnan, Matt Hunter & Sara Salinas, *Mark Zuckerberg Has Been Talking About Privacy for 15 Years—Here's Almost Everything He's Said*, CNBC (Apr. 9, 2018), https://www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html [https://perma.cc/Q4QM-JGFA] ("'When I built the first version of Facebook, almost nobody I knew wanted a public page on the internet. That seemed scary. But as long as they could make their page private, they felt safe sharing with their friends online. Control was key.'"); Emily Stewart, *The Privacy Question Mark Zuckerberg Kept Dodging*, VOX (Apr. 11, 2018), https://www.vox.com/policy-and-politics/2018/4/11/17225518/mark-zuckerberg-testimony-facebook-privacy-settings-sharing [https://perma.cc/DQ84-Q2GD] ("'Every time that a person chooses to share something on Facebook, they're proactively going to the service and choosing that they want to share a photo, write a message to someone, and every time, there is a control right there, not buried in settings somewhere but right there when they're posting, about who they're sharing with.'").

45. *See* Edenberg & Jones, *supra* note 1; *see also* Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is And What It Means*, 28 INFO. & COMM. TECH. L. 65, 68 (2019) ("[T]he GDPR is constitutionally skeptical of U.S. lawyers' favorite tool: consent, particularly of the low-quality or 'take it or leave it' variety. The GDPR's architects realized that if low-voluntariness consent could justify data activities, the GDPR would just become another exercise in clicking 'I agree' to unread, unnegotiable terms. The GDPR requires high-quality consent, on par with important life decisions, such as consent to medical treatment. In many contexts, the burdens the GDPR places on consent make consent impossible as mechanism to make data uses legal. Moreover, many rules in the GDPR are not waivable and continue to apply after somebody has consented to data use.").

46. Regulation 2016/679, pmbl. ¶ 7, 2016 O.J. (L 119) 1, 2.

47. Regulation 2016/679, art. 7, 2016 O.J. (L 119) 1, 37.

EU ePrivacy Directive is that it "enhances end-user's control by clarifying that consent can be expressed through appropriate technical settings."[48] But as we will discuss in the Parts that follow, hard-coding consent through legal or technical code is fraught at best. It also probably makes things worse because it offers an illusion of control that dulls impetus for meaningful change while entrenching the pathologies of the concept into the very design of information technologies.[49]

American constitutional law does not recognize a broad constitutional right to privacy the way the EU does. But when constitutional rights are at issue in privacy or elsewhere, U.S. law (like the EU) puts consent at the core of rights jurisprudence. Indeed, consent is at the very core of American constitutionalism. Consider these familiar founding words from the beginning of the Declaration of Independence: "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.—That to secure these rights, Governments are instituted among Men, deriving their just powers *from the consent of the governed*."[50]

Consent's importance runs throughout constitutional law, particularly with respect to the doctrine of waiver. Constitutional rights can be waived, and waiver is essentially the consent to give up that right. When it comes to waiver, however, the Supreme Court has made clear that consent to waiver must be clearly and freely given. Sometimes this is textual, such as where the Third Amendment expressly includes consent as a defense to the quartering of soldiers in private homes: "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[51] More significantly, numerous constitutional rights can only be waived where there is a showing that such waivers are *knowing*, *intelligent*, and *voluntary*. This is the case,

48. *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC*, at 3.4, COM (2017) 10 final (Jan. 10, 2017).

49. *See, e.g.*, HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 43; Lee Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, 4 OSLO L. REV. 105 (2017); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROTECT. L. REV. 423 (2018), https://edpl.lexxion.eu/article/edpl/2018/4/5/display/html [https://perma.cc/T4LA-HNE8] [hereinafter Hartzog, *The Case Against Idealising Control*].

50. THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776) (emphasis added).

51. U.S. CONST. amend. III.

for example, for both the right to counsel[52] and the right to trial by jury.[53] Many constitutional rights can also be contracted around. For example, the First Amendment permits non-disclosure agreements—contracts not to speak—such as where journalists agree with confidential sources not to disclose their names in exchange for a story.[54] The Supreme Court has held that such contracts are enforceable against the press consistent with the First Amendment even where the identity of the source is itself newsworthy.[55]

Consent is also a critical element of health law. Reflecting the importance of the human interests involved, rules for consent in the health context are strict in ways resembling constitutional law, often requiring a heightened form of consent known as "informed consent." One of the foundations of modern biomedical ethics is the Belmont Report, a product of the National Research Act of 1974, which established a commission to study the basic ethical principles that should undergird biomedical and behavioral research involving human subjects.[56] The Belmont report announced three "Basic Ethical Principles" of "respect for persons," "beneficence," and "justice," and it offered three "applications" of these principles, the first of which was "informed consent."[57] The Belmont Report's definition of informed consent states "[r]espect for persons requires that subjects, to the degree that they are capable, be given the opportunity to choose what shall or shall not happen to them."[58] In practice, the Report urged that subjects be given the relevant *information* on which to make their decision, that researchers ensure that test subjects have *comprehension* of the information surrounding their decision, and that decisions be made in accordance with the idea of *voluntariness*.

The Belmont Report has been tremendously influential in the field of biomedical ethics, and today its recommendations are reflected in the Common Rule, the ethical rule that governs U.S. government funded biomedical and behavioral research. The Common Rule prescribes detailed

52. Davis v. United States, 512 U.S. 452, 458 (1994).
53. Adams v. United States ex rel. McCann, 317 U.S. 269, 275 (1942).
54. Cohen v. Cowles Media, 501 U.S. 663, 669–70 (1991).
55. *Id. See generally* Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650 (2009).
56. The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, 44 Fed. Reg. 23,192 (Apr. 18, 1979).
57. *Id.* at 23,193.
58. *Id.* at 23,195.

substantive and documentary requirements for "informed consent."[59] There are extensive professional and academic literatures on informed consent in a variety of medical contexts reflecting substantial work and reflection. One classic treatise, for example, identifies five critical elements for truly informed consent—disclosure; comprehension or understanding; voluntariness; decision-making capacity or competence; and authorization.[60]

The "knowing and voluntary" waiver standard from constitutional law and the informed consent standard from biomedical ethics each represent a kind of what we might think of as a "gold standard" consent. One could add another such example from the commercial context—freely negotiated agreements between sophisticated parties who have equal bargaining power, significant resources, and who knowingly and voluntary agree to assume contractual or other legal obligations. These are the models from which consent derives its strength—decisions to engage in activity based upon full information and free, voluntary, and informed choice. They are consent in its strongest and most legitimate form.

Let's take a step back at this point and look at the forest rather than the trees. Our review of consent models in the law can be distilled into three important principles. First, consent requirements are prevalent in many—if not most—areas of American law, running throughout common law, constitutional law, and regulatory law. Second, consent models vary in how strictly they protect consenting individuals, from the stringent consent requirements in constitutional law and health and human subjects research all the way down to the opt-out consents in commercial transactions that are so common in the digital environment. Third, despite this variance, there does exist a "gold standard" of consent, which is stringent and highly protective of individuals, whether we call it "informed consent," "knowing and voluntary" agreement or waiver, or something else entirely. We would suggest that in spite of consent's variance in practice, it is this gold standard of consent that policymakers, advocates, and others refer to when they talk about consent. Indeed, even Facebook's public statements about "control" in the abstract evoke a much stronger notion of consent than the watered-down legal requirements under which the company operates in practice (at least in the United States). When companies like Facebook negotiate

59. *See* Common Rule, 45 C.F.R. §§ 46.116 (general requirements for informed consent), 46.117 (documentation requirements for informed consent).

60. RUTH R. FADEN & TOM L. BEAUCHAMP, A HISTORY AND THEORY OF INFORMED CONSENT 274 (1986); *see also* Natalie Ram, *Tiered Consent and the Tyranny of Choice*, 48 JURIMETRICS 253, 259–60 (2008).

acquisitions or commercial deals with other companies, they typically enjoy (for themselves) gold standard consent informed by the finest lawyers money can buy. Yet when their individual human customers agree to use their services, it is fair to say that the level of information and power available to those individual humans is some distance away from the gold standard. It is to this gap between the gold standard of consent companies enjoy and the weaker kinds of consent many consumers "enjoy" in the digital environment that we will now turn.

II. THREE PATHOLOGIES OF CONSENT

When he was a young academic, the American economist Richard Thaler kept a list of ways in which people consistently acted irrationally. Thaler's list was not merely a lark by a bored iconoclastic graduate student. His list documented a series of human behaviors that the dominant theory of economics, the rational actor theory, failed to adequately explain. Again and again, Thaler kept encountering observable patterns of human behavior that were squarely at odds with the foundational assumption of economics that human beings act rationally to maximize their utility.

Thaler's list became a research agenda, as he and others began experimental studies of the behaviors he had observed. This community of scholars kept working, and these critiques of the dominant rational actor model helped to create the field of behavioral economics.[61] This field proceeds from the evidence that human beings do not always behave as the rational actor model assumes that they would—Thaler refers to these fictional humans as "econs." Instead, the field assumes that people behave in an observable and empirically-demonstrable way like "humans": sometimes acting rationally, sometimes less than fully rationally, and sometimes irrationally. Behavioral economists, building on the work of Thaler and his mentors Daniel Kahneman and Amos Tversky, attribute these behaviors to cognitive structures—and limitations—in the human brain.[62] They argue that humans, in the words of another leading scholar in the field, are not merely irrational, but predictably so.[63] Kahneman offers helpful metaphor for understanding how the human mind works. Most of the time, we operate using "System One," an automatic system of cognition that relies upon heuristics and assumptions to help us navigate the world.

61. *See generally* THALER, *supra* note 11.

62. *See* DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2011); Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124 (1974).

63. *See* DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS (2008).

Other times, when we encounter something new or really want to think something through, we use what Kahneman calls "System Two." System Two is more analytical and rational, but it is also lazy and relies as much as it can on System One because "thinking slow" is taxing on our energies and on the sugar reserves in our brain. System One allows us to drive to work while what we think of as our mind ("System Two") is occupied by the news. System One allows us to carefully read a law review article, even though we might derive more pleasure when we breeze through a novel (or a Netflix stream) using System Two.[64]

In this Part, we adapt Thaler's list methodology to privacy law—specifically to three scenarios we have observed in which consumers in the digital environment "consent" to data practices in ways that seem irrational. We offer these cases as "Pathologies of Consent" and conclude that sometimes the behavior can be explained by defects in the law, especially where the law requires less than "gold standard" consent, whereas other times the behavior may be explained by particular features of human cognition. Nevertheless, like Thaler's list, our suggestions are theoretical. To the extent we make empirical claims, such claims are primarily anecdotal rather than (at present) proven by experimental social science. In this respect, we follow a similar privacy law methodology to the one used by Anita Allen in her classic work *Unpopular Privacy*.[65]

Thaler's list complicated a relatively simplistic story that the rational actor model told about human behavior. We believe that our list of consent pathologies complicates a more specific (but equally simplistic) rational actor story that has circulated in privacy circles for a number of years as the "privacy paradox." The "privacy paradox" is the assertion that although people might express a concern for privacy in the abstract, their actual behavior suggests that they do not actually care about their privacy in practice. Observers coming from a rational actor perspective suggest that the actions of consumers (what an economist would call their *revealed preferences*) indicate that consumers do not really care about privacy at all, and that concerns about privacy in the consumer context are overblown.[66] To return to Mark Zuckerberg's testimony before Congress, if Facebook puts consumers in *control* of their privacy, but consumers continue to consent to privacy-revealing practices and act in privacy-destructive ways, they have no one to blame but themselves. Buyers beware.

64. KAHNEMAN, *supra* note 62, at 20–24.

65. *See* ALLEN, *supra* note 11.

66. *E.g.*, Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, 41 J. CONSUMER AFF. 100 (2007).

We believe that the three pathologies we offer in this Part complicate this simplistic and self-serving story, and we explain why consumers might understandably care about their privacy *and* agree to data practices that undermine their privacy and expose them to the risks of informational harms. (We also note that scholars working in the Thaler tradition have already begun the process of experimental testing of the ways in which consumers understand privacy in practice, with initial findings that confirm the intuitive and theoretical model we offer here.)[67]

There are certainly more than three ways in which consent in practice can deviate from gold standard consent, but for present purposes the three we offer here will suffice. They are *unwitting consent*, *coerced consent*, and *incapacitated consent*.

A. Unwitting Consent

Let's say that you are signing up for a new account with a tech company whose app or web site will let you do something. Perhaps you are signing up for a loyalty club at your local coffee or bagel shop, perhaps you are signing up for a new taxi app, dating app, or social network, or perhaps your iPhone or Android needs a security update that you fear will lead to a data breach if you don't agree. Like most consumers, you're in a hurry. (In the bagel example, maybe the people queuing behind you want to buy their bagels,[68] or maybe you are just hungry and want to finish the transaction so you can eat.) In any event, most consumer transactions these days have an informational component—the social network you join, the bagel app you download, the web sites you read, or the car you buy. The problem is, most consumers don't know what data practices are possible, what they have agreed to, or what the informational risks of the transaction are.

This is the problem of *unwitting consent*. In the complex technological and legal landscape in which the contemporary digital consumer finds herself, understanding what is going on can be challenging. Yet people are harried, busy, and distracted, so they understandably click the "I agree" button and move on with their day, hoping that all will be well. This is

67. For excellent reviews of the theoretical and empirical research in this field, see Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442 (2016); Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015).

68. In full disclosure, this is exactly what happened to one of the authors of this article recently, at an Einstein Brother's Bagels. The friendly clerk urged him to install the loyalty app at the point of sale, while the hungry customers behind him pressured him into clicking "I agree."

unwitting consent. Unwitting consent takes the "knowing" out of "knowing and voluntary." Simply put, far too often, far too many people in the digital environment have little to no idea about what data practices or exposure that they are consenting to. Compounding this problem (and enabling business practices that create and prey upon unwitting consent) is the conclusion reached by several courts that privacy policies, standing alone, are simply not enforceable as contracts.[69] At the same time, privacy policies that are incorporated into the terms of use that people consent to by clicking "I agree" are generally recognized as part of a binding contractual agreement.[70]

In fact, one of the reasons consent is such a poor fit for data practices is that boilerplate contract law is largely agnostic to whether people actually know what they are agreeing to. This is known as the objective theory of contracts. Under this theory, the intent of the parties, for example, 'I thought I was agreeing to "X," is irrelevant. Instead, the contract is formed based on what a reasonable person would have been led to believe in the relevant context (an objective standard).[71] Although this doctrine is criticized by many as it applies to boilerplate contracts,[72] generally parties need not have a "meeting of the minds" in the classic contractual sense. Rather, a "reasonable communication" of the terms will suffice.[73] In data processing contexts with lengthy terms of use agreements, this dynamic puts all of the risk on the user, because consent can be effective even if you have no idea what you just agreed to. Once again, buyer beware.

Unwitting consent can take several forms. First, *consumers can fail to understand the legal agreement* governing the information relationship they now have with the company. This can happen when the legal agreement is

69. *In re* Nw. Airlines Privacy Litig., No. 04-126, 2004 WL 1278459, at *16–18 (D. Minn. 2004); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 316–18 (E.D.N.Y. 2005).

70. Hartzog, *The New Price to Play*, *supra* note 4, at 408; Woodrow Hartzog, *Website Design As Contract*, 60 AM. U. L. REV. 1635, 1635 (2011) ("When courts seek to determine a website user's privacy expectations and the website's promises to that user, they almost invariably look to the terms of use agreement or to the privacy policy.").

71. Hartzog, *The New Price to Play*, *supra* note 4, at 416; *see also* Wickberg v. Lyft, No. 18-12094-RGS, 2018 U.S. Dist. LEXIS 213281 (D. Mass. Dec. 19, 2018)

72. *See* KIM, WRAP CONTRACTS, *supra* note 3; RADIN, *supra* note 3; Hartzog, *The New Price to Play*, *supra* note 4.

73. *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 429 (2d Cir. 2004); Molnar v. 1-800-Flowers.com, No. 08-cv-0542, 2008 WL 4772125, at *7 (C.D. Cal. Sept. 29, 2008) (stating that "courts have held that a party's use of a website may be sufficient to give rise to an inference of assent to the terms of use contained therein"); Southwest Airlines Co. v. Boardfirst, LLC, No. 3:06-cv-0891, 2007 U.S. Dist. LEXIS 96230, at *5 (N.D. Tex. Sept. 12, 2007); Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974, 982 (E.D. Cal. 2000) (stating that "the browser wrap license agreement may be arguably valid and enforceable").

too long (such as Apple's notoriously lengthy Terms of Services Agreement),[74] the legal agreement uses confusing language, structure, and syntax (such as when consent forms deploy double and triple negatives or switch from "opt out" to "opt in" options in a series of choices),[75] the legal agreement is too technical for ordinary readers to understand (many privacy policies reference technologies like pixel tags and MAC addresses, which are likely foreign concepts to the average user),[76] or the legal agreement is too vague to specify exactly what is being agreed to (consider Amazon's notoriously vague "Privacy Notice" which features terms like "we share your information with third parties, to permit them to send you marketing communications."). [77]

A second dimension of unwitting consent is where *consumers do not understand the technology* that mediates their relationship with the company. For example, most people don't realize that telecommunications

74. Apple's iOS Terms of Service (TOS) is notoriously long. Its current version, for iOS12, is 6,901 words long. *iOS Software Agreement*, APPLE, https://www.apple.com/legal/sla/docs/iOS12.pdf [https:// perma.cc/VC8B-8V48]. However, Apple's web site also contains thirteen other TOS agreements for iOS 3.1, 4.1, 5.0, 5.1, 6.0, 7.0, 8.0, 8.1, 9.0, 9.1, 10, 11, and 11.2. In 2017, cartoonist R. Sikoroyak turned the related Apple iTunes TOS agreement into a 96-page comic book starring Steve Jobs as its hero and featuring classic comic book styles and characters from The Simpsons to Snoopy to Family Circus. *See* Bonnie Burton, *Steve Jobs, Superhero: Graphic Novel Meets iTunes Service Terms*, CNET (Mar. 8, 2017), https://www.cnet.com/news/itunes-terms-of-service-graphic-novel-comic-r-sikoroyak/ [http://perma.cc /DC88-8PS5].

75. Consider this example from a request by a California school system regarding student directory information:

4. Decline Release of Directory Information **(Note: most parents do not choose this option)**

Decline Release of Directory Information	
I **do not** want the District to release "directory information" (see Packet for examples) to qualified individuals or groups, such as official parent-teacher organizations, college recruiters, Oakland Education Fund, or employers.	
Student's Name	
Parent/Guardian's Signature	

HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 43, at 145. Or this confusing series of choices from "opt out" to "opt in":

☐ Please do not send me details of products and offers from Currys.co.uk

☐ Please send me details of products and offers from third party organisations recommended by Currys.co.uk

Trick Questions, DARK PATTERNS, https://darkpatterns.org/types-of-dark-pattern/trick-questions [https://perma.cc/7R7F-6FYD].

76. *Privacy Policy,* THE STREET, INC., http://corporate.thestreet.com/privacy [https://perma.cc/3WS9-RMT3].

77. *Amazon.com Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 [https://perma.cc/2AE4-B4L7].

systems are remarkably insecure.[78] We give consent to these companies upon the assumption that their systems will protect us, but we are often mistaken about how those systems are configured. A prominent recent example is the scandal over Facebook's user interface that allowed for the exfiltration of massive amounts of data to Cambridge Analytica, the data firm accused of, among other things, dubious data practices with respect to electoral politics.[79]

Technically, Facebook users "consented" to the collection and sharing of this data via their privacy settings.[80] Facebook went to great lengths to emphasize this fact, stating "Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information."[81] But a closer look reveals that this consent was basically manufactured through obfuscation, abstraction, and sleight of hand via a user interface. Users likely had little idea what they were agreeing to, in no small part because the way the technology actually worked was opaque to users.

Professor Ian Bogost, who also had an application using the same interface as that at issue in the Cambridge Analytica scandal, wrote of Facebook's system:

> App authorizations are not exceptionally clear. For one thing, the user must accept the app's request to share data with it as soon as they open it for the first time, even before knowing what the app does or why. For another, the authorization is presented by Facebook, not by the third party, making it seem official, safe, and even endorsed.[82]

---

78. Sarah Jamie Lewis (@SarahJamieLewis), TWITTER (Jan. 8, 2019, 10:34 PM), https://twitter.com/SarahJamieLewis/status/1082888359008120832 [https://perma.cc/U632-3P5F]; Joseph Cox, *Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911 Calls,* VICE, (Feb. 6, 2019), https://motherboard.vice.com/en_us/article/a3b3dg/big-telecom-sold-customer-gps-data-911-calls [https://perma.cc/DDH8-HEMH].

79. *See, e.g.*, *The Cambridge Analytical Files,* GUARDIAN, https://www.theguardian.com/news/series/cambridge-analytica-files [https://perma.cc/TL6P-PA3Y].

80. Ian Bogost, *My Cow Game Extracted Your Facebook Data,* ATLANTIC (Mar. 22, 2018), https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214/ [https://perma.cc/CN2R-9LD4].

81. Paul Grewal, *Suspending Cambridge Analytica and SCL Group from Facebook*, FACEBOOK: NEWSROOM (Mar. 17, 2018), https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytic a/ [https://perma.cc/76FD-7MUR].

82. Bogost, *supra* note 80.

Bogost was critical of Facebook's flimsy consent structure, explaining that "[t]he part of the Facebook website where apps appear, under the blue top navigation (as seen above), introduces further confusion. To the average web user, especially a decade ago, it looked like the game or app was just a part of Facebook itself."[83] Bogost noted the seamless nature of the website that lacked a clear boundary between Facebook's navigation and the third-party app. He explained that "[i]f you look at the browser address bar while using a Facebook app on the website, the URL begins with "apps.facebook.com," further cementing the impression that the user was safely ensconced in the comforting, blue cradle of Facebook's care.[84]

Of course, that impression bore little relationship to reality. When people opened a third-party app, Facebook's servers passed along a request to the server where the app developer hosts their services. Then, the app sent all of its responses back to Facebook, which formatted the responses as if they were coming from Facebook rather than the third party.[85] Through this setup, the third-party app was able to access significant amounts of personal and potentially sensitive information.[86]

As the previous description suggests, consumer are unlikely to understand the complexities of layered applications and their correlated, opaque, data flows. We certainly are no experts. Lacking such knowledge, the "consent" requested by Facebook in this manner seems farcical. Bogost accused Facebook of "presenting apps as quasi-endorsed extensions of its core service to users who couldn't have been expected to know better."[87] The reason people felt so violated by Facebook could be that "they might never have realized that they were even using foreign, non-Facebook applications in the first place, let alone ones that were siphoning off and selling their data. The website always just looked like Facebook."[88]

Another prominent example of unwitting consent involves third party tracking through the use of advertising technology, or "ad tech," as it is

83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.* (describing that as an app developer using Facebook's interface "I was able to access two potentially sensitive pieces of data without even trying. The first is a player's Facebook ID. . . . Those data could be correlated against other information—data collected from Facebook, fashioned by the app, or acquired elsewhere. . . . The second type of information is a piece of profile data [my app] received without asking for it. Back in 2010, Facebook still allowed users to join "networks" —affiliations like schools, workplaces, and organizations. In some cases, those affiliations required authorization, for example having an email address at a domain that corresponds with a university.").
87. *Id.*
88. *Id.*

known in the industry. Ad tech involves technologies like ad networks, which serve "as a broker between a group of publishers and a group of advertisers,"[89] and ad servers, which are "used by ad networks, publishers, advertisers, and ad agencies to manage, run, and report on their advertising campaigns."[90] These networks and technologies are remarkably complex, with auctions conducted in milliseconds and involve a bevy of different companies processing your data to serve ads personalized on the basis of that data.[91] Even advocates of consent regimes realize how daunting this problem is, conjuring up euphemisms like "consent strings" for ad tech to simplify and streamline compliance.[92]

In January 2017, the FTC released a staff report on the problem of cross-device tracking, the practice discussed above in which "platforms, publishers, and ad tech companies try to connect a consumer's activity across her smartphones, tablets, desktop computers, and other connected devices. The goal of cross-device tracking is to enable companies to link a consumer's behavior across her devices."[93] The FTC's proposed solutions to this problem, however, were underwhelming. It recommended merely that "companies engaged in cross-device tracking: (1) be transparent about their data collection and use practices; (2) provide choice mechanisms that give consumers control over their data; (3) provide heightened protections for sensitive information, including health, financial, and children's information; and (4) maintain reasonable security of collected data."[94] Consistent with much of American privacy law, this amounted to notice, choice, heightened notice and choice for a few sensitive areas, and data security.

---

89. Maciej Zawadziński, *What is an Ad Network and How Does It Work?*, CLEARCODE (Mar. 7, 2018), https://clearcode.cc/blog/what-is-an-ad-network-and-how-does-it-work/ [https://perma.cc/4D64-DP7D].

90. *Id.*

91. *Id.*

92. Nicole Lindsey, *Could GDPR Consent String Fraud Bring Down the Whole Ad Tech Ecosystem?,* CPO MAGAZINE (Dec. 5, 2018), https://www.cpomagazine.com/data-protection/could-gdpr-consent-string-fraud-bring-down-the-whole-ad-tech-ecosystem/ [https://perma.cc/V5MT-VUGF] ("A consent string is a unique series of numbers generated by a publisher's consent management platform (CMP) and then shared with all digital ad partners. The consent string includes information such as the identity of a vendor, whether or not they have user consent to use data to serve them personalized ads, and how any identifying personal data can be used. The most important consent data is a single bit (a '1' or a '0') that tells an ad tech vendor whether they can serve up personalized ads. If the value is '1,' then the ad tech vendor has user consent; if the value is '0,' then the ad tech vendor does not have user consent.").

93. FED. TRADE COMM'N, *supra* note 41, at i.

94. *Id.* at ii.

But given the complexity of ad tech, this puts companies in a nearly impossible situation: either they must simplify enough to keep the information digestible or be detailed enough to fully explain data collection and use practices, which requires some explanation of how the technology actually works. This approach will let everyone down, and consumers will be lost either way. As one of us has explained:

> The modern data ecosystem is mind-bogglingly complex, with many different kinds of information collected in many different ways, stored in many different places, processed for many different functions, and shared with many other parties. All that nuance gets glossed over when companies try to simplify and shorten information, the risk hidden or made to seem more benign through abstraction.[95]

But if companies are *too* specific, people will suffer from decision fatigue and depleted limited resources to actually reach or process the tomes of information thrown at them. Unwitting consent lies in every direction.

A third version of unwitting consent is that *consumers might not understand the consequences or risks of the informational relationship*. As a general rule, people have difficulty assessing future risks created by present decisions.[96] We're far too optimistic; we rely too much on the past and lived experience over reliable, generalizable data; we discount future costs too much; and we think the way things are now will stay that way.[97]

But this is what we are asked to do every time a company asks for consent to collect and process our data. Even on good days where people are feeling sharp and contemplative, they are asked to construct scenarios where the granting of consent might come back to bite them or somehow be used in an adverse way against them. But unlike playing football or having surgery, where at least people can get a ballpark sense of risk through guestimation,

---

95. Woodrow Hartzog, *User Agreements are Betraying You*, MEDIUM (June 5, 2018), https://medium.com/s/trustissues/user-agreements-are-betraying-you-19db7135441f [https://perma.cc/2MWQ-JCJC].

96. *See, e.g.*, Caroline Beaton, *Humans Are Bad at Predicting Futures That Don't Benefit Them,* ATLANTIC (Nov. 2, 2017), https://www.theatlantic.com/science/archive/2017/11/humans-are-bad-at-predicting-futures-that-dont-benefit-them/544709/ [https://perma.cc/4NPP-KHQG]; Kate Morgan, *Why You're So Bad at Predicting the Future,* MEDIUM (Jan. 3, 2019), https://medium.com/s/2069/why-youre-so-bad-at-predicting-the-future-68e14a5f41a4 [https://perma.cc/3SKY-CXN5]; Bruce Schneier, *Why the Human Brain is a Poor Judge of Risk,* WIRED (Mar. 22, 2007), https://www.wired.com/2007/03/security-matters0322/ [https://perma.cc/4PLD-DQQ7].

97. *See* Beaton, *supra* note 96.

there's an entire universe of consequences that most people don't even think about when asked for consent to data practices.

Privacy—the rules governing human information—is valuable because it helps protect against a wide array of harms. Privacy protects against so many harms, in fact, that it can be easy to overlook them. Some harms occur far downstream from the points of salience for people, like the point of collection, initial disclosure, or data breach. Consider consent to things like biometrics, particularly facial recognition technology.[98] These surveillance technologies intuitively implicate the dangers of surveillance: the chilling effect of being watched and a generalized fear of retaliation or adverse consequences that might follow.[99] But many of the harms of facial recognition might not immediately spring to mind when people ask for consent to use this technology. People's faceprints can make harassment and stalking easier.[100] They can gradually shift communally supported due process values like "presumed innocent" to "people who have yet to be found guilty of a crime."[101] They can facilitate the suffocation that follows when rules are perfectly enforced.[102] They can reduce the cost of sorting, categorizing, discriminating, and denying opportunities, benefits, or needed support and treatment in furtherance of surveillance capitalism.[103]

Data analytics and advertising surveillance can also involve this kind of unwitting consent. For example, consider how many times people are asked to click "I agree" to certain advertising technologies. There are credible allegations that the process used to target advertisements to internet users

98. Woodrow Hartzog & Evan Selinger, *Facial Recognition is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/45RL-6HXD].

99. *See* Neil Richards, *The Dangers of Surveillance,* 126 HARV. L. REV. 1934 (2013).

100. *See* Kevin Rothrock, *Facial Recognition Service Becomes a Weapon Against Russian Porn Actresses,* ARS TECHNICA (Apr. 26, 2016), https://arstechnica.com/tech-policy/2016/04/facial-recognition-service-becomes-a-weapon-against-russian-porn-actresses/ [https://perma.cc/F4HG-6SXF].

101. Anne-Marie Slaughter & Stephanie Hare, *Our Bodies or Ourselves,* PROJECT SYNDICATE (July 23, 2018), https://www.project-syndicate.org/commentary/dangers-of-biometric-data-by-anne-marie-sla ughter-and-stephanie-hare-2018-07?barrier=accesspaylog [https://perma.cc/4N8L-8FC9].

102. *See* Tara Francis Chan, *22 Eerie Photos Show How China Uses Facial Recognition to Track Its Citizens as They Travel, Shop—And Even Use Toilet Paper*, BUSINESS INSIDER (Feb. 12, 2018), http://www.businessinsider.com/how-china-uses-facial-recognition-technology-surveillance-2018-2 [http://perma.cc /TE5E-3HVX].

103. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2018); Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75 (2015); Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/47699 1/ [https://perma.cc/N64Q-ZYG7].

based upon surveillance of their reading habits allows inferences (and targeting) based upon sensitive characteristics, such as race, sexual orientation, health, pregnancy status, and other factors.[104] The possibly apocryphal big data anecdote that is now infamous in tech circles involves a story in the *New York Times Magazine* describing how retail giant Target was able to use a young woman's purchase history and other seemingly benign pieces of information to accurately guess that she was pregnant (and subsequently send her targeted advertisements) before the teenager's father found out.[105] In any event, predictive analytics are no doubt outstripping most peoples' notions of what is capable with data.[106] Asking people to consent to risks that seem like science fiction is another example of consent's sickness. But the bottom line remains that much if not most consent in the digital context suffers from the pathology of unwitting consent.

B. Coerced Consent

Sometimes a choice is not really a choice; it can be an unpleasant game of "would you rather" with a choice between a bad option and a terrible one. This is the problem of *coerced consent*, a choice that takes the "voluntary" out of "knowing and voluntary." Coerced consent can occur, for example, where a person is confronted with a choice between consent and the loss of an important asset such as their life or their job. "Coercion" is of course a provocative term. We use it intentionally here to describe a number of cases on the continuum from fully "voluntary" consent to truly involuntary "sign or die" consent. The closer we get to "sign or die," the more coercive a consent will be. While this category might include traditional forms of coercion that would invalidate agreements under the doctrine of duress, mediated environments that manufacture consent can also be coercive in more manipulative and subtle ways.

---

104. *See* Natasha Tiku, *Privacy Groups Claim Online Ads Can Target Abuse Victims*, WIRED (Jan. 27, 2019), https://www.wired.com/story/privacy-groups-claim-online-ads-can-target-abuse-victims/ [https://perma.cc/AE4D-8T4V].

105. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp [https://perma.cc/K247-ZGHZ]; *see also* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#7f3530266686 [https://perma.cc/B7FJ-7JX7].

106. *See, e.g.*, Hideyuki Matsumi, *Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?*, 48 CUMB. LAW REV. 149, 159–69 (2017).

Like the case of unwitting consent, coerced consent uses the language of gold standard consent to obscure unpleasant consequences. For example, in 2017 the U.S. Congress eliminated Obama Administration privacy protections limiting what cable providers like Verizon and Comcast could do with consumer internet browsing history. At a town meeting with constituents, Congressman James Sensenbrenner declared that when it comes to ISP privacy:

> Nobody's got to use the Internet. . . . Internet companies have invested an awful lot of money in having almost universal service now. The fact is that, you know, I don't think it's my job to tell you that you cannot get advertising for your information being sold. My job, I think, is to tell you that you have the opportunity to do it, and then you take it upon yourself to make that choice. . . . [sic] That's what the law has been, and I think we ought to have more choices rather than fewer choices with the government controlling our everyday lives.[107]

When pressed for clarification by the press, Sensenbrenner's office explained that "people can choose whether or not they want to use certain websites. For instance, in using Facebook, people have the option to agree (or not agree) with its terms of agreement, which covers what kind of information the social media site collects from its users."[108]

There are of course obvious problems with this logic—the very logic that has been used by industry and regulators to avoid meaningful privacy regulation in the United States for decades. First, to "choose" not to use the Internet is in a very real sense to "choose" not to participate in modern society or the modern economy. This might not quite be "sign or die," but it's close to "sign or not live like most people." Second, when it comes to Internet Service Providers, consumers often face no practical choice between providers. ISPs like Comcast or Verizon often operate in virtual or actual monopolies for broadband services. To "choose" not to use one's monopolist cable company for wired broadband is functionally to "choose" once again not to use the Internet at home. (Good luck streaming Netflix on your phone data plan.) Third, even with respect to individual services at the platform layer, there is once again a paucity of choice. If you want to use social networking to connect to your friends or family, Facebook is often

107. Kristine Phillips, *'Nobody's Got to Use the Internet': GOP Lawmaker Who Voted to Scrape Web Privacy Rules*, CHICAGO TRIB. (Apr. 15, 2017), https://www.chicagotribune.com/news/nationworld/politics/ct-sensenbrenner-web-privacy-20170415-story.html [https://perma.cc/JZS9-AZSS].

108. *Id.*

the only real choice. And even if your friends are on Instagram, Facebook (and its data practices) own that too.

Our point is that most consumers in the digital environment have highly limited options for consent, much less for bargaining. This is particularly the case where monopoly power or something like it applies. Even where there is some choice among services (Lyft versus Uber, for example), those services may offer functionally identical data terms. Finally, even where there is "choice" among alternatives, this is by no means the end of the ways in which firms can structure, influence, and nudge consumer choice in ways they desire. The coercion continuum is a function not only of the market power of companies, but also of those companies' power over the design of interfaces to shape and to influence consumer decision-making. This results in "dark patterns," a term coined by user experience designer Harry Brignull. According to Brignull, dark patterns are "tricks used in websites and apps that make you buy or sign up for things that you didn't mean to."[109] Security researcher Greg Conti calls these patterns "malicious" or "evil interfaces."[110] Conti and Edward Sobiesk define malicious interfaces simply as those that "deliberately violate usable design best practices in order to manipulate, exploit, or attack the user."[111] And they are *everywhere*.

Common examples of malicious interfaces include "disabled back buttons, browsers with 'sponsored' default bookmarks, unexpected and unnecessary forms, blinking advertisements, and pop-ups covering desired content."[112] These malicious interfaces often coerce users into disclosing private information.[113] Conti and Sobiesk identified eleven kinds of malicious interfaces:

Coercion – Threatening or mandating the user's compliance.

---

109. DARK PATTERNS, https://darkpatterns.org/ [https://perma.cc/7322-X5ME].

110. Gregory Conti & Edward Sobiesk, *Malicious Interface Design: Exploiting the User*, 2010 WORLD WIDE WEB CONFERENCE 271, 271 (2010), http://www.gregconti.com/publications/201004_malchi.pdf [https://perma.cc/5HN4-HUWY] [hereinafter Conti & Sobiesk, *Malicious Interface Design*] (arguing that security and human-computer interaction committees need to come together to fix deceptive designs); *see also* Tim Jones, *Facebook's 'Evil Interfaces,'* ELEC. FRONTIER FOUND. (Apr. 29, 2010), https://www.eff.org/deeplinks/2010/04/facebooks-evil-interfaces [https://perma.cc/PQT6-MSEV].

111. Conti & Sobiesk, *Malicious Interface Design*, *supra* note 110, at 271 (arguing that security and human-computer interaction committees need to come together to fix deceptive designs).

112. Gregory Conti & Edward Sobiesk, *Malicious Interfaces and Personalization's Uninviting Future*, IEEE COMPUT. SOC'Y & RELIABILITY SOC'Y 72, 72 (May/June 2009), http://www.rumint.org/gregconti/publications/j3pri.pdf [https://perma.cc/WWD2-S6B5] [hereinafter Conti & Sobiesk, *Malicious Interfaces and Personalization's Uninviting Future*] (noting that many individuals are tricked or coerced into divulging information they do not intend or do not want to divulge).

113. *Id.*

> *Confusion* – Asking the user questions or providing information that they do not understand.
>
> *Distraction* – Attracting the user's attention away from their current task by exploiting perception, particularly pre-attentive processing.
>
> *Exploiting Errors* – Taking advantage of user errors to facilitate the interface designer's goals.
>
> *Forced Work* – Deliberately increasing work for the user.
>
> *Interruption* – Interrupting the user's task flow.
>
> *Manipulating Navigation* – Creating information architectures and navigation mechanisms that guide the user toward interface designer task accomplishment.
>
> *Obfuscation* – Hiding desired information and interface elements.
>
> *Restricting Functionality* – Limiting or omitting controls that would facilitate user task accomplishment.
>
> *Shock* – Presenting disturbing content to the user.
>
> *Trick* – Misleading the user or other attempts at deception.[114]

Because companies have strong incentives to obtain consent, it is no surprise many of these malicious interfaces are used to coerce, wheedle, and manipulate people to grant it. Examples ranging in severity abound. Some terms of use agreements just won't let you say no. They only let you put off saying yes until "later." Other kinds of mediated consent leverage psychological pressure to manufacture consent. Consider the concept of what Brignull calls "confirmshaming," that is, "the act of guilting the user into opting into something. The option to decline is worded in such a way as to shame the user into compliance."[115] Consider the request from MyMedic to send users notifications, which forces those who do not wish to receive notification to click a button labeled "no, I prefer to bleed to death."[116] It's a subtle form of psychological coercion, but at scale these attempts can deplete our resolve.

---

114. Conti & Sobiesk, *Malicious Interface Design*, *supra* note 110, at 273.

115. *Confirmshaming*, DARKPATTERNS, https://darkpatterns.org/types-of-dark-pattern/confirmshaming [https://perma.cc/5BEZ-RCQL]; *see also Confirmshaming*, TUMBLR http://confirmshaming.tumblr.com/ [https://perma.cc/K8UA-N963].

116. MYMEDIC, https://mymedic.com/ [https://perma.cc/TZY3-HCTG].

Other examples abound. "Roach motels" make it easy to enroll or give consent, but difficult to leave.[117] "Forced continuity" quietly extends your consent past initial authorizations with affirmative opt-out obligations.[118] While Richard Thaler and Cass Sunstein's book *Nudge* offered an optimistic account of how to use the insights of behavioral economics to influence "choice architecture" for social good through what they called "benevolent paternalism," many tech companies today seem to be using it as a cookbook for coercive and manipulative decision structures.[119]

C. Incapacitated Consent

The third pathology of consent is incapacitated consent. Like coerced consent, incapacitated consent takes the "voluntary" out of "knowing and voluntary," but in this case it does so as a matter of law rather than as a matter of circumstance. Incapacitated consents are those where *voluntariness is simply not available as a matter of law*, such as with children and others who are categorically incapable of legally consenting.

While incapacitated consent may be the easiest of the pathologies to understand, here, too, some examples will help to illuminate the problem. Laws in the United States and Europe have regulated the ways in which companies can collect data about children for some time, though with limited effectiveness.[120] For example, the one area in which the United States has a generally applicable Internet data protection regime is the Children's Online Privacy Protection Act of 1998 (COPPA), which regulates online data collection from children. Yet even though the general age of contractual consent in the United States is 18, COPPA only regulates collection from children under the age of 13.[121] This means that even though children from 13–18 are legally incapable of contractual consent, it is perfectly legal to treat them as consenting adults for data collection purposes under the prevailing "notice and consent" regime.[122]

---

117. *Types of Dark Pattern*, DARKPATTERNS, https://darkpatterns.org/types-of-dark-pattern [https://perma.cc/G89G-FZDN].

118. *Id.*

119. *See* RICHARD R. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008); *see also* Conti & Sobiesk, *Malicious Interfaces and Personalization's Uninviting Future*, *supra* note 112.

120. *See* Simone van der Hof, *I Agree, Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World*, 34 WIS. INT'L L.J. 409, 412, 425 (2016).

121. 5 U.S.C. §§ 6501–6505 (2019); 16 C.F.R. § 312.2 (2018).

122. While an amendment to COPPA has been proposed that contains additional protections, the statute would still heavily rely upon consent. *See* Makena Kelly, *New Privacy Bill Would Give Parents*

In practice, moreover, whether legally or illegally, it has been trivially easy to circumvent the consent of legally incapacitated minors in ways that have led to serious financial and even physical harm. For example, both Apple and Facebook have come under fire for making it too easy for children to run up large debts in app stores or in-app purchases using their parents' credit cards.[123] More recently, the dating apps Tinder and Grindr were investigated by the UK government after police investigated more than thirty cases of child rape resulting from children avoiding the age checks on the application interfaces.[124] Companies may protest after such incidents that they do not intend minors to use their services (and that they put in place measures to forestall this). However, the combination of easy-to-install applications and a permissive regulatory regime makes it all but inevitable that minors will use apps and engage in online and offline activities, ranging from data collection to sex, that they lack the legal capacity to consent to. Simply put, a notice and choice regime coupled with the general goal of "putting users in control" cannot solve the problem of incapacitated consent.

While the Mark Zuckerbergs of the world might lionize control and consent, the digital consumers of the world face a very different reality than the idealized one presented by the CEOs and marketing departments of technology companies. The idealized model paints a picture of consent that evokes the knowing and voluntary gold standard, and relies upon the gold standard's power for its legitimacy. In practice, however, the version of consent that most consumers face is a significant and pathological departure from the gold standard. Unwitting consent takes the "knowing" out of "knowing and voluntary;" coerced and incapacitated consent take the "voluntary" out of "knowing and voluntary." Our articulation of this vocabulary for pathologies of consent is intended to provide a useful way to identify and critique the ways in which consents in practice fall short of the gold standard in theory. Once we can identify the problems, we will be better placed to prescribe solutions, and it is to this that we now turn.

---

an 'Eraser Button' and Ban Ads Targeting Children, VERGE (Mar. 12, 2019), https://www.theverge.com/2019/3/12/18261181/eraser-button-bill-children-privacy-coppa-hawley-markey [https://perma.cc/UU9X-LLG7].

123. *See* Nathan Halverson, *Facebook Knowingly Duped Game-Playing Kids and Their Parents Out of Money*, REVEAL NEWS (Jan. 24, 2019), https://www.revealnews.org/article/facebook-knowingly-duped-game-playing-kids-and-their-parents-out-of-money/ [https://perma.cc/4KLK-7QTR]; Press Release, Fed. Trade Comm'n, Apple Inc. Will Provide Full Consumer Refunds of at Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent (Jan. 15, 2014), https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million [https://perma.cc/P5UJ-4E2R].

124. *See* Ben Quinn, *Tinder and Grindr Face Questions Over Age Checks After Rape Cases*, GUARDIAN (Feb. 10, 2019), https://www.theguardian.com/society/2019/feb/10/tinder-and-grindr-face-questions-over-age-checks-children [https://perma.cc/Z5ED-8NKK].

III. IDEAL CIRCUMSTANCES FOR CONSENT

Although the notion of informed consent in digital environments is deeply problematic, it could still play an important role under the right circumstances. The key is to understand the conditions under which consent can meaningfully enhance autonomy and self-determination. Of course, as discussed above, the foundational notion of informed consent to data practices is that it must be "freely given, specific, informed and unambiguous." This includes notions of voluntariness and revocability.

However, we contend that the problem with consent for data practices isn't necessarily in the *form* or *substance* of the consent itself. Many scholars have examined how to substantively improve requests for informed consent.[125] But an additional, sometimes fatal, problem lies with the circumstances in which consent is given. Informed consent is only useful in particular contexts. If the circumstances and structure under which consent is asked and given are wrong, that consent will be ineffective even if it is "freely given, specific, informed and unambiguous." In this Part, we propose three circumstances necessary for an ideal environment for effective consent. To be meaningful, requests for consent must be *infrequent*, the risks of giving consent must be *vivid* and easy to envision, and data subjects must have an *incentive to take each request seriously*. Sadly, these conditions are scarce in modern data exchanges, but we believe that identifying the problems consumers face in these transactions allows us to identify the contexts in which consent can do valuable and legitimate work.

A. Infrequent Requests

One key to understanding why the pathologies of consent to data practices are so problematic in the digital environment is the fact that there are no limits on the number of requests for consent. Every day, every digital consumer is implicitly or explicitly asked to consent to data collection and processing practices for many, if not most, of the websites they visit, the online accounts they create, the services they sign up for, and the apps they use. Consider your web browsing on laptop and phone, GPS navigation, search engines, smartphone operating systems, social networks, taxi services, travel booking, video and audio streaming services, and all of the

125. *See, e.g.*, Florian Schaub, Rebecca Balebako, Adam Durity & Lorrie Faith Cranor, *A Design Space for Effective Privacy Notices*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 365 (Evan Selinger et al. eds., 2018); Batya Friedman, Peyina Lin & Jessica K. Miller, *Informed Consent by Design*, *in* SECURITY AND USABILITY 495 (Lorrie Faith Cranor & Simson Garfinkel eds., 2005).

other "free" or paid services you use which serve you ads or otherwise collect your data. The result is a casual familiarity turned ennui that leads us to gloss over the terms because we know that another request is just around the corner. Because each consent request is a drain on our time and cognitive load, we wisely choose to conserve our efforts. As one of us has written elsewhere,

> Anyone that has turned off notifications for apps like Facebook's Messenger can attest to the relentless, grinding requests for the user to turn them back on almost every time the app is opened. Many can relate to the experience of a child asking for candy, over and over, until the requests become too much to ignore and we give in, simply to quiet them. Willpower can feel like a finite, vulnerable, and subjective resource, and systems are designed to deplete and erode it. Once our willpower and ability to make choices has been compromised, the control users have been given is meaningless.[126]

Compare this depressing state of affairs to environments with informed consent, such as medical treatment, clinical trials, surgeries, and scientific research. Request for consent to these practices do not come often, by sheer virtue of the fact that treatment and trials are relatively uncommon. Thankfully, surgery is not a daily routine. This provides a necessary downtime and the space to both take consent requests seriously and go about living the rest of our lives. People have the ability to consider informed consent to surgery carefully because they know that they will not be asked for consent to another surgery in a few minutes. Critically, if they decline to give consent to a surgery, people know that they won't be pestered again and again until they say yes. Necessary medical intervention is something of a flashpoint in time: people either agree or don't agree to treatment and then get on with it. Practically speaking, the very need to ask for consent to surgery just doesn't present itself very often.

There is no such practical constraint for consent requests for data collection and processing. Data collection and sharing in the modern world is frequent, and is becoming as routine as walking, eating, and breathing. Data subjects are ceaselessly bombarded with requests for consent. There are no limits on the number of times a company is allowed to ask for a

126. *See, e.g.*, Hartzog, *The Case Against Idealising Control*, *supra* note 49, at 429 (footnote omitted) (citing AM. PSYCHOL. ASSOC., WHAT YOU NEED TO KNOW ABOUT WILLPOWER: THE PSYCHOLOGICAL SCIENCE OF SELF-CONTROL (2012), https://www.apa.org/helpcenter/willpower.pdf [https://perma.cc/A2DH-QBE8]); John Tierney, *Do You Suffer From Decision Fatigue?*, N.Y. TIMES (Aug. 17, 2011), https://www.nytimes.com/2011/08/21/magazine/do-you-suffer-from-decision-fatigue.html [https://perma.cc/LJ68-4MJ6].

person's consent, and there are no limits on the number of companies that may simultaneously ask for it. Even if we could consider each individual request rationally, our cognitive bandwidth is overwhelmed.

If consent is to be effective, it must happen infrequently. This means hard choices regarding which requests are more important than others and which kinds of companies should be prioritized. This might feel inherently paternalistic. Who are lawmakers to demote the importance of particular requests? But when all consent requests are important, none of them are. Failing to limit who can ask for informed consent, when they can ask, and how many times ignores the reality that people need time and space if their choices are to be meaningful. When choices are too frequent, consent loses its moral legitimacy as a justification for action.

B. Vivid Risks

At the JFK Medical Center, the consent form for open heart surgery explicitly states that the risks for the procedure include "bleeding requiring blood transfusion or return to surgery for repair, nerve damage, heart, liver, kidney or lung complication and/or even in rare cases death."[127] That's serious stuff. But the list goes on, including "complications arising in the post-operative period preventing normal recuperation. . . . [including] long term ventilation, confusion, fluid accumulation of the lungs, pneumonia, cardiac arrhythmias, fever and abnormal laboratory results. Also infection, long term healing and/or scarring of the surgical site incisions may occur and may require further treatment including surgical repair."[128]

Scars, bleeding, fluid accumulation, and death. These are *vivid*—and thus easy—risks for us to envision. So is the risk of consenting to things like government searches, which might result in imprisonment. These risks might even be *too* vivid, as once we've thought of them they can be difficult to push out of our heads.[129] We even consent to accept the risk of harm in everyday goods and services like rental car agreements that hold the driver

127. JFK MEDICAL CENTER, CONSENT FORM FOR OPEN HEART SURGERY 1, https://jfkmc.com/util/forms/Consent-for-Open-Heart-Surgery.pdf [https://perma.cc/QA4V-GKLC].

128. *Id.*

129. *Cf.* KAHNEMAN, *supra* note 62, at 326 (discussing experimental research suggesting that such so-called "vivid" outcomes tend to be viewed as more likely by human brains than a strict rationality calculus would suggest). One of the ongoing debates for informed consent to surgery is that the more vivid risks, even if incredibly unlikely, might have undue sway over a patient's decision. *See* David Thomasma, *Telling the Truth to Patients: A Clinical Ethics Exploration*, 3 CAMBRIDGE Q. HEALTHCARE ETHICS 375 (1994).

responsible for losses or dry cleaners who limit liability for damage to clothes to things like replacing or repairing. But personal data is different from bodily integrity or damage to our liberty or property. The risks of data practices are so opaque that there's an ongoing debate as to whether they should even be legally recognized.[130] Certain kinds of surveillance and data practices might be "creepy," but that's the word we use when we have difficulty specifying exactly the risks we are facing.[131] In fact, most of the risks we face from modern data practices arrive not with a bang but a whimper, if we hear them at all. Information is accumulated bit by bit, with risk accruing incrementally. This makes envisioning the plethora of harms difficult because there is rarely a single moment in time that people can point to when the envisioned risk materializes. Unlike severed arteries and being put in prison, how can people envision "databases of ruin" that have reached the critical mass of jeopardy?[132] Informed consent regimes for data will only work if the risks are vivid.

Even worse, these risks that we are being asked to waive through consent might materialize without our even knowing it. People typically know when they have a heart attack or suffer complications from surgery or pharmaceuticals. But our data could be being used against us this very moment, and we wouldn't know it. Hackers could, right now, be opening credit cards in your name as a result of that data breach last year that you didn't know you were involved in either. That lack of feedback further frustrates our ability to adequately envision the risks. Even when manifested, data harms often stay hidden. And our risk calculus is further funneled into wild speculation, paranoia, or overconfidence.

Of course, some data-related harms are easy to envision, such as being humiliated because a deeply-held secret is revealed, having your identity stolen, or being fired or denied insurance coverage on the basis of a personal data dossier or big data prediction. But the problem is that these harms are difficult to predict and difficult to trace from particular disclosures of information. This leads us to our final pre-condition for gold standard consent.

---

130. *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1 (2011) (offering a theory of privacy harm as legally-cognizable); Daniel Solove & Danielle Keats Citron, *Risk & Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018) (same).

131. Evan Selinger, *Why Do We Love to Call New Technologies "Creepy?,"* SLATE (Aug. 22, 2012), https://slate.com/technology/2012/08/facial-recognition-software-targeted-advertising-we-love-to-call-new-technologies-creepy.html [https://perma.cc/KXT6-7UMY]; *see also* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 3.

132. Paul Ohm, *Don't Build a Database of Ruin*, HARV. BUS. REV. (Aug. 23, 2012), https://hbr.org/2012/08/dont-build-a-database-of-ruin [https://perma.cc/G2MS-QR48].

C. Incentives to Take Each Request Seriously

Certain decisions demand to be taken seriously. The reason people hesitate before consenting to skydiving and surgery is that if it goes wrong, they could die. Mental and physical safety are powerful motivators to understand the risks of particular decisions. Imprisonment and exoneration are powerful motivators to weigh when granting consent to government searches. Even some frequent decisions to grant consent demand to be taken seriously, like participating in sports involving physical contact. It's not just that the choices are infrequent and the risks are vivid. It's that for gold standard consent there must be a clear incentive to critically analyze and deliberate the request for consent because of the magnitude of the stakes involved and the close relationship between the consent and those stakes.

Requests for informed consent are, by definition, individualized and atomized. The moral weight of these frameworks is concentrated in the information delivered to the subject and the subject's voluntary execution of a legally significant choice. Through this call and response, people's autonomy is ostensibly respected, which can justify a host of actions that would otherwise be objectionable. But these justifications break down when people have little incentive to meaningfully consider what is being asked of them. This incentive can be diminished either because the stakes appear insignificant or because people cannot easily see how their decision is consequential because the relationship between the consent and the risks is too remote. Others simply have little incentive to take each request seriously because they feel powerless.[133]

Consider the common fatalistic sentiment that privacy is already dead.[134] Ian Bogost argues that it's hopeless to try and opt out of surveillance capitalism, proclaiming that "the age of privacy nihilism is here."[135] Bogost

---

133. Kimberlee Morrison, *Pew: Internet Users Feel Powerless Against Digital Data Mining*, ADWEEK (Nov. 12, 2014), https://www.adweek.com/digital/pew-internet-users-feel-powerless-digital-data-mining/ [https://perma.cc/manage/create?folder=4014-40406-40412-48449] (describing PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA (Nov. 12, 2014), https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [perma.cc/6VDK-5UFP]); Brian Byer, *Internet Users Worry About Online Privacy But Feel Powerless to Do Much About It*, ENTREPRENEUR (June 20, 2018), https://www.entrepreneur.com/article/314524 [https://perma.cc/2YR6-ZLQS].

134. *See* Neil M. Richards, *Four Privacy Myths*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 33 (Austin Sarat ed., 2015) (debunking the "Privacy is Dead" myth).

135. *See* Ian Bogost, *Welcome to the Age of Privacy Nihilism*, ATLANTIC (Aug. 23, 2018), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198/ [https://perma.cc/A83C-GEJE].

paints a bleak picture, in which "[e]verything you have done has been recorded, munged, and spat back at you to benefit sellers, advertisers, and the brokers who service them. It has been for a long time, and it's not going to stop."[136]

It's hard to blame anyone who feels this way, even if there's so much privacy left to fight for.[137] Tech companies are now the backbone of the American economy. They are multi-billion dollar companies that have their fingers in nearly every aspect of our lives. Even if people were merely skeptical of the tech giants with the most personal data, sometimes called the "Big Five" (Amazon, Google, Facebook, Apple, and Microsoft), people would likely find it difficult, if not impossible, to live a normal, modern life without interacting with them.[138] For the ninety-one percent of Americans that feel that they have lost control over their data, why should any single request for consent compel any forethought at all?[139] Under this view, our consent is a *fait accompli*—something to quickly agree to without deliberation, because there is little point in resistance.

Another way consent can break down is it can be very difficult to draw a line from the practices that need consent to the stakes of the decision. Data harms, unlike physical harms, are not localized. They occur offstage and far away, on servers in remote countries and in boardrooms in faraway cities. The Internet is littered with infographics attempting to chart the flow of data from users to platforms to third party vendors and onward downstream.[140] The expanse of it all is mind boggling. In this light, data subjects have little reason to avoid clicking "I agree" because the services they are using are local, such as the Facebook or Uber app, and the risks are remote, such as unobserved data flows on the other side of the world. Again, people would have little incentive to deliberate because, frankly, they have little notion of the stakes, and the benefits of consent are right at their fingertips.

Finally, consent justifications are weakened when each particular request is just one tiny piece of the larger risk puzzle. Our consent to data practices

---

136. *Id.*

137. Evan Selinger, *Stop Saying Privacy is Dead*, MEDIUM (Oct. 11, 2018), https://medium.com/s/story/stop-saying-privacy-is-dead-513dda573071 [https://perma.cc/WD74-6DUZ].

138. For an in-depth exploration of the difficulties of escaping the Big Five, see Kashmir Hill, *Life Without the Tech Giants*, GIZMODO (Jan. 22, 2019), https://gizmodo.com/life-without-the-tech-giants-1830258056 [https://perma.cc/2P4E-E9J6].

139. *See* Kimberlee Morrison, *Pew: Internet Users Feel Powerless Against Digital Data Mining*, ADWEEK (Nov. 12, 2014), https://www.adweek.com/digital/pew-internet-users-feel-powerless-digital-data-mining/ [https://perma.cc/2SNP-F296].

140. *See, e.g.*, ImBrentJames, *A Healthcare Data Flow Diagram Showing the Complexity That TKY Could Help Simplify*, REDDIT (Aug. 2017), https://www.reddit.com/r/THEKEYOFFICIAL/comments/99q4ny/a_healthcare_data_flow_diagram_showing_the/ [https://perma.cc/2V22-98M4].

is astonishingly dispersed. Thousands of apps and services ask us for small, incremental disclosures, few of which involve the kind of information collection that might give people pause. While dating apps and platforms that collect sensitive and large amounts of personal data might cause some people to consider their risks, it's not as though people share all their information at once. Instead, it trickles out over time, such that our incentives to deliberate at the point of agreement are small because we don't know how much information we will ultimately end up sharing. Most of the time, it probably seems like a small amount. This is like the problem of death by a thousand cuts. And there's little guidance for people regarding which individual cuts matter. So people make the transaction-rational decision to chalk up each individual request for consent as "no big deal" in perpetuity. Such an environment is no place to condition our well-being.

Finally, people don't have great incentives to weigh the externalities of consent. That is, typically people only consider how a particular consented-to action will affect themselves. By allowing consent to companies to collect and process my data, those companies can then better target ads to everyone else who uses the service. One person's data becomes a point of comparison that allows for refined targeting, processing, and use elsewhere in the system. People probably don't take into account this externality when deciding whether to agree or not to give consent for data processing. There just aren't enough incentives for people to consider the implications of data processing for other people on a consistent basis, which creates a collective action problem, another pathology of consent to data practices to add to the list.

IV. BEYOND CONSENT

America desperately needs a new direction for its privacy rules. Notions of consent, control, and transparency have dominated data protection discussions for years, and the result is a sea of "I agree" buttons, drop-down menus, and switches that we are unable to navigate.[141]

In terms of meaningfully protecting our privacy, this approach has been a spectacular failure. The shortcomings of consent and transparency are

141. We have offered a preliminary version of these thoughts here: Woodrow Hartzog & Neil Richards, *It's Time to Try Something Different on Internet Privacy*, WASH. POST (Dec. 20, 2018), https://www.washingtonpost.com/opinions/its-time-to-try-something-different-on-internet-privacy/2018/12/20/bc1d71c0-0315-11e9-9122-82e98f91ee6f_story.html?utm_term=.5cd05e778a52 [https://perma.cc/F67G-DF5Y].

particularly visible in the United States. Congress is still trying to settle on its approach to privacy, but most of the current proposals still build off the notice and choice model.[142] The FTC has made a heroic effort to be the top U.S. privacy cop, but it has been starved of the legal tools and financial resources it needs to do a proper job.

America has a bad reputation for privacy.[143] The world is watching and judging, and the economic stakes are enormous. International data flows are essential for the global economy to function without fundamentally—and expensively—restructuring the Internet to America's huge financial detriment. American tech companies depend on being able to smoothly import European data for processing. But, in 2015, a European Court ruled that America's privacy protections were so poor that it struck down the "Safe Harbor" agreement, which helped enable an international flow of data.[144] Our current data sharing agreement with Europe, called the EU/U.S. "Privacy Shield," is in jeopardy.[145] If it fails, we will need a good replacement.

Europe and others have encouraged the U.S. to adopt a law similar to the EU's new General Data Protection Regulation. But a "U.S. GDPR" seems destined to suffer from the same consent pathologies we have explored in this article. As discussed above, the GDPR and forthcoming ePrivacy directive borrow too heavily from the control and transparency playbook.

---

142. CAMERON F. KERRY, BROOKINGS INSTITUTE, BREAKING DOWN PROPOSALS FOR PRIVACY LEGISLATION: HOW DO THEY REGULATE? (Mar. 8, 2019), https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate/ [https://perma.cc/QGR9-FUYL]; CAMERON F. KERRY, BROOKINGS INSTITUTE, WHY PROTECTING PRIVACY IS A LOSING GAME TODAY—AND HOW TO CHANGE THE GAME (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/5HVK-FLHS]; CONSUMERS INT'L, THE STATE OF DATE PROTECTION RULES AROUND THE WORLD (2018), https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf [https://perma.cc/6N5L-DRLR].

143. MARY MADDEN, PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA (Nov. 12, 2014), https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [perma.cc/6VDK-5UFP]; *Copy That: America Should Borrow From Europe's Data-Privacy Law*, ECONOMIST (Apr. 5, 2018), https://www.economist.com/leaders/2018/04/05/america-should-borro w-from-europes-data-privacy-law [https://perma.cc/RKM2-3ENN]; Samuel Gibbs, *What Is 'Safe Harbour' and Why Did the EUCJ Just Declare It Invalid?*, GUARDIAN (Oct. 6, 2015), https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection [https://perma.cc/B4PS-SFV8].

144. *See* Ellen Nakashima, *Top E.U. Court Strikes Down Major Data-Sharing Pact Between U.S. and Europe*, WASH. POST (Oct. 6, 2015), https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html?utm_term=.9ac8bcde9495 [https://perma.cc/SUK3-WD6M].

145. *See* Hayley Evans & Shannon Togawa Mercer, *Privacy Shield on Shaky Ground: What's Up With EU-U.S. Data Privacy Regulations*, LAWFARE (Sept. 2, 2018, 2:31 PM), https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations [https://perma.cc/895C-Y3EW].

Our current approach too often results in nothing more than cluttered minds and inboxes, with people resigned to take-it-or-leave it choices for ad-supported web or social media. Relying upon consent to justify data practices rests on the dubious assumptions that people understand what they are being told, and we can meaningfully calculate the risk of our choices online and exercise agency through mediated technologies.

It should be no wonder that under this framework, privacy—our human information policy—has begun to fall apart, often in breathtaking ways. We've seen a cascade of high-profile privacy failures like the Edward Snowden disclosures, the Cambridge Analytica scandal, the targeting of fake news based on data about political preferences, and data breach after data breach after data breach. Backing this up is an entire ecosystem dependent upon an illusion of control and wheedling, cajoling, and extracting consent by any method possible.

In spite of the failures of control and transparency, some lawmakers are considering doubling down on this failed strategy. But no matter how much control we are given, it will never work online. As we've tried to show in this essay, consent regimes burden data subjects with all of the risks of understanding and self-protection while keeping the data machine humming. Consent does not scale without losing its legitimacy.[146] The control that consent regimes promise us ends up being illusory and overwhelming. Even when companies are transparent, it doesn't lead to reform. Big tech platforms and shadowy advertising companies make their fortunes while the rest of us are watched, nudged, exploited, and exposed to data breaches and the manipulation of politics and elections.

There is a better way.

We should have rules that are more sensitive to relationships and power disparities. One way to do this is for lawmakers to create rules designed to protect our trust—trust in the Internet, trust in those entities that hold our data and promise to use it for our benefit, trust in our economy and in our digital society.[147] Being trustworthy in the digital age means being *discreet* with our data, *honest* about the risk of data practices, *protective* of our personal information, and, above all, *loyal* to us, the data subjects.[148]

There are some indications that lawmakers are willing to consider a trust-based approach to modern privacy rules. In late 2018, U.S. Senator Brian

146. *See, e.g.*, Julie Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1 (2019).
147. *See* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 3.
148. *Id.*

Schatz introduced the "Data Care Act of 2018."[149] Among other things, the bill goes beyond control and transparency goals in favor of three key non-waivable trust-based obligations for companies that use the Internet to collect personal information about people: duties of care, loyalty, and confidentiality. These duties are modeled after what is required of those in a fiduciary relationship, such as a trustee designed to care for a trust on behalf of a beneficiary, but they would apply more broadly if this bill were to pass.[150] They would require tech companies of all kinds to act more like doctors than telemarketers.

Trust rules would eschew consent regimes in favor of obligations to be protective and discrete and refrain from manipulative practices. They would aim to keep tech companies from elevating their short-term profits over our long-term interests. And ideally, legislative efforts built around trust would give regulators the resources they need and prohibit companies from using dense terms of use agreements to get us to waive those obligations. An explicit rejection of flimsy "consent" regimes is an important step forward for American privacy regimes.[151] Companies should be obligated to be trustworthy regardless of what we clicked to "agree" to online.

Another way lawmakers could address some of the pathologies of consent is by targeting abusive trade practices. Sunstein and Thaler's *Nudge* is not a cookbook for manipulators, but it has been used as such, and the law should step in to negate these practices. One of us has argued elsewhere that rules against abusive trade practices and abusive design of information technologies can help mitigate some of the inherent vulnerabilities of control regimes.[152]

The notion of abusive design can be found in consumer protection law, which aims to protect consumer choice. The most prominent prohibition on abusive practices in the United States comes from the relatively new Consumer Financial Protection Bureau (CFPB). The Dodd-Frank Wall Street Reform and Consumer Protection Act authorized the CFPB to prohibit any "abusive" act or practice that:

> (1) *materially interferes* with the ability of a consumer to understand a term or condition of a consumer financial product or service; or

149. S. 3744, 115th Cong. (2018). (In full disclosure, we provided feedback on this bill in draft form.)

150. *See* HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 43, at 99.

151. The bill specifically provides that "The rights and remedies provided under this Act may not be waived or limited by contract or otherwise." S. 3744, 115th Cong. § 5 (2018).

152. HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 43.

(2) *takes unreasonable advantage* of—

> (A) a *lack of understanding* on the part of the consumer of the material risks, costs, or conditions of the product or service;
>
> (B) the *inability of the consumer to protect* the interests of the consumer in selecting or using a consumer financial product or service; or
>
> (C) the reasonable *reliance* by the consumer on a covered person to act in the interests of the consumer.[153]

Rules against abusive trade practices look to the problems people have in assessing risks and benefits even with accurate, truthful information. They should begin with an internal inquiry into how we process information.[154] Since the pathologies of consent are all related to our limitations in processing information, this seems as good of a place as any for privacy reform to begin with.

It's time to take a bold step forward. America has an opportunity to redefine itself as the country that protects the trust that people give to companies. By embracing trust, America can become a leader on privacy instead of following the path of false promises, diminishing returns, and the tedium and vicious banality of mindless clicks of "I agree" buttons. Call it legal innovation, if that's what it takes. But whatever we call it, by requiring that companies respect our trust, America can pave the way for a safe, sustainable, and profitable digital future.

CONCLUSION

Tools are only fit for certain purposes. Legal tools are no different from physical tools in this respect. Frederick Schauer once likened legal tools to the problem of driving a nail into a board when you have a pipe wrench but no hammer. Pipe wrenches are great for tightening or loosening pipes, but

153. 12 U.S.C.A. § 5531 (West 2019) (emphasis added).

154. Patrick M. Corrigan, *"Abusive" Acts and Practices: Dodd-Frank's Behaviorally Informed Authority over Consumer Credit Markets and Its Application to Teaser Rates*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 125, 127 (2015) ("While shopping for the best offer, consumers may misperceive the real costs and benefits of a consumer product or service because of a lack of information about the product or service or due to a misunderstanding of the information available to them. The former is said to be a problem of imperfect information, while the latter is said to be a problem of imperfect or bounded rationality. Problems of imperfect information are extrinsic to the consumer, while problems of imperfect rationality are intrinsic.").

they make lousy hammers. You could certainly try to drive the nail into the board with a pipe wrench, but you probably wouldn't get it in straight, if you get it in at all. And you'd probably damage the pipe wrench.[155] Schauer was talking about the First Amendment, but consent is a bit like a pipe wrench as well—it is incredibly useful, even necessary, where it's the right tool for the job, but it can be easily overused, to the detriment of both the task and the tool.

We have over-used the tool of consent to the point that it has become badly damaged. Consent does and should play an essential role in our law, but it cannot do everything well all the time. The over-use of consent in the digital context, combined with limited legal policing of the sufficiency of consent has allowed great fortunes to be created on the basis of personal data, but it has also exposed consumers to data breaches, identity theft, and a surveillance economy unprecedented in human history, one which stretches the very notion of "consent" to say that it was ever actually agreed to. More fundamentally, the manufacturing of consent by exploiting consent's pathologies has diminished the trust in our digital environment that is the key ingredient toward a better future. We can do better, but in order to do so, we need to recognize the pathologies of consent, and limit consent to the contexts in which it is most justified. Going forward, we must rely on strategies other than fictive, manufactured, or coerced consent to minimize the risks and harms of our information economy, if we seek to take advantage of its benefits in a sustainable, ethical, and progressive way.

155. Frederick Schauer, *First Amendment Opportunism*, *in* ETERNALLY VIGILANT: FREE SPEECH IN THE MODERN ERA 175 (Lee C. Bollinger & Geoffrey R. Stone eds., 2002).