Pace Law Review

Volume 40 | Issue 1 Article 7

January 2020

Consent as a Free Pass: Platform Power and the Limits of the Informational Turn

Elettra Bietti

Recommended Citation
Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 Pace L. Rev. 310 (2020)
DOI: https://doi.org/10.58948/2331-3528.2013
Available at: https://digitalcommons.pace.edu/plr/vol40/iss1/7

Consent as a Free Pass: Platform Power and the Limits of the Informational Turn

Elettra Bietti*

TABLE OF CONTENTS

Abstract

Across the United States and Europe, notice and consent, the act of clicking that "I have read and agree" to a platform's terms of service, is the central device for legitimating and enabling platforms' data processing, acting as a free pass for a variety of intrusive activities which include profiling and behavioral advertising. Notwithstanding literature and findings that lay significant doubts on notice and consent's adequacy as a regulatory device in the platform ecosystem, courts, regulators and other public authorities across these regions keep adopting and legitimating these practices. Yet while consent seems a good proxy for ensuring justice in the platform economy, it is an empty construct. This Article explains how notice and consent practices in the platform economy are not only normatively futile but also positively harmful. Narrow understandings that focus on voluntariness and disclosure such as the ones generally adopted by regulators and courts fail to account for the systemically unjust background conditions within which voluntary individual acts of consent take place. Through such narrow approaches, regulators are failing to acknowledge that consent cannot be reasonably taken to morally transform the rights, obligations and relationships that it purports to reshape. Further, it positively harms consumers in at least three ways: burdening them with decisions they cannot meaningfully make;

subordinating their core inalienable rights to respect and dignity to the economic interests of platforms and creating widespread ideological resistance against alternatives. Notice and consent as a discourse is hardly contestable and is currently part of the rigid background of assumed facts about our digital environment. As new legislation is devised in the US and new opportunities to reinterpret the GDPR present themselves in the EU, we must be more courageous in looking beyond the façade of individual control and instead grapple with the core structure of corporate surveillance markets. The longer we fail to acknowledge consent's irrelevance to data governance, the longer we will deny ourselves respect and protection from the ever-growing expansion of digital markets into our lives.

Introduction

When attempting to create an account on *Facebook.com*, individuals are prompted to read a set of *Terms of Service*,[1] which they can choose to scroll through and ignore, and are simultaneously asked to tick a box, usually situated at the bottom of the screen, to indicate their agreement to such terms. These contractual terms, alongside multiple annexed clauses and webpages,[2] form the basis of a user's contractual agreement with Facebook, an agreement which, amongst other things, broadly regulates the types of data that Facebook can collect from its users and the possible uses it can make of such data. Facebook collects data provided by individuals at the moment of

---

* *S.J.D. Candidate at Harvard Law School.* *I thank Professors Yochai Benkler, Richard Fallon, Urs Gasser, Meira Levinson, Mathias Risse, Thomas Scanlon, and Lucas Stanczyk for their valuable input on this piece. I also thank the Edmond J. Safra Center's Graduate Fellows of 2018-19 and the Berkman Klein Center's fellows, affiliates and staff for conversations and inspiration on this topic.*

1. *Terms of Service*, FACEBOOK, https://www.facebook.com/legal/terms/update?ref=old_policy (last visited Nov. 24, 2019).

2. *See Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Nov. 24, 2019); *About Facebook Ads*, FACEBOOK, https://www.facebook.com/ads/about (last visited Nov. 24, 2019); *Your Ad Preferences*, FACEBOOK, https://www.facebook.com/ads/preferences/?entry_product=education_page (last visited Nov. 24, 2019).

opting-in and throughout their relationship with the company, for a variety of uses and purposes including but not limited to the targeting of advertising, content moderation, and the improvement of platform functionality.[3] Facebook has also recently been found to combine data from its users' Facebook profiles with other data collected on them through other Facebook and non-Facebook services such as Instagram and others.[4]

The increasing risks attached to intrusive data harvesting practices, including the targeting of content and ads based on a person's personal features, prompt us to ask anew why the law, along with other factors, enables and incentivizes data-driven activities by placing unjustified regulative power in notice and consent mechanisms? The law could directly shape and constrain dataflows and hold companies accountable by determining the kinds of information that should and should not be generated, collected, and used. Instead, around the globe the emphasis on what Daniel Solove has called "*privacy self-management,*"[5] reliance of contractual privacy policies, shifts the regulatory burden on users, leaving the industry free to engage in harvesting activities as they wish. Within the existing ecosystem, notice and consent's main function seems to be to performatively legitimate otherwise unregulated unacceptable corporate practices, and to facilitate permissionless innovation.

It is striking to note how recurrent the emphasis on individual consent and disclosure requirements is in privacy legislation and company practices around the world. In the United States, privacy self-management is the primary check on companies' ability to engage in data-driven activities as they wish, albeit being a voluntary and self-regulated practice.[6] The

3. *See Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Nov. 24, 2019).

4. *Case Summary: Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing*, BUNDERSKARTELLAMT (Feb. 15, 2019), https://perma.cc/95X5-83DW; *Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources,* BUNDESKARTELLAMT (Feb. 7, 2019), https://perma.cc/3PFM-7MVP; *Background Information of the Facebook Proceeding*, BUNDESKARTELLAMT (Feb. 7, 2019), https://perma.cc/RB4P-S9Y8.

5. *See* Symposium, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

6. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014). Note that the FTC

European Union has a more substantive approach to consent based on informational self-determination.[7] Under the recent EU General Data Protection Regulation (GDPR),[8] the burden of proving valid consent is greater, as consent must be informed, specific, unambiguous, freely given,[9] and consent is not the only basis for lawful processing.[10] Yet even the European approach places too much emphasis on informed consent, thus failing to protect users in the platform economy.

While much past and recent academic work has emphasized the limits of notice and consent,[11] few are those who present a

---

has a role in bringing civil actions against entities that engage in unfair or deceptive acts or practices in or affecting commerce under 15 U.S.C.S. § 45 (LEXIS through Pub. L. 116-72).

7. *See, e.g.*, Symposium, *Privacy and Technology: The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013); Woodrow Hartzog & Neil M. Richards, *Privacy's Constitutional Moment and the Limits of Data Protection* (May 2019) (draft presented at the Privacy Law Scholars Conf.); Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy* (May 2019) (draft presented at the Privacy Law Scholars Conf.).

8. Gen. Data Protection Reg. 2016/679 of Apr. 27, 2016.

9. *Id.* at arts. 4, 6, and 7. (*E.g.* Article 7 of the GDPR on "conditions for consent" reads as follows: *"(1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. (2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. (3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. (4) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*").

10. There are six bases for lawful processing of data under the General Data Protection Regulation 2016/679 of Apr. 27, 2016. One of these bases is that '*the data subject has given consent to the processing of his or her personal data for one or more specific purposes*' under Article VI(1)(a).

11. *See, e.g.*, Solon Barocas & Helen Nissenbaum, *Computing Ethics: Big Data's End Run Around Procedural Privacy Protections*, 57 COMMC'N OF THE ACM 31, 33 (Nov. 2014), https://perma.cc/X8FF-8C27; Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, PROCEEDINGS OF THE ENGAGING DATA FORUM: THE FIRST INT'L FORUM ON THE APP. AND MGMT. OF PERS. ELEC. INFO. (2009); Fred H. Cate & Viktor Mayer-Schonberger, *Notice and Consent in a World of Big Data*, 3 INT'L DATA PRIVACY LAW 67 (2013); Julie

nuanced account of consent that attempts to guide concrete policy.[12] Much of the existing work on digital consent falls into one of two clusters. It either usefully articulates consent's normative force but then mirrors the industry's consent-friendly stance, or otherwise it engages in abstract or indiscriminate rejections of the practice without sufficient articulation of how consent operates and what is at stake. Yet, as Elizabeth Edenberg and Meg Leta-Jones have shown, the legitimacy of consent is not a binary question and must be evaluated contextually.[13] Consent has an important normative function: the potential to transform an act of trespass into a legitimate invitation, or an act of battery into legitimate contact. We must scrutinize both the normative role and the discursive force of digital consent to explain when and why regulators must depart from the centrality of this practice in certain contexts.

When it comes to the digital economy, as early as 2014 Helen Nissenbaum and Solon Barocas argued that *"[c]onsent . . . should not bear, and should never have borne, the entire burden of protecting privacy*."[14] This Article goes a step further. It argues that the ideal of autonomous consent cannot be reached in practice in the platform economy because the conditions which constitute consent as a morally transformative device are absent. These conditions are three-fold: (1) that which is being transformed through consent must be capable of being transformed; (2) that acts of consent must not significantly harm third parties; and (3) that objectionable power imbalances must not be shaping the environment within which a decision to consent is made. In other words, consent is structurally incapable of empowering individuals in the platform economy. What remains is an empty construct. This is not an argument about the validity of individual instances of digital consent, but rather about the justifiability of relying on notice and consent as

E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES IN L. (2019); Julie E. Cohen, *Law for the Platform Economy*, 51 U.C.D. L. REV. 133 (2017); *Privacy Self-Management and the Consent Dilemma*, *supra* note 5; SHOSHANA ZUBOFF, *infra* note 213.

12. *See, e.g.*, Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't*, 9 J. INFO. POL. (2019).

13. Elizabeth Edenberg & Meg Leta-Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, NEW MEDIA & SOC'Y 1 (2019)

14. Barocas & Nissenbaum, *supra* note 11, at 33.

a default practice.

The discourse[15] of autonomous consent and the assumptions that underlie it positively harm consumers in two ways: by imputing responsibility on users for outcomes that no one could have reasonably chosen; and by focusing attention on the wrong kinds of values and creating collective resistance around alternatives that should be promoted. It seems that notice and consent in fact act as technologies of power:[16] a default practice that has become hard to contest and is part of the background of assumed facts about our digital environment. When faced with the effects of such a default practice, entrepreneurs and regulators too often recite arguments about the absolute primacy of individual autonomy. *Individuals need greater control over their digital lives*, they say, *and consent is the best, if not the only, option we have*. These responses are symptomatic of a dismaying lack of imagination around existing and future alternatives.

This Article proceeds in five parts. Part I of this Article articulates the subjective and objective dimensions of consent, its morally transformative function, and shows that for consent to operate as a morally transformative device it must be given under just background conditions. This requires three things: (1) that what is being transformed through consent must be capable of being transformed; (2) that acts of consent must not significantly harm third parties; and (3) that there must be no objectionable power imbalances.

Part II of this Article looks at how notice and consent are interpreted and relied on in the United States and Europe, showing that even the most stringent of approaches to data privacy seem to rely on interpretations of consent's role that fail to protect consumers.

Part III of this Article explores what individuals have reason to demand (in the platform economy), their digital "interests," and compares those interests to what the reality of

---

15. On the notion of discourse, see MICHEL FOUCAULT, THE HISTORY OF SEXUALITY, VOL. 1: AN INTRODUCTION (Robert Hurley trans., Random House 1978) (1978); MICHEL FOUCAULT, THE ARCHAEOLOGY OF KNOWLEDGE AND THE DISCOURSE ON LANGUAGE (A.M. Sheridan Smith trans., Tavistock Publications Limited 1971) (1969).

16. The term is borrowed from Foucault. *See* Michel Foucault, *About the Beginning of the Hermeneutics of the Self: Two Lectures at Dartmouth*, 21 POL. THEORY 198 (1993).

notice and consent enables them to demand from platforms. It shows that reliance on notice and consent structurally presupposes that we subject our fundamental interests to platforms' own selfish interests.

Part IV of this Article develops these insights by showing that privacy and protection from digital harms, such as manipulation and discrimination, have aspects that cannot be disposed of through consent: they have an inalienable core and interpersonal aspects that must be managed collectively. Further, it shows that subjecting any residual alienable aspects to the operation of notice and consent can lead to systemic harm in the platform economy.

Part V of this Article concludes by re-evaluating notice and consent's normative salience, asking whether paternalism can be an argument for resisting alternatives and develops an understanding of platform power that helps explain the existing gap between what we have reason to want in the platform economy, and what relying on notice and consent prevents us from obtaining under the mirage of autonomy, transformative power and coveted free services.

I. What Consent Is For

Consent is a contested concept that serves important social, political and normative functions in our society. In moral philosophy, an act of consent between two people is a reason to normatively reassess their relationship. Consent has a transformative normative function, it changes the justifications individuals have toward one another, the moral rights and obligations that exist between them. By consenting to someone entering into my house, I allow them to be inside it, transforming a trespass into a legitimate visit. By consenting to a doctor's auscultation, I transform a battery into an act of legitimate contact. Consent is key to the moral transformation of these and many other human relationships, and it would be difficult to imagine a world in which consent had absolutely no legitimating function or value. Yet when it comes to the digital economy, such value becomes at least questionable.

To evaluate whether digital consent has the moral force it is said to possess, we should look not only at whether the consenter acted autonomously of his own will, but also at the background

conditions that constitute consent as a morally transformative device. This section articulates these two key aspects of moral consent, emphasizing that background conditions and underlying power dynamics constitute the moral transformative force of consent.

A. Elements of Consent

1. Three Scenarios

The following three fictional scenarios might guide our intuitions about the core case of moral consent.

Imagine a society, not so different from many existing ones, call it society A, where being born a girl means you will undergo a female genital mutilation procedure. Is being born a girl a form of consent to these procedures? No one in society A asks the baby whether it wants to undergo the procedure. Being born a woman does seem to legitimate a variety of degrading or discriminatory treatments, yet saying that these treatments have been normatively legitimated through consent seems absurd. An inborn characteristic such as sex at birth can hardly be a form of consent.

Imagine now a second society, society B, where a person must give a stone to another person to indicate that they accept physical contact. In society B, women cannot legitimately be touched unless they transfer a stone to the persons they accept to be touched by. It seems that the passing of a stone serves as a form of consent: it is a self-directed act and is capable of changing the rights and obligations between stone givers and stone receivers.

Imagine finally a society C where if a woman wears a red dress, people can approach and talk to her, and if she does not wear a red dress, then they cannot. In such a society whether or not a woman can be spoken to is partly determined by herself and her decision to wear red, and partly subject to arbitrary cultural constraints about when wearing red is appropriate. Depending on context, women might intentionally choose to wear red or be forced to wear red. One might envisage different varieties of society C: somewhere red dresses are very rare, others where women must wear red on most social occasions. Where wearing a red dress is fully voluntary, an argument

might be made – likely controversially - that it is a form of consent.

These fictional examples provide us with three insights. First, they help us see a spectrum that ranges from intentional acts of the consenter self-directedly imposing normative consequences on themselves, to social norms or practices that persons are subjected to or forced to follow by virtue of their existence in a society (birth, social pressure, other external factors). Second, the examples point to an intuition, that the more an act is intentional and self-directed, the more it can be said to fall within the moral core of consent. Third, it seems that consent is a performative act whose normative meaning is highly dependent on the social, political and cultural conditions that enable it: things that amount to consent in one society or group may not amount to consent in other contexts.

The question, then, is what distinguishes a core case of morally transformative consent from things that are not understood as consent and what characteristics indicate whether a given cultural ritual, action or attitude amounts to consent. In other words: is there a test that allows us to *recognize* morally significant consent?[17]

2. Accounts of Consent

This subsection outlines possible accounts of consent with the aim of exploring the nature and contours of morally significant consent rather than defending any specific account. Consent between persons is said to have a "*transformative role in interpersonal interactions.*"[18] It transforms the rights and obligations that exist between persons, rendering impermissible things permissible and changing the expectations between consenter and consentee. Two core cases of consent between individuals can be identified:[19]

17. Note: the work of H.L.A. Hart on the normative "core" and "periphery" of a rule of law and the rule of "recognition" for law is impliedly in this passage. *See* H.L.A. HART, THE CONCEPT OF LAW (2d ed. 1961).

18. Edenberg & Leta-Jones, *supra* note 12. *See also* John Kleinig, *The Nature of Consent, in* THE ETHICS OF CONSENT: THEORY AND PRACTICE (Franklin Miller & Alan Werthmeier, eds., 2009).

19. Kleinig, *supra* note 18, at 4.

> [C]onsent can sometimes function like a proprietary gate that one opens to allow another's access, access that would be impermissible absent the act of voluntarily opening the gate. [. . .] Or, sometimes, consent can function like a normative rope whereby one binds oneself to another.[20]

In spite of significant overlap between these two cases, digital consent mainly falls within the former case: it operates as a gate that allows access to personal data. Consenting to an online privacy policy effectively authorizes a tech company to perform actions vis-à-vis users that prior to their consent would not have been justifiable. Having obtained user consent, the company can now engage freely in otherwise illegitimate data collection and uses such as profiling or microtargeting.

But what exactly is consent and how to explain its transformative moral power? Joseph Raz offers a helpful analytical understanding of how consent works:

> Consent is given by any behaviour (act or omission) undertaken in the belief that (1) it will change the normative situation of another; (2) it will do so because it is undertaken with such a belief; (3) it will be understood by its observers to be of this character.[21]

Raz understands consent as being mainly about how the consenter perceives their act. Yet we can see it as having two components. First, it has a *subjective* dimension: the consenter's intention or mental acceptance that their act of consent (or omission) will change the rights and obligations of another, and that the act will be perceived by others as consent. Unless there is a self-directed act of the will on the consenter's part, there can be no consent. Second, consent has an *objective* dimension: it must be perceived by external observers as changing the rights and obligations between consentee and consenter. Both subjective and objective elements are reflexive: the subjective act of the will cannot acquire moral salience without belief in

20. *Id.*
21. JOSEPH RAZ, THE MORALITY OF FREEDOM 81 (1986).

external recognition, and external recognition must go to the subjective element too. Accounts of consent are divided on the question of which of these two elements should have more salience. While some believe consent is mostly about the mental state of the consenter, and exists insofar as a subjective act of the will was present, others believe the notion of consent is contextual and must be understood as a communicative act: unless external observers perceive the act as being one of consent there can be no consent at all.[22]

Moreover, according to some philosophers the core function of consent is in its authorizing function.[23] Consent allows us to authorize others to perform certain actions vis-à-vis us. This particular function of consent as an authorization mechanism is particularly problematic in the digital economy. Consent operates as an authorizing mechanism for corporate actions, shielding the actors from otherwise legitimate complaints. While consent can operate as an enabling device for companies, the flipside is that it deprives users of some of their complaints against platforms.

B. Conditions and Transformation

1. Conditions for Consent

At its best, an exercise of moral consent allows the consenter to shape and change the course of their life and is an expression of individual autonomy.[24] At its worst, consent is a mere fictional performance with no effects on existing power structures and individual expectations. There is a vast literature on the conditions of moral consent, the various "tests" we might need in order to distinguish autonomous acts of consent from things that are not properly acts of consent.

Richard Fallon provides a helpful taxonomy on what he calls the "*conditions of [descriptive] autonomy*."[25] If indeed we

22. Kleinig, *supra* note 18, at 4.

23. *See, e.g.*, A. JOHN SIMMONS, MORAL PRINCIPLES AND POLITICAL OBLIGATIONS 76 (1979).

24. Tom L. Beauchamp, *Autonomy and Consent*, *in* THE ETHICS OF CONSENT: THEORY AND PRACTICE 55 (2009).

25. Richard H. Fallon, Jr., *Two Senses of Autonomy*, 46 STANFORD L. REV. 875, 886 (1994).

understand the best cases of consent as constituted by a self-directed act, consent must at least fulfill the following conditions for autonomous choice: (i) a critical and self-critical ability, (ii) competence or capacity to act and choose, (iii) a sufficient number of alternatives to choose from, and (iv) absence of coercion or objectionable manipulation.[26] Raz also specifies that there must be an adequate range of morally acceptable options meaning that the options must be varied in kind: it is more autonomous to choose among a few good options than among many very bad ones.[27] For him, choosing among bad options may not be autonomous at all.

Elizabeth Edenberg and Meg Leta Jones provide a list of core conditions that are specific to digital settings.[28] The first condition they isolate is that (i) there must be a common and clear understanding of the "*background conditions for justifiable and unjustifiable terms for collecting, using, and sharing personal data,*" which for them means broad societal agreement on baseline and ceiling levels of permissible data use.[29] The other four conditions they identify all operate within the parameters set by the first: (ii) a clearly defined scope for digital consent; (iii) sufficient information and a sufficient understanding of such information on the part of the consenter; (iv) a viable set of options that the consenter can voluntarily choose from; and (v) fair treatment of each of the parties to the consensual relationship.[30]

Taking stock of various existing formulations of the conditions of moral consent, including some that are included in current laws, one could tentatively define moral consent as possessing the following overlapping characteristics:

a) The person consenting must have the *rational capacity* to meaningfully consent, i.e. they must not be too young, mentally or physically impaired. They must have what

26. *Id.* *See also* GERALD DWORKIN, THE THEORY AND PRACTICE OF AUTONOMY (1988) (distinguishing between two aspects of autonomy understood as self-rule: independence of one's deliberation and choice from manipulation by others and capacity to rule oneself).

27. RAZ, *supra* note 21, at 372.

28. Edenberg & Leta-Jones, *supra* note 12.

29. Edenberg &Leta-Jones, *supra* note 12, at 1811.

30. *Id.*

Fallon calls *critical and self-critical ability*,[31] i.e. a capacity to rationally foresee the effects of one's actions, evaluate them and assess alternatives.

b) The act of consenting must not be *subject to coercion or objectionable manipulation of the will*.
c) The act of consenting must be voluntary in the sense that there must be *at least one viable and morally acceptable alternative* in the form of a viable option to walk away. An ambitious version of this condition would include both an ability to withdraw consent and the power to shape the content of the agreement transforming it into a better alternative agreement.
d) The *scope* of the consent must be limited fairly.
e) Consent must be fully *informed*, it must be preceded by a reasonable disclosure of the context, as well as the possible and probable effects of consenting.
f) Consent must be *present* consent: a person should be free to confirm or withdraw their consent at any moment in their relationship with the other party. If the conditions change, these must be disclosed. If consent is only expressed once at the start of a relationship, changes in circumstances may weaken its moral force and arguably also its legal validity.
g) Consent must be given under otherwise *just background conditions*: which includes the pre-condition of a full and transparent disclosure of options available and their content and implications, the fact that having the choice must not consistently and unfairly lead to discriminatory or unjust results for certain classes of people, possibly a basic structure complying with Rawlsian justice requirement.[32]

2. Identifying Morally Transformative Consent

In analyzing these lists of criteria, the goal has been to distinguish acts or omissions that an external observer would see as consent from acts or omissions that would not be understood as consent. However, an ambiguity underlies these

31. Fallon, *supra* note 25, at 886.
32. JOHN RAWLS, A THEORY OF JUSTICE (Otfried Hoffe eds., 2d ed. 1999).

lists of conditions. Some of these criteria help us distinguish acts of consent from things that are not consent, while other criteria help us determine whether an existing act of consent has a morally transformative role. Bill might have consented to John eating his snack in school, but if he did so because he has been repeatedly bullied in the past then we can see how his consent, no matter how autonomous and freely given, can hardly be understood to justify John's act transforming it into a legitimate food sharing arrangement. Consent cannot change the injustice of John's act given the history of John's relationship with Bill. As Franklin Miller and Alan Wertheimer have emphasized, the key question is not really whether consent exists or is valid, but whether an act of consent can be taken to justify a legitimate transformation of rights, obligations and expectations.[33]

The key question for us, therefore, is which conditions constitute consent as a morally transformative act? Subjective conditions of autonomous self-directed consent tell us whether an act can properly be classified as consent in accordance with Raz' definition, but offers poor guidance when it comes to determining whether consent legitimizes given consequences. The fact that an act is self-directed and performed in the belief that such act is an act of consent and will be perceived as such is insufficient to legitimizing transformative consequences. Legitimacy is contextual and depends on background conditions (Edenberg and Leta Jones' first condition, or our condition (g)), which include questions of power and influence exercised over users even when they don't know it.

An important question in the platform economy is whether ensuring just background conditions is possible.

C. Three Aspects of Morally Transformative Consent

What are just background conditions in the platform economy, and when can ideal consent perform its transformative role? Morally transformative consent cannot be identified by drawing up a list of representative background conditions of justice, or a "test" for recognizing morally transformative

33. Franklin G. Miller & Alan Wertheimer, *Preface to a Theory of Consent Transactions: Beyond Valid Consent*, *in* THE ETHICS OF CONSENT: THEORY AND PRACTICE (Miller & Wertheimer ed., 2010).

consent. It is a question that must be assessed by looking at how power materializes in any given context in which consent is relied on. Three characteristics of consent are nonetheless worth isolating to make sense of consent's transformative role.

1. Consent and Alienability

Taking consent to be transformative of states of affairs, rights, and obligations between persons presupposes that these states, rights, and obligations are of a kind which can be transformed through consent. Letting someone enter into one's house transforms a trespass into a license to stay in the house and also changes the position of the consentee from trespasser into guest. The right to prevent strangers from entering into one's house appears to be modified when one invites a stranger inside, so that one now has less reason to object to their being inside. Similarly, it seems that our right to prevent others from using certain information about us, such as our date of birth, is of a kind which can be amended by consent. After providing our date of birth to another, we have less reason to object to their use of that information. However, there are certain kinds of rights or entitlements of persons which cannot be transformed through consent. In a famous French case, it was found that dwarfs could not consent to being thrown by a nightclub's clients in exchange for money because the personal dignity and respect owed to persons with physical disability could not be given away for money.[34] Similarly, it could be argued that certain particularly intrusive data practices, such as behavioral targeting for political purposes, should not be capable of being consented to, that our right to be immune from undue political influences is inalienable.

2. Consent and the Collectivity

Moral consent operates between a consentee and a consenter, generally to amend the consenter's relationship with the consentee. Consent may affect third parties who are unaware or have no means of influencing the act of consent. If

34. Conseil d'Etat [CE] [French Administrative Court] Ass., Oct. 17, 1995, 136727, Rec. Lebon. CE Ass., Oct. 27, 1995, 136727, Rec. Lebon 372.

an act of consent has far-reaching consequences for third parties, it is argued that letting the consenter and consentee regulate such consequences can be inappropriate. In other words, the core case for morally transformative consent is a case where the only persons affected by an act of consent are the consenter and the consentee(s). As we shall see, digital notice and consent is the opposite kind of case, one where the consent of one person has the potential to affect larger groups of people.

3. Power

Third, considering the moral significance of consent amounts to investigating the kinds of power dynamics that underlie an act of consent and determining when the act, even if autonomous, no longer gives rise to justifiable consequences. In some cases indeed an act could be self-directed yet be affected by factors that delegitimate its effects. Questions that might reveal underlying power dimensions of this kind include: Was the act voluntary and made under just background conditions? What reasons did the consenter have to consent and what reasons did they have not to consent? Were there imbalances in the degree of influence that the parties to the consent relationship exercised over the formation of consent? What other structural, contextual, or environmental factors might generate doubt on the consenter's decision to consent?[35]

To sum-up, it seems that although morally transformative consent can hardly be defined through lists of conditions, it is constituted by three factors: (a) what is being transformed through consent must be capable of being transformed and not inalienable; (b) acts of consent must not significantly harm third parties; and (c) consent must be autonomous in a wide sense, i.e. it must not be the result of nudging, manipulation, false beliefs or knowledge gaps. In other words, consent has no value if it is shaped by systemic and invisible exercises of power.

D. Morally Transformative vs. Idealized Consent

Sometimes consent is arguably absent, for example where Bill is told that if he does not give his snack to John someone will

35. *See* STEPHEN LUKES, POWER A RADICAL VIEW (2005), ch. 1.

beat him. Other times consent exists but does not have transformative moral force, i.e. it does not provide reasons for accepting transformative consequences. This is where Bill is so used to being repeatedly bullied that he consents to giving his snack to John or another innocent schoolboy Alex, having had the freedom not to do so. In a third set of circumstances, consent exists and has morally transformative force. This is where for instance Bill and John are friends and willingly consent to sharing snacks with one another.

If an act of consent possesses all of the subjective features of consent outlined above, but lacks the constitutive conditions that give it morally transformative force, for instance by operating under unacceptable background conditions, then we can say that consent does not have morally transformative force. In many instances, consent that falls short of being transformative is nonetheless treated as if it were transformative. In those cases, we call the appearance of morally significant consent *idealized consent*.

Treating the bullying case as a valid case of consent is *idealizing* Bill's consent. When ticking a box indicating that we "*have read and understood the terms*" we seem to consent to the terms. But ticking a box resembles the bullying scenario more than it resembles the third scenario in which Bill and John are friends and choose to share their snacks in an act of reciprocal friendship. There are several reasons why this might be so. Users hardly have access to viable alternatives to existing terms, and if they do have alternatives, these are often shaped by the platform itself and are alternatives within a platform service rather than a fair choice amongst competing platforms. There are additional concerns relating to lack of visibility, knowledge asymmetries, and the manipulability of users. We might even want to go as far as saying that digital notice and consent schemes have been *designed* to get individuals to decline authority over certain matters. We might want to say, then, that many cases of online consent are cases of *idealized* consent.

E. Conclusions to Part I

To sum up, saying that an act of consent gives us reason to normatively reassess the relationship between two or more parties entails assuming that at least three things are true.

First, it entails assuming that any states of affairs, rights, and obligations purportedly being transformed through consent are of a kind which can be so transformed. Second, it entails assuming that any effects of consent on persons that are not parties to the consent relationship are not significantly harmful. Third, it entails assuming that consent can be largely free and autonomous and that the background context for consent is not structurally unjust or skewed in favor of some parties in the consent relationship. As this article will show, these three propositions are hardly all true in the platform economy.

As we will see in Part II of this Article, the core issue with practices of notice and consent in the United States and Europe is not necessarily that they exist, but rather that they are premised on the assumption that digital consent can be morally transformative in the platform economy as long as the conditions of disclosure can be strengthened. Instead, what the lawyers and regulators constructing the meaning of legal consent routinely miss is that in the digital economy legal consent operates in the absence of all of the three essential elements that give consent its transformative moral force. In other words, notice and consent is an instance of idealized consent.

**

II. The Construction of US and EU Notice and Consent Practices

This section provides an overview of key aspects of the regulation of consumer privacy through notice and consent on two sides of the Atlantic: the Federal Trade Commission's limited powers to oversee the industry's "notice and choice" practices in the United States, and European national data protection authorities' powers under the General Data Protection Regulation. It shows that in both systems, enforcement efforts that promote the centrality of information disclosure and of subjective criteria of informed consent are based on unreasonable assumptions about these devices' morally transformative force. By failing to scrutinize the background conditions within which notice and consent frameworks come into play, courts, agencies and regulators who construct the meaning of legal consent in the platform economy are legitimizing a practice that appears to have no legitimizing

moral force. While in the US legal reform that counters voluntary notice and choice industry practices is needed, the EU case shows that the deeper issue is not just legal reform, but rather the need for a change in perception and in regulatory attitudes toward data intensive industry practices.

A. "Notice and Choice" in the United States

1. Brief History of Voluntary "Notice and Choice"

With the advent of the Internet in the 1990s, the question of how to protect privacy in a massively replicable and connected environment became a concern. It quickly became apparent that pre-Internet legislation would not protect individuals against new digital privacy interferences.[36] Back in the 1970s, the Fair Information Practices Principles (FIPPs)[37] had established the privacy self-management paradigm in the United States by introducing three core ideas: notice, consent, and purpose limitation.[38] Under the FIPPs individuals had to be notified about the data collected about them and about the uses made of such data, and had to consent to such practices. Such principles however never made it into a comprehensive U.S. privacy law, and were instead incorporated in a piecemeal fashion in various sectoral legislative instruments, the most salient example possibly being the 1974 Privacy Act which only applies to Federal Agencies.[39]

Notwithstanding the United States' sectoral approach, the voluntary practice of "notice and choice" progressively

---

36. *See, e.g.*, *In re* DoubleClick Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001), (holding that DoubleClick's cookies did not violate the Electronic Communication Privacy Act (ECPA) by intercepting a group of plaintiffs' communications because the websites had "consented" to DoubleClick's access).

37. U.S. Dep't of Health, Educ., & Welfare, Records, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Computers, and the Rights of Citizens 41-42 (1973).

38. Marc Rotenberg, *Fair Info. Pracs. and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 44 (2001). *See also* Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, MAR. L. REV. (2019) (draft presented at PLSC 2019, p. 12).

39. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended in 5 U.S.C. § 552a).

established itself as the digital privacy management default for US consumers. Self-certification emerged in the late 1990s through organizations such as TRUSTe which issued "seals" to companies that had privacy policies that complied with certain standards,[40] and by 2001, almost all websites had privacy notices.[41] Yet the fact that privacy policies were voluntary rather than legally mandatory served industry players who could develop new products without undergoing any regulatory scrutiny as long as individuals kept opting in.

As a matter of contract law, the enforceability of digital privacy policies is debated. These policies have been repeatedly held unenforceable either because they were not considered to be binding under contract law, or for failure to show the harm suffered.[42] In *Dyer*, for example, the District Court for North Dakota held that an airline's privacy policy was a broad statement of company policy and did not constitute a contract.[43] Scrolling through a web page or clicking on the "download" button for a new software product has been held insufficient to constitute assent to the underlying terms and conditions.[44] Such browsewrap agreements have been enforced in cases where the relevant link or pop-up was repeatedly brought to a consumer's attention and the consumer was held to have had an opportunity to walk away, and therefore, have assented.[45] Clickwrap

40. Solove & Hartzog, *supra* note 6, at 593.

41. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 594 (2007).

42. Solove & Hartzog, *supra* note 6, at 595–97. *See, e.g.*, In re JetBlue Corp. Privacy Litig., 379 F. Supp. 2d (E.D.N.Y. 2005); Dyer v. Northwest Airlines Corps., 334 F. Supp. 2d (D.N.D. 2004); In re Nw. Airlines Privacy Litig., 2004 WL 1278459 (D. Minn. 2004); Daniels v. JP Morgan Chase Bank, *N.A.*, 2011 N.Y. Misc. LEXIS 4510 (N.Y. Sup. Ct. 2001); Loeffler v. Ritz-Carlton Hotel Co., No. 2:06-CV-0333-ECR-LRL, 2006 WL 1796008 (D. Nev. 2006). *See also* RESTATEMENT OF CONTRACTS (AM. LAW INST. TENTATIVE DRAFT, 2019) (seeking to establish new rules for browserwrap contracts.).

43. *Dyer*, 334 F. Supp. 2d at 1200.

44. *See* Specht v. Netscape, 306 F.3d 17 (2d Cir. 2002); Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171 (9th Cir. 2014); In re Zappos.com, Inc., Customer Data Security Breach Litig., 893 F. Supp. 2d 1058 (D. Nev. 2012); *see also* Aaron Hall, *Are Clickwrap or Browsewrap Contracts Enforceable?*, AARON HALL ATTORNEY (November 1, 2018), https://perma.cc/6H9P-XDMQ.

45. *See, e.g.*, Hubbert v. Dell Corp., 835 N.E. 2d 113 (Ill. App. Ct. 5th Dist. 2005). *See also* ProCD Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (discussing the analogous case of shrinkwrap contracts, which are included within the sealed package of a new product, and which have been enforced when there was an opportunity to walk away).

contracts, which require the positive ticking of a box unambiguously indicating that one has read and understands the terms and conditions, have instead generally been enforced,[46] though the case law on this point is surprisingly limited. Users have, therefore, not been able to rely on contract law to challenge companies' privacy policies. Tort law has also mostly been unhelpful for addressing the limits of privacy policy-based governance on the Internet, particularly because expansive interpretations of privacy torts are generally held to clash with First Amendment protections.[47]

Generating accountability around these policies has, therefore, required the involvement of a different kind of enforcement apparatus. The United States Federal Trade Commission (FTC) started to consider consumer privacy violations in 1995,[48] through its powers under Section 5 of the FTC Act to police "unfair or deceptive" trade practices.[49] As Daniel Solove and Woodrow Hartzog have stated, the plan was that*"[t]he FTC would serve as a backstop to the self-regulatory regime, providing it with oversight and enforcement – essentially with enough teeth to give it legitimacy and ensure that people would view privacy policies as meaningful and trustworthy."*[50] In other words, the FTC's enforcement would provide legitimacy to an otherwise unchecked self-governing practice.

The FTC is a civil law enforcement agency that operates by bringing lawsuits or settling matters directly with the companies who have committed violations, and does not have statutory powers to enforce its own agenda. It starts at ten privacy-related actions per year on average based on its powers to prevent deceptive and unfair commercial practices.[51] The number seems low considering these are the most effective means of policing commercial privacy violations in the US, the number of violations likely to occur every year and the general

46. *See, e.g.*, Feldman v. Google, Inc., 513 F. Supp. 2d 229 (E.D. Pa. 2007).

47. *See* Alicia Solow-Niederman, *Reinvigorating a Common Law Approach for Data Breaches*, YALE L. J. F. (2018); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1185 (2016).

48. Solove & Hartzog, *supra* note 6, at 598.

49. 15 U.S.C.S. § 45 (LEXIS through Public Law 116-72).

50. Solove & Hartzog, *supra* note 6, at 598-9 (emphasis added).

51. Solove & Hartzog, *supra* note 6, at 600; *see also* Federal Trade Commission, Privacy & Data Security: Update 2018 (2018), https://perma.cc/2UGB-KZ23 .

unavailability of remedies under private law or statute. Furthermore, the procedure before the FTC normally ends in a settlement or consent order and not in a decision that can be appealed. This further limits consumers' ability to litigate privacy violations.

The practice of "notice and choice" leaves us with two questions: (1) Is FTC enforcement bold enough to deter unwelcome privacy intrusions, or does it remain a performative façade?; and (2) If voluntary "notice and choice" practices are insufficient to address consumer harms, what kind of legislation is needed?

2. The FTC's Enforcement Action against "Deceptive" and "Unfair" Trade Practices

In 1998 the FTC began its enforcement against "deceptive" practices, with a weak enforcement apparatus and a limited scope of action.[52] Its theory of deception developed to cover not only promises that had been breached, but also deceptive inducements by companies to disclose customer data and cases of insufficient notice and disclosure in relation to privacy-invasive activities. Deception is made of three elements: (a) a representation, omission, or practice likely to mislead the consumer; (b) it was reasonable for someone within the target consumer group to be misled; and (c) the representation, omission, or practice was "material" in the sense that it was likely to affect a consumer's choice regarding products or services.[53] The deception doctrine entrenches the assumption that information can solve consumer privacy issues: the key element is the disclosure or its absence, and the main question is whether the disclosure was sufficient and accurate. If a practice has been properly disclosed and consumers have accepted its related risks, there is no reason for the FTC to use its deception powers.

Yet the FTC also has "unfairness" powers. Dennis Hirsch has argued that contrary to the FTC's deceptiveness doctrine, the unfairness doctrine can address most algorithmic privacy

52. Solove & Hartzog, *supra* note 6.

53. *See* U.S. Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), https://perma.cc/826X-X9YN.

harms.[54] As it currently stands, however, the doctrine has a quite limited scope. A practice will be deemed unfair if it "*causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.*"[55] In practice, this three-part test, and in particular the fact that the injury must be reasonably unavoidable, heavily constrains the FTC's scope of action. If a consumer had options to choose a different competitor or product, or if the injury was otherwise avoidable through a proper exercise of judgment, then the FTC has no power to intervene.

Data practices, however, can be very harmful to consumers even when they are disclosed, consented to, and hypothetically avoidable. As highlighted by behavioral economists: people frequently do not choose the best for themselves. They rarely read privacy policies before opting in, and when they do, they fail to understand them.[56] There are various psychological factors at play when choosing to opt in,[57] e.g. incompatible preferences or ethical stances, contradictory needs, internal biases, or biases in the choice architecture.[58] Information that is complete can be presented in ways that manipulate individuals to opt in.

It has been argued that the FTC's unfairness doctrine already covers latent manipulation.[59] It encompasses behavioral considerations and is evolving toward encompassing

54. Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, MD. L. REV. (forthcoming 2019).

55. 15 U.S.C.A. § 45(n) (West, West Law through P.L. 116-72).

56. *See, e.g.*, Omri Ben-Shahar & Carl Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647 (2011).

57. Alessandro Acquisti, Laura Brandimante & George Lowenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015).

58. *See* Alessandro Acquisti, *Nudging Privacy*, 7 IEEE SECURITY & PRIVACY 82 (2009); *See also* Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk 1-26* (Nat'l Bureau of Econ. Research, Working Paper No. 23488, 2017), https://perma.cc/9UNW-K9SL; SUNSTEIN & THALER, *infra* note 201; Erik Brynjolfsson, Felix Eggers & Avinash Gannamaneni, *Using Massive Online Choice Experiments to Measure Changes in Well-being 1-74 (*Nat'l Bureau of Econ. Research, Working Paper No. 24514, 2018), https://perma.cc/T8Z8-NU7N.

59. Hirsch, *supra* note 54.

predictive analytics and behavioral advertising practices. Practices that have been considered unfair by the FTC include retroactive policy changes,[60] deceitful data collection,[61] improper uses of data,[62] unfair default settings,[63] and unfair information security practices.[64] It remains to be seen how innovatively the FTC will interpret its powers in future. Still, a regulatory apparatus premised on the supremacy of consumer choice and on the importance of informational disclosures arguably cannot go far enough in the digital economy. The FTC's powers under section 5 are based on the assumption that consumers must bear the ultimate burden of privacy governance in the digital economy. Yet individuals are not always the most appropriate locus of governance in a platform context, particularly if choice is likely to be distorted by power asymmetries and unjust background conditions.

3. Facebook and Beyond

The FTC's current unfairness doctrine is the result of an evolutionary process, yet one that hardly seems sufficient to fully protect consumer privacy in the United States because it remains centered on individual choice and information disclosures. A salient example of the FTC's enforcement powers in action will serve to illustrate this argument.

In *In re Facebook, Inc.*, the FTC found that Facebook had not properly notified its users of changes to its privacy settings, and that some of these changes constituted deceptive and unfair practices.[65] The new policy was considered *deceptive* because it inaccurately informed users that they could restrict access to profile information,[66] and because it failed to disclose the fact that users could no longer restrict access to their Name, Profile

60. *See, e.g.*, In re Gateway Learning Corp., 138 F.T.C. 443 (2004); In re Facebook Inc., 2012 WL 3518628 (2012) [hereinafter Facebook Complaint].

61. *See, e.g.*, In re Aspen Way Enters., Inc., 155 F.T.C. 483 (2013).

62. *Id.*

63. *See, e.g.*, In re Sony BMG Music Entm't, 2007 WL 1942983 (2007).

64. *See, e.g.*, United States v. Rental Research Servs., Inc., FTC File No. 072-3228 (D. Minn. Mar. 5, 2009).

65. Facebook Complaint, *supra* note 60.

66. *Id.* at 6–7.

Picture, Gender, Friend List, and Pages.[67] The policy was also considered *unfair* because it retroactively designated as public, information that had previously been held private, without users' informed consent.[68] The unfairness count could have been avoided if users had given informed consent to the re-designation, something which Facebook would have had no difficulty obtaining. The case ended with a *Consent Order*,[69] which included disclosure obligations, obligations to make certain information private, and also the requirement to establish "*a comprehensive privacy program*" to address some of the violations,[70] coupled with the obligation to carry out impact assessments twice a year for twenty years.[71]

Notwithstanding these seemingly stringent requirements, in March 2018 a personality quiz app called "*thisisyourdigitallife*" was revealed to have been installed by 300,000 people in 2013, enabling the data analytics and voter profiling firm Cambridge Analytica to obtain information about those 300,000 Facebook users and all of their Facebook friends.[72] In total this amounted to approximately 87 million user profiles.[73] In December 2015, Facebook removed the app which was purportedly in breach of its Platform Policies and demanded assurances from all parties involved that the user information had been destroyed. All parties certified to Facebook that they had destroyed the data, and the matter was put to rest.[74] Cambridge Analytica, however, had not deleted all user data,[75]

---

67. *Id.* at 9.

68. *Id.*

69. In the Matter of Facebook Inc., F.T.C. No. 092-3184 No. C-4365 (F.T.C., July 27, 2012) (Decision and Order).

70. *Id.* at 5.

71. *Id*. at 6.

72. Paul Grewal, *Suspending Cambridge Analytica and SCL Group from Facebook*, FACEBOOK NEWSROOM (Mar. 17, 2018 9:50 AM), https://perma.cc/JLJ8-HSJ9; Facebook: Transparency and Use of Consumer Data Before the H. Comm. on Energy and Commerce, 115th Cong. (2018) (Questions for the record response by Mark Zuckerberg, Chairman & Chief Executive Officer, Facebook).

73. Nadeem Badshah, F*acebook to Contact 87 Million Users Affected by Data Breach*, THE GUARDIAN (Apr. 8, 2018 6:40 PM), https://perma.cc/F6AL-72NS.

74. Facebook: Transparency and Use of Consumer Data, 115th Cong. (2018) (Questions for the record response by Mark Zuckerberg Hearing before the US House of Representatives Committee on Energy and Commerce).

75. Grewal, *supra* note 72.

and users were never notified of the breach or the data transfers until a leak in early 2018 caused public outrage. Suddenly pressured for answers, Facebook offered partial responses.[76] Paul Grewal for instance asserted that there had been no breach on Facebook's part:

> The claim that this is a data breach is completely false. [Cambridge Analytica] 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, no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked.[77]

Zeynep Tufekci reacted:

> Mr. Grewal is right: This wasn't a breach in the technical sense. It is something even more troubling: an all-too-natural consequence of Facebook's business model, which involves having people go to the site for social interaction, only to be quietly subjected to an enormous level of surveillance. (. . .)
>
> Despite Facebook's claims to the contrary, everyone involved in the Cambridge Analytica data-siphoning incident did not give his or her "consent" — at least not in any meaningful sense of the word. It is true that if you found and read all the fine print on the site, you might have noticed that in 2014, your Facebook friends had the right to turn over all your data through such apps. (Facebook has since turned off this feature.) If you had managed to make your way through a bewildering array of options, you might have even discovered how to turn the feature off. This wasn't informed consent. This was the exploitation of

76. *Id.*
77. *Id.*

user data and user trust.[78]

A reform of the FTC's enforcement of consumer privacy thus seemed in order. However creative the 2012 Consent Order had been, it had dramatically failed to prevent the harms caused to consumers from 2013 to 2018. Religious faith in voluntary notice and choice provided Facebook with a shield to hide behind and continue to pursue its corporate interests on the backs of users.

One year later, the FTC fined Facebook five billion dollars for non-compliance with the *Consent Order* and for other violations under Sections 5 and 16 of the FTC Act.[79] The settlement introduced a series of innovative compliance measures including monitoring of data sharing arrangements with third party developers and app providers; new channels to hold Facebook accountable, including a new Board of Directors committee focused on privacy risks; quarterly compliance certifications; and enhanced FTC access to internal documents.[80] Still, the measures were criticized as insufficient.[81] Amongst other shortcomings was the recognition that the Order remained the result of a voluntary settlement, accepted, and acceptable to Facebook itself:

> Our colleagues lament that the Order does not do more. (. . .) As a civil law enforcement agency (and not a regulator), we can only get what we can win in litigation or via hard-fought negotiations. The FTC does not have the authority to regulate by fiat. The extent to which Facebook, or any other

78. *See* Zeynep Tufekci, *Facebook's Surveillance Machine*, N.Y. TIMES (Mar. 19, 2018), https://perma.cc/2ERY-T5TE.

79. Complaint for Civil Penalties, Injunction, and Other Relief at 1, USA v. Facebook, Inc., No. 91-cv-2184, 2019 WL 3318596 (D.D.C., July 24, 2019).

80. Stipulation Order For Civil Penalty, Monetary Judgement, and Injunctive Relief, United States v. Facebook, Inc. (D.C. 2009) (No. 19-cv-2184).

81. Dissenting Statement of Commissioner Rohit Chopra Regarding the Matter of Facebook Inc., No. 092-3184 No. C-4365 (July 24, 2019), https://perma.cc/C59W-JUZE; Dissenting Statement of Commissioner Rebecca Kelly Slaughter Regarding the Matter of FTC vs. Facebook, No. 092-3184 No. C-4365 (July 24, 2019), https://perma.cc/YD7L-DW33; *see, e.g.*, Siva Vaidhyanathan, *Billion-dollar Fines Can't Stop Google and Facebook. That's Peanuts for Them*, THE GUARDIAN (July 26, 2019), https://perma.cc/2FXV-M9BB.

> company, should be able to collect, use, aggregate, and monetize data, is something Congress should evaluate in its consideration of federal privacy legislation. Our 100 year-old statute does not give us free rein to impose these restrictions.[82]

A self-regulatory and individual choice-centric approach to data and consumer harms remains predominant in the United States. While legislative progress has been made at state level, notably with the California Consumer Privacy Act (CCPA) which came into force in early 2020, Federal legislation is yet to be seen. As long as we rely on voluntary disclosures and individual choice, the full scope of the acts and activities we recognize as abusive will never be addressed.

B. The European Approach to Consent

1. Consent and Control under the GDPR

Contrary to the United States approach, which favors voluntary privacy safeguards, European data protection law has developed as a principled umbrella body of law, following two influences. First, the FIPPs, as first formulated in a report of US Department of Health Education and Welfare in 1973[83] and as subsequently reconfigured in the OECD's 1980 *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*,[84] came to form the backbone of European data protection law. Their three core principles of notice, consent, and purpose limitation still form the skeleton of EU data protection today. Another important factor was the German Constitutional Court's jurisprudence on the right to informational self-determination, which centered around the imperative of affording individuals the power to control

---

82. Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson Regarding the Matter of Facebook, Inc., No. 092-3184 No. C-4365 (July 24, 2019), https://perma.cc/9PWC-ZMVK.

83. U.S. Department of Health, Education and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems, No. (OS)73-94* (1973).

84. OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), https://perma.cc/RM25-2ZPF.

information about themselves.[85] "*Natural persons should have control of their own personal data,*" establishes Recital 7 of the EU General Data Protection Regulation, the much acclaimed new European umbrella privacy law.[86] The idea of informed consent under EU data protection law is closely tied to that of informational self-determination. As explained by the Article 29 Working Party: "*[t]he notion of consent is traditionally linked with the idea that the data subject should be in control of the use that is being made of his data. From a fundamental rights perspective, control exercised through consent is an important concept.*"[87]

In May 2018, the EU GDPR came into force, repealing the previous data protection regime[88] and introducing a radical reconfiguration of privacy protection worldwide. It reinforced the requirements for informed consent as one of the bases, and not the only basis,[89] for legitimate data processing, and introduced new inalienable data subject rights that cannot be waived by consent. It also expanded rights to access information about the personal data being processed, rights to rectify and erase personal data, the right to data portability, and the right to have human intervention in AI-based decision-making.[90] The GDPR also introduced new compliance mechanisms: internal codes of conduct for companies;[91] data protection impact assessments (DPIAs) whereby companies are encouraged to describe and evaluate aspects of their data processing practices likely to result in high risk;[92] data protection seals and

85. BVERFGE, 1 BvR 484/83, Oct. 18-19, 1983, 65 BVerfGE 1, available in German at: https://perma.cc/LT44-NX3K. *See also* Herbert Burkert, *Privacy - Data Protection: A German/European Perspective*, SECOND SYMPOSIUM OF THE GERMAN AMERICAN ACADEMIC COUNCIL'S PROJECT "GLOBAL NETWORKS AND LOCAL VALUES", Woods Hole, Massachusetts 44 (1999).

86. Gen. Data Protection Reg., *supra* note 8, at art. 7.

87. EU Article 29 Working Party, *Opinion 15/2011 on the definition of consent,* 01197/11/EN WP187, at 8 (July 13, 2011).

88. 1995 O. J. (L281) Directive 95/46/EC.

89. Gen. Data Protection Reg., supra note 8, at art. 6.

90. Gen. Data Protection Reg., *supra* note 8, at arts. 12-23.

91. *Id.* at art. 40.

92. *Id.* at art. 35. *See* EU Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "likely to result in a high risk" for the Purposes of Regulation 2016/679*, 17, WP 248 (Apr. 4, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

certifications overseen by apposite certification bodies;[93] and perhaps most importantly data protection by design and by default which for example require setting up appropriate internal data minimization standards.[94] The Regulation further requires each EU Member State to put in place a National Data Protection Authority (NDA) to ensure "the consistent application of [GDPR] throughout the Union."[95]

Under the GDPR, informed consent is one of six bases for lawful processing, the others being that the processing is necessary for the performance of a contract, for compliance with a legal obligation, or a closed list of other reasons including the pursuit of a legitimate interest of the person or entity responsible for data processing or a third party.[96] Consent is required for the processing of special categories of personal data, for example data relating to racial characteristics, political or religious beliefs, and genetic and biometric data,[97] but it is not required for the processing of other data which can be carried out under any of the other five bases of lawful processing. The GDPR defines consent as "*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*."[98] To be valid under the GDPR, an expression of consent must be informed, it must be specific and unambiguous, meaning that it cannot be sufficient to present individuals with pre-ticked boxes or to bundle consent with other actions,[99] and it must be *freely given*, in that it must provide individuals with real

93. Gen. Data Protection Reg., *supra* note 8, at arts. 42-43.

94. Gen. Data Protection Reg., *supra* note 8, at art. 25. *See also* Gen. Data Protection Reg., *supra* note 8, at art. 5(c) (discussing the principle of data minimization in the GDPR).

95. Gen. Data Protection Reg., *supra* note 8, at art. 51(2). *See* Gen. Data Protection Reg., *supra* note 8, at arts. 51-59 (explaining the powers and jurisdiction of national NDAs).

96. Gen. Data Protection Reg., *supra* note 8, at art. 6.

97. Gen. Data Protection Reg., *supra* note 8, at art, 9.

98. Gen. Data Protection Reg., *supra* note 8, at art. 4(11).

99. *See* Opinion of Advocate General Szpunar, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V*, Case C-673/17, ECLI:EU:C:2019:246 (Mar. 21, 2019) (explaining the principles of specific consent and ambiguity), https://perma.cc/5K6D-DHQQ.

choice and control, and must be uncoerced.[100] Article 7 of the GDPR, which specifies additional conditions for the validity of consent, adds that in assessing whether consent is freely given, "*utmost account shall be taken*" of whether the processing is "*necessary for the performance of that contract.*"[101] This amounts to saying that obtaining free and valid consent becomes more burdensome for a company as the data it acquires becomes peripheral to the services it provides. Article 7 also specifies that there is a right to withdraw consent at any time,[102] and that consent "*shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.*"[103]

EU data protection law as we see it today is characterized by fundamental rights protection coupled with a strong emphasis on informed consent, user choice, and control. Both consent and data subject rights assume that the individual can and should be the ultimate decision-maker regarding opaque commercial data practice, thus neglecting the power asymmetries and information externalities that make individual-centric decision-making objectionable. It must be noted that this state of affairs is not a necessity; in theory EU data protection could be seen as centrally concerned with privacy defaults and one could understand consent under the GDPR as applying only in exceptional circumstances. Yet the reality of the law's current interpretation and implementation is different. While the Regulation does include compliance measures that go beyond individual control over data, the way such measures are to be implemented is still far from clear and so far remains up to the voluntary efforts of companies themselves. Much of the case law on the GDPR since its coming into force has scrutinized the question of what constitutes legally compliant informed consent, without sufficiently questioning whether consent is the most appropriate basis for legitimating processing in given contexts. As the GDPR's scope and mode of application is progressively clarified through the intervention of courts, regulators, and civil society amongst others, a shift away from consent and control

100. *See generally* EU Article 29 Working Party, *Guidelines on Consent Under Regulation 2016/679, 17/EN WP259* (Apr. 10, 2018).

101. Gen. Data Protection Reg., *supra* note 8, at art. 7(4).

102. Gen. Data Protection Reg., *supra* note 8, at art. 7(3).

103. Gen. Data Protection Reg., *supra* note 8, at art. 7(2).

seems unlikely, especially as these notions leak into neighboring legal fields such as competition enforcement. In the long run, this enforcement strategy is likely to benefit companies more than consumers. In what follows, we explore two cases that illustrate the shortcomings of an EU approach centered on individual informed consent.

2. Disclosure and Transparency: the French CNIL's Decision against Google

As the GDPR was coming into force, the French Data Protection Regulation, the "Commission nationale de l'informatique et des libertés" (CNIL) received two complaints, respectively by NOYB a non-profit based in Austria and the French la Quadrature du Net, both claiming that Google did not have a sound legal basis under the GDPR for engaging in processing of personal information as it did. On January 21, 2019, the French authority issued its first decision under the GDPR, and first amongst EU DPAs, imposing a fine of 50 million Euro against Google for failing to comply with the requirements for valid consent under the GDPR.[104]

The substantive ruling in this case consists of two parts. First, CNIL decided that Google had failed to comply with its obligation to provide access to transparent information about data processing to users, because the information available to users was too disseminated, and was not clear and comprehensive. Second, CNIL found that Google's targeted advertising practices were not covered by valid consent. It found that consent not only failed to be "informed," but that it also failed to be sufficiently "specific" and "unambiguous" under the GDPR.

We here expand on CNIL's approach further. First, therefore, CNIL found that Google did not make the required information easily accessible to users under Articles 12 and 13

104. Commission nationale de l'informatique et des libertés [CNIL] [French Data Protection Authority] *Délibération de la formation restreinte n° SAN – 2019-001 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC,* SAN-2019-001 (January 21, 2019), https://perma.cc/VHK7-YUFE.

of the GDPR.[105] Information essential to the exercise of data subject rights, such as the purposes of data processing, the modalities of storage and the types of personal data used in targeted advertising could not be accessed in one single place and were instead disseminated across several documents, sometimes requiring up to five or six steps for a user to get relevant information on his or her data. Further, the information provided by Google was not always clear or comprehensive. Google's processing operations span across about twenty services and entail the collection and use of a wide range of data, including data directly provided by users such as name and date of birth, data generated through a user's activities such as geolocation, and data inferred on the basis of other data. CNIL found that the information Google provided to users was too generic and vague to properly notify individuals of the processing at stake and of the importance of their consent to the practices' legitimacy.

Second, CNIL found that Google failed to obtain valid

105. *See* Gen. Data Protection Reg., *supra* note 8, at art. 12(1): "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means*." Article 13(1) GDPR reads: "*Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*

- *the identity and the contact details of the controller and, where applicable, of the controller's representative;*
- *the contact details of the data protection officer, where applicable;*
- *the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
- *where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*
- *the recipients or categories of recipients of the personal data, if any;*
- *where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation [sic] and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available*."

consent from users, and thus failed to engage in lawful processing when it relied on consent as a basis for lawfulness under Articles 6 and 7 of the GDPR. Consent was considered invalid because it was not sufficiently informed (the information provided by Google to its users was lacking in accessibility and clarity) and it was insufficiently "specific" or "unambiguous." When creating an account, users could click on the button "more options" to access certain data processing defaults and untick them. However, CNIL considered that linking to pre-ticked ads personalization defaults placed an excessive burden on users' ability to control processing on their personal data, and that under those circumstances consent to the defaults could not be considered specific and unambiguous.

The requirements on information access, disclosure, and consent that underlie the decision are revealing. While CNIL's intention was to protect individual consumers, its decision appears problematic on at least two fronts. First, the findings are highly design-sensitive. CNIL grounds its arguments on how information is presented: browsing to a different page, the number of steps needed to access information, etc. These criteria may be valuable, but they are ephemeral and easy to design around. One could imagine information that is perfectly readable on the front page and yet remains impenetrable. Second, transparency on Google's behavioral advertising practices is unlikely to ever be achieved, let alone through disclosure and consent. Google has no incentive to disclose full and complete information about its most valued business model to its customers, users and competitors, and it has too much power to affect the shape of any disclosure it makes. The information Google will disclose to users is unlikely to change much if the practice of notice and consent remains as it currently is.

The problem is that by focusing on perfecting consent so that it complies with idealized informed consent, CNIL is leaving behind an essential part of the structural injustice. The problem is not that individuals consent to opaque behavioral advertising as much as it is that behavioral advertising is harmful and should not be engaged in as extensively as it currently is. As said, consent cannot serve a legitimizing role unless it operates under just background conditions. Here, it is clear that users will keep accepting the terms set by Google in order to access its

services, and Google's interests will always prevail over any individual's interests in the information disclosure. CNIL's focus on the criteria and nature of volition and informed consent seems to add moral legitimacy to a practice that acts as an empty vessel. This approach will not do justice to individuals in the long run.

3. Monopoly Power: The German Bundeskartellamt Decision against Facebook

Not long after CNIL's decision, in February 2019 another decision considered a platform's breach of EU consent requirements, this time however it was issued by an antitrust authority.[106] In this much awaited case the German Competition Authority, or Bundeskartellamt, found that Facebook had violated German antitrust law by forcing those who wanted to access the Facebook platform to accept—through notice and consent—certain data collection and use practices such as the combination of data gathered through Facebook-owned services including WhatsApp and Instagram and third party websites in one Facebook user-account. Much of the Bundeskartellamt's case is premised on user-control and consent, yet this time the analysis is pushed further and also scrutinizes the power asymmetries at play between users and Facebook. In the authority's words, "*[t]here is no effective consent to the users' information being collected if their consent is a prerequisite for using the Facebook.com service in the first place.*"[107]

In the decision, the Bundeskartellamt first finds that Facebook is dominant on the market for social networking

106. *Prohibition Decision: Facebook Inc. i.a. - The use of abusive business terms pursuant to Section 19 (1) GWB*, Bundeskartellamt (June 2, 2019), https://perma.cc/D8PK-D82G; *See* Bundeskartellamt, *Case Summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing* (Feb. 15, 2019), https://perma.cc/JJN9-8URN; Bundeskartellamt, *Press Release Bundeskartellamt prohibits Facebook from combining user data from different sources* (Feb. 7, 2019), https://perma.cc/33YH-PDB9; Bundeskartellamt, *Background information of the Facebook proceeding* (Feb. 7, 2019), https://perma.cc/HS94-EJNU.

107. *See* Bundeskartellamt, *Case Summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing* 1 (Feb. 15, 2019).

services in Germany, with a market share of daily active users of ninety-five percent.[108] Second, it finds that Facebook abuses its dominance by engaging in an abusive data policy, i.e. collecting user and device-related data from a variety of external sources, and conditioning access to their platform to their combining it with Facebook profile data. The Bundeskartellamt's foundational philosophy in this case is that "*[i]n order to protect the fundamental right to informational self-determination,*[109] *data protection law provides the individual with the right to decide freely and without coercion on the processing of his or her personal data.*"[110]

The competition authority then argues that reliance on EU data protection law as a standard for determining the existence of exploitative abuse is justified and explains that consent under the GDPR cannot be voluntary and freely given if "*users consent to Facebook's terms and conditions for the sole purpose of concluding the contract*."[111] Further, none of the other bases for lawful processing under Article 6 GDPR are present, particularly as the processing of all that user-data cannot be considered necessary for the performance of the users' contract with Facebook. Thus, Facebook's processing violates data protection laws.

The further step the Bundeskartellamt takes in its analysis is to consider such violation as evidence of an abuse of dominance, stating that what was required under German law was a showing that dominance and the violation of German law and data protection rules are causally related.[112] The way the authority explains this causality is two-fold. First, a reason why consent cannot be considered voluntary and freely given is precisely because Facebook is dominant on the market for social networking services. If users had more options to avoid Facebook's collection and processing of combinations of data

108. *Id.* at 3–7.

109. In 1983, the German Constitutional Court developed the right to informational self-determination relying on Articles 1 and 2 of the German Federal Constitution. BVerfGE, 1 BvR 484/83, Oct. 18-19, 1984, 65 BVerfGE 1, available in German at: https://perma.cc/LT44-NX3K.

110. *See* Bundeskartellamt, *Case Summary: Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing* 8 (Feb. 15, 2019).

111. *Id.* at 10.

112. *Id.* at 11.

then it is possible that there would be valid consent. Second, those unlawful contracts allow Facebook to access, collect, and benefit from larger amounts of data than its competitors and arguably larger amounts of data than its users would agree to. The authority does not consider the particulars of how Facebook's exploitative data policies (advertising, profiling) can harm individuals other than stating that the combination of these factors undermines users' ability to "*decide autonomously on the disclosure of their data*."[113] In other words, the competition harm in question is a loss of user control over how their data is processed. Andreas Mundt, President of the Bundeskartellamt, characterized the decision's effect as an "*internal divestiture of Facebook's data*."[114] The Bundeskartellamt's goal in the decision in other words was to make the combination of data from different services across the web more difficult, and to give individuals real choices to disaggregate those datasets.

While combining competition law and privacy in one decision is a very interesting new development, the decision's focus on consent and loss of control appears to go both too far and not far enough. It allegedly goes too far because it subsumes questions of data protection within the competition law analysis, a move that has been harshly contested on the grounds that it conflates two fields of enquiry, uncovers questions that competition law is unequipped to address, and leads to jurisdictional inconsistencies that would be better addressed through a different route.[115]

The main problem, however, is that the decision does not go far enough. On the one hand, the authority's approach is ambiguous on whether Facebook's monopoly status

113. *Id.* at 12.

114. *See* Bundeskartellamt *Press Release Bundeskartellamt prohibits Facebook from combining user data from different sources* (Feb. 7, 2019), https://perma.cc/33YH-PDB9.

115. *See, e.g.*, Giuseppe Colangelo & Mariateresa Maggiolino, *Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the U.S.*, 8 INT'L DATA PRIVACY L. 224 (2018); Jakob Kucharczyk, *The German FCO's Facebook Case: Blurring The Line Between Competition And Data Protection Enforcement, Disruptive Competition Project* (Feb. 8, 2019), https://perma.cc/M9E8-JJYE; Geoffrey Manne, *Doing Double Damage: The German Competition Authority's Facebook Decision Manages to Undermine both Antitrust and Data Protection Law*, TRUST ON THE MARKET BLOG (Feb. 8, 2019), https://perma.cc/4RSS-U8AP.

automatically makes users' consent less free and voluntary. In fact, larger companies hardly violate data protection law more consistently than smaller ones,[116] even though they do have the ability to access, process, and control more information and, thus, arguably have greater compliance obligations. The Bundeskartellamt's approach, however, does not really tackle that point. Its analysis is that dominance means that Facebook should not be able to impose unfair terms such as default data combinations as part of their terms of service, without offering viable alternatives and opt-outs.

If the analysis is limited to giving individuals more options to aggregate and disaggregate datasets, than in important ways it seems to undermine the argument about power asymmetries. Indeed, the authority oscillates between two kinds of harms: it insists that the problem is coercion of users into an unfair bargain, yet defines the harm as a loss of control recoverable through the design of more choices at the consent stage. A power imbalance requires more than a set of options to choose from, which is the remedy the authority puts forward in this case. In light of Facebook's power, increasing the number of choices will not solve the problem; users will keep opting for the least burdensome option amongst those that Facebook deems tolerable. Choice and control should imply an ability to negotiate or walk away, but users do not have it, nor will they.

Decisions that focus on "voluntary consent" as the desired goal, makes authorities vulnerable to responses, such as Facebook's public response in this case, that users in fact have a lot of choice on these markets, and that other options are only a click away.[117] The decision has now been overturned by the Düsseldorf Higher Regional Court, which has offered a narrow analysis of consent and has entirely neglected the question of power in the platform economy.[118] In proceedings for interim relief, the German court states that individuals in fact decide to opt into Facebook's terms autonomously, and that Facebook's

116. Justus Haucap, *The Facebook Decision: First Thoughts*, D'KART ANTITRUST BLOG (Feb. 7, 2019), https://perma.cc/CB7N-FZ2W.

117. Yvonne Cunnane & Nikhil Shanbhag, *Why We Disagree With the Bundeskartellamt*, FACEBOOK NEWSROOM (Feb. 7, 2019), https://perma.cc/XG8R-D9EH.

118. Oberlandesgericht [OLG], Aug. 26, 2019, VI-Kart 1/19 (V), https://perma.cc/QGR7-FR54.

data collection and combination practices have not been proved to harm Facebook's competitors; concluding that the German Bundeskartellamt's decision is, therefore, not good law.

The court's ruling confirms that correcting power asymmetries in the platform economy through consent is a fraught approach. No matter what we think of the Bundeskartellamt's innovative take, focusing on consent as a means of protecting individuals against platform power is reductive or vulnerable to criticism or both. We must become readier, as a society, to move beyond informed consent and to ask what kind of platform economy individuals deserve, regardless of the choices they might be able or willing to make in such economy.

C. Conclusions to Part II

Regulators and courts in both the United States and Europe focus narrowly on the criteria for freely given consent instead of asking whether the practice of consent is justified in the platform economy. Assuming the moral salience of a practice without asking whether it is justified in the circumstances, i.e. whether the background conditions for having the practice in the first place are just, unreasonably legitimizes it.

It might be argued that the GDPR's approach protects users and that it aims to achieve privacy by default with limited exceptions that consumers can consent to. This aspirational vision hardly matches the way the legislation is currently interpreted and complied with. Further, as long as voluntariness and disclosure are considered to be paramount, underlying questions of power and platform justice will remain obscured. This should serve as a warning for US policy-makers currently considering federal privacy legislation.

In what follows it will be shown that we in fact lack reason to understand the practice of notice and consent as legitimate in context under either of these regimes. Taking the three conditions for the morally transformative force of consent in turn, it will be argued that the legal practice we described does not take place under just background conditions in the platform economy, it attempts to transform things which cannot be so transformed, and it unreasonably affects third parties who lack a chance to be heard under the circumstances.

III. What Should Consent Protect Us Against?

Upon consideration, the legal practice of notice and consent seems a performative facade. However, our conclusion in this regard may be wrong and requires careful examination. To understand if there is reason to find the practice morally relevant in the platform economy, the first question we must ask is what consent is supposed to enable us to do. What does it allow us to protect and what can it shield us from? Considering notice and consent from this perspective allows us to realize that little of what consent allows us to do in fact serves our interests, and little of what we really need to do is enabled through notice and consent. Consent enables us to access a platform in exchange for access to our data, yet it hardly transforms our relationship with platforms in a way that benefits us more than them, and it hardly seems capable of protecting us against abusive and covert interferences. This discrepancy between what we have reason to want and what we actually tend to get through individual acts of consent will serve as important evidence to ground an argument about platform power and the lack of morally transformative force of consent in this context.

A. Interests in Data

Interests are what people value and care about. Interests here will not be understood as what people selfishly or subjectively care about but rather as things people objectively have reason to value.[119] Interests in dataflows and in the digital infrastructure can broadly be divided into three classes: (a) economic interests, individual or collective, over data and infrastructure as productive assets, including interests in the creation of new value through those data and infrastructure; (b) non-economic interests, mostly personal, in data or other infrastructure as constitutive of and/or significantly related to

119. In this sense, I adopt Thomas M. Scanlon's understanding of interests as objective things we have reason to value. *See* THOMAS M. SCANLON, WHAT WE OWE TO EACH OTHER (1998). This is in contrast to other views of interests as selfish motives. *See* DAVID HUME, ENQUIRIES CONCERNING HUMAN UNDERSTANDING AND CONCERNING THE PRINCIPLES OF MORALS (1975).

the shaping of one's own person in one's own eyes or in the eyes of others; and (c) interests, mostly collective, in using data or infrastructure for the pursuit of non-economic common goals.

These conflicting types of interests in data and infrastructure exist simultaneously: a hospital might have an economic interest, for instance a proprietary interest, over a list of patient names, treatments, and outcomes that one or more of their employees scrupulously compiled; Barbara, on the other hand, might have a non-proprietary data privacy interest in the display or not of her name and information on the list. Both interests could be said in the abstract to reasonably justify claims that each the hospital and Barbara might have against one another. While there may be circumstances where it would be reasonable for the hospital's claim to prevail, it seems that this would hardly be solely on economic or proprietary grounds, and that there would need to be other good reasons for overriding Barbara's interest, e.g. that the health of the nation depended on the maintenance of such a detailed list of patient names, treatments and outcomes, or that substantial healthcare research and innovation were being made possible through such list.

When it comes to the platform economy, notice and consent mechanisms are primarily used to allow claims based on economic interests (a) to prevail over claims based on personality or privacy interests (b). Collective interests of type (c) are rarely promoted or clarified through notice and consent. For instance, by consenting to Uber's collection and use of our browsing or geolocation data, we effectively preclude local governments from being able to access such information on their own terms, forcing them instead to negotiate with Uber on Uber's terms for data valuable to the collectivity. In some ways, therefore, it seems that by centering the attention on individualistic interests, the act of consenting in fact leads to the neglect of broader societal interests of type (c). On the other hand, as a hypothesis, interests of the non-economic (b) type appear to be protectable through consent. These include interests in data privacy, interests in protection against certain forms of personalized microtargeting, interests against being treated in a discriminatory or biased way, interests in due process, etc. As we will see, this hypothesis will prove largely incorrect. None of these interests can really be protected through notice and

consent. The interests that consent protects, if any, are the interests of individuals as consumers to purchase and try new products, and possibly the interests of individuals as political and cultural citizens to engage with others in a privately managed cultural and political public sphere.[120]

Before turning to an analysis of the individual interests that arise in the platform economy, three further remarks can be made on the basis of the example of Barbara and the hospital: (1) interests in data can vary in importance; (2) as a general hypothesis, interests of the non-economic (b) type appear to have greater moral salience than interests of the economic (a) type; and (3) consent plays an important role in allowing less salient, or inferior, interests to take priority over allegedly superior ones.

B. Online Interests and Online Harms:

1. Consumer Interests

For the sake of the argument in this Article, it will not be necessary to engage in an in-depth analysis of the nature and normative appeal of consumer interests in the context of the platform economy. It suffices to say that individuals in market economies such as the United States and the European Union have an interest in being able to choose amongst a variety of available products and services as consumers subject to normative constraints set by fundamental rights, consumer welfare, and general standards of fairness in market practices.

This also means that in a market economy, consumers' interests in making autonomous purchasing decisions can be constrained by normative considerations such as safety, fairness, or human dignity. Consumers in other words do not have an interest in being able to opt into or buy consumer products that have the potential to harm themselves or others. There are constraints on markets. An example are the very strict rules around food processing and labelling in both the United States and Europe, which forbid long distance sales of food that

120. On the meaning of a digital public sphere. S*ee* Jack M. Balkin, *Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society*, 79 N. Y. U. L. REV. 1 (2004); Jack M. Balkin, *Fixing Social Media's Grand Bargain*, Hoover Working Group on Nat'lSec., Tech., and Law, Aegis Series Paper No. 1814 (Oct. 16, 2018).

do not comply with certain regional or transnational standards of safety, origin, labelling, etc. The same is true of products or services that violate other basic fundamental rights. Consumers for example should not have the right to purchase products that are unacceptably manipulative or intrusive on their person or other persons.

This point will be explored below, but it is important to understand that the interests of consumers in choosing or purchasing on a market do not exist in a vacuum and are constrained by a variety of normative considerations.

2. Privacy

A Western right to privacy enforceable in courts was first recognized by Samuel Warren and Louis Brandeis in a famous piece in 1890.[121] A century later or more, academics and non-academics alike still debate the contents and contours of privacy law. This subsection traces a brief genealogy of our understanding of privacy as an interest that requires institutional protection. It traces the debate on privacy from questioning its very existence to understanding it as control over a personal sphere, to conceiving it as a more capacious right to a contextually reasonable flow of information about the self. It will be argued that a view of privacy as control over the self is too limited to account for our objective interests in privacy, which have to do with what others can access and learn about us. Thus, the boundaries of privacy cannot be managed through individualized decision-making but must be the fruit of a societal effort at redefining what fundamental rights mean and what the limits of markets must be in the 21st century.

a. Privacy Skepticisms

In an article entitled "The Right to Privacy,"[122] Judith Jarvis Thomson famously expressed the view that there can be no unitary and coherent content to the right to privacy and,

121. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

122. Judith J. Thomson, *The Right to Privacy*, 4 PHILOSOPHY & PUB. AFFAIRS 295, 310 (1975).

therefore, that, as a matter of theory, the right to privacy is an unhelpful construct. In her view, privacy is a bundle of rights that intersects with other clusters of rights including the right to property and rights over the person; any interference which we understand as a violation of privacy in her view amounts to a violation of some other right (e.g. the right to exclude others from one's body or possessions), or is overridden by other considerations (freedom of the press, voluntary disclosures of information to others). The issue with such account of privacy is that it does not make sense of our intuition that privacy interests require protections that in certain circumstances go beyond the protections commonly afforded to property, reputation, or personal integrity; lending one's car to a friend does not necessarily imply that the friend can look into every corner of the car and read any information left in there by accident. Thomas Scanlon has addressed this point, arguing that although there may be no unitary and coherent *right* to privacy, there is a unitary and coherent set of interests which we have in privacy and which require institutional protection.[123]

Yet even this view of a unitary set of interests in privacy has been doubted. A number of economists and social scientists have been busy carrying out experiments showing that our preferences for privacy are elusive or nonexistent, and do not seem to match the purported solidity of our preferences for other market goods. For instance, when privacy comes into conflict with other values such as the need to share information with others, Diana Tamir and Jason Mitchell have shown that disclosure tends to win because it provokes the activation of neural mechanisms associated with reward, such that humans are predisposed for self-disclosure.[124] Some economists have shown that privacy preferences are not always reliable,[125] yet others have been able to show that we have interests in placing limits on other people's access to information about us. While individuals at times give up personal data irrationally, they also

123. *See* Thomas M. Scanlon, *Thomson on Privacy*, 4 PHILOSOPHY & PUB. AFFAIRS 315, 315 (1975).

124. Diana I. Tamir & Jason P. Mitchell, *Disclosing Information About the Self is Intrinsically Rewarding*, 109 Proceedings of the Nat'l Acad. of Sci. of the United States of America 8038, 8038 (2012).

125. Susan Athey et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* 1–26 (Nat'l Bureau of Econ. Research Working Paper No. 234882017), https://perma.cc/9UNW-K9SL.

at other times display exceptional commitment to shielding their information from access.[126] Once a person has privacy they seem to want to keep it.[127]

These findings tell us something about our revealed market preferences and whether or not we have stable preferences for privacy, but they do not tell us much about our *objective* reasons for valuing privacy, i.e. why we need to place limits on the extractive, exploitative, and manipulative extension of digital markets into our lives no matter what we tend to subjectively prefer or want on these very markets. Without a theory on why and how to limit the expansion of digital markets, it seems we are missing an essential component of human life and resigning to alienation and hopelessness in an increasingly connected, dataveilled and colonized modern life.

b. Privacy as Control

Because the contours of privacy are difficult to delineate though patterns of revealed preferences, many have thus wanted to understand privacy not as a set of stable 'things' we must protect but rather as being about the self-policing of personal boundaries, or control over a sphere of self-defined personal autonomy. The idea that privacy is fundamentally about control is ubiquitous: the journalist Charlie Warzel defines privacy as being "*about how . . . data is used to take away our control,*"[128] and tech CEOs like to emphasize "privacy controls" in their speeches on privacy.[129]

A number of scholars have provided normative justifications for the claim that privacy is a right to individually control personal information. For Alan Westin it is "*the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is*

126. Acquisti et al., *supra* note 57, at 510.

127. Alessandro Acquisti et al., *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249, 264 (2013).

128. Charlie Warzel, *Privacy Is Too Big to Understand*, N.Y. TIMES (Apr. 18, 2019), https://perma.cc/5MMG-5HH8.

129. Josh Constine, *Zuckerberg Says Facebook Will Offer GDPR Privacy Controls Everywhere*, TECHCRUNCH (Apr. 4, 2018), https://techcrunch.com/2018/04/04/zuckerberg-gdpr/. *See also Privacy Controls*, GOOGLE, https://perma.cc/94KW-YFVU.

communicated to others,"[130] Jerry Kang defines it as "*an individual's control over the processing – i.e., the acquisition, disclosure, and use – of personal information.*"[131] Proprietary understandings of data are also strongly correlated to notions of control over information.[132] Charles Fried's account of the foundations of privacy illustrates the general understanding of privacy as a form of control.[133] Fried rejects instrumental arguments such as Thomson's that privacy is only a means to protect some other values, and instead advances a positive Kantian view of the right to privacy: to make most human relationships of respect, love, friendship, and trust meaningful we need to make space for an interest in privacy. He states that:

> As a first approximation, privacy seems to be related to secrecy, to limiting the knowledge of others about oneself. This notion must be refined. It is not true, for instance, that the less that is known about us the more privacy we have. Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.[134]

Centrally, the emphasis on control is premised on a faith in individual decision-making as the default means for governing personal information. Where Fried's view starts to break down is in contexts where individuals can hardly be understood as good decision-makers. In those circumstances, which are exactly the circumstances that this Article explores, we need to look for a different way to understand how the extension of markets into private life should be limited.

---

130. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

131. JerryKang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV 1193, 1203 (1998).

132. *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 17 HARV. L. REV 2055, 2057 (2004); Lauren H. Scholz, *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113 (2016); Jeff Sovern, *Opting in, Opting out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

133. Charles Fried, *Privacy: A Moral Analysis*, 77 YALE L. J. 475, 482 (1968).

134. *Id.* at 482.

c. Beyond Control

When it comes to the digital economy, pervasive behavioral manipulability, enclosure, and conditioning of individuals have led more than one scholar to argue against an understanding of privacy as control.

In her work, Julie Cohen shows that accounts based on individual control and consent are theoretically misleading.[135] One of her arguments is that grounding privacy on rational decision-making, autonomy, and dignity prioritizes some forms of autonomy, generally individual-centric interests in receiving information, over other autonomy interests, such as the interest in engaging and coexisting with others. She points out that these autonomy-based accounts rarely show us how to adjudicate conflicts between different sets of autonomy interests. As she puts it, "*[i]nterrogating the conceptions of autonomy that exist in privacy theory exposes a deep conceptual poverty about what selves are made of.*"[136]

Helen Nissenbaum's view of privacy as contextual integrity also goes beyond individualized preferences and control over the self.[137] She argues that visions of privacy as control fail to account for the fact that privacy is not only about self-policing but also about how others access and experience information about us. She envisions privacy as a right over a contextually appropriate flow of information, understood by reference to the notion of contextual integrity, which is a method for evaluating the appropriateness of existing informational norms in context. Informational norms, according to Nissenbaum, vary depending on the people between whom information flows, the types of information being shared and the normative principles governing the transmission of any given information.[138] By applying a contextual approach to privacy, Nissenbaum is able to depart from control and to adopt a more holistic perspective

135. *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE AND THE PLAY OF EVERYDAY PRACTICE (2012), ch.5 [hereinafter *NETWORKED SELF*].

136. *Id.* at 114.

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

138. *Id.* at 140.

on information governance.

More broadly, what scholars such as Cohen, Nissenbaum or Shoshana Zuboff see as central to a normative understanding of privacy today is the need to limit the advancement of digital markets and the focus on economic efficiency in order to safeguard, protect, and honor human life in a commodified environment. Rather than focusing on the empirical stability of our privacy preferences, or on the philosophical coherence of our privacy interests, we ought to focus on the reasonable limits that should be placed on extractive commercial incentives' ability to erode spaces for the self.

3. Interests in Enjoying the Benefits of the Informational Public Sphere without Suffering Manipulation, Microtargeting and other Algorithmic Harms

Looking beyond the contested notion of privacy, we seem to have an interest in enjoying the benefits of the informational economy without suffering objectionable forms of manipulation and other harms such as algorithmic bias, discrimination, polarization, and lack of due process. While we might want to understand notice and consent as being aligned with our interest in accessing online content, blank access to content, without protection from manipulation and other online harms, does not seem tolerable. Insofar as notice and consent purports to allow us to access platforms without protecting us from these harms, its operation does not seem to align with our interests.

a. Access to the Informational Public Sphere

We have an interest, as members of social communities, in exchanging information, imparting, and being imparted information. We have reasons, for instance, to access content on Facebook, YouTube, Twitter, or Google Search, in participating in discussions and making personal content available on these platforms.

One philosophical justification for this interest can be found in John Stuart Mill's notorious utilitarian defense of speech and freedom of conscience, that our ability to speak and develop thoughts without constraints is deeply connected to our individuality, and that suppressing speech and the ability to

exchange information risks propelling us into tyranny.[139] One could think this means that we need unrestrained access to as much content and opportunities for exchange as possible and that notice and consent practices' limited interference with the ability of individuals to access platform content offers the ideal means of promoting our interest in accessing and participating in the informational public sphere. Consent as an enabler of permissionless speech in other words seems to align with Mill's vision of a liberal society.

A Millian rationale for minimizing constraints on imparting and being imparted information rests on at least two false assumptions, however. The first assumption is an unreasonable faith in the self-regulating free flow of opinions, or "*marketplace of ideas*,"[140] i.e. the fact that opinions that are misleading or false can be corrected by allowing unrestrained flows of counter-speech to progressively displace them. This might have been empirically true in 1859 or in the 1920s when speech used to be channeled in a top-down manner through a limited number of closely controlled bottlenecks and when the main concern was to ensure that the information that reached individuals would remain as diverse as possible. This is certainly no longer true in the platform economy, where the oversupply of ideas seems to be saturating the marketplace leading to purported 'market failures.'[141] Flows of counter-speech today are in fact leading to greater polarization and conspiracies, rather than a healthy and pluralistic informational public sphere.[142] Therefore, we may need to place constraints on users' terms of access and

139. *See generally* JOHN STUART MILL, ON LIBERTY (1859).

140. *See, e.g.*, Abrams v. United States, 250 U.S. 616 (1919) (Holmes, J., dissenting); Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring).

141. *See* Stanley Ingber, *The Marketplace of Ideas: A Legitimizing Myth*, 1 Duke L.J. (1984) (discussing the notion of a failure of the marketplace of ideas); *see also* C. Edwin. Baker, 8 CONST. COMMENT. 164 (1989) (book review). Oreste Pollicino has been discussing the notion of market failures in relation to the issue of "fake news." *See* Oreste Pollicino, *Editorial, Fake News, Internet and Metaphors (to be handled carefully)*, 9 ITALIAN J. PUB. L. (2017).

142. *See, e.g.*, CASS R. SUNSTEIN, #REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA (2017); YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS (2018); Claudio Lombardi, *The Illusion of a "Marketplace of Ideas" and the Right to Truth*, AMERICAN AFFAIRS J., Vol III (Spring 2019), https://americanaffairsjournal.org/2019/02/the-illusion-of-a-marketplace-of-ideas-and-the-right-to-truth/ (last visited Nov. 25, 2019).

participation that go beyond individual consent.

The second related assumption is that speech can best be protected if the individual is recognized as the sole and ultimate source of authority regarding how and what information can be shared on the marketplace of ideas. Platforms are constantly designing and manipulating the kinds of speech that is shared and accessed online, through design nudges and the intervention of their employees, reviewers, and algorithms.[143] The information we access is always *mediated* by others, who have their own purposes and manipulative intentions.[144] The likelihood that individuals will be manipulated when accessing a platform is indeed very high. It is not factually accurate to understand individuals as the ultimate decision-makers regarding content flowing online.

Richard Strauss argues that we must understand the interest in imparting and being imparted information as grounded in a Kantian principle of autonomy that individuals have a right to communicate and cultivate themselves as ends in themselves and never as means.[145] By allowing individuals to be manipulated on digital platforms, we in fact allow others, e.g. Facebook or political propagandists, to treat these individuals as means instead of ends and to hinder their ability to determine their own life plans. Thus, we must enable speech and information exchange on platforms in a permissive way only to the extent permissionless exchange aligns with the imperative of respecting persons as ends and never to instrumentalize or manipulate them.

Even if we were to reject Strauss' Kantian principle of autonomy as a persuasive understanding of our reasons to access and share information in digital settings, we can infer from this discussion that we retain an interest in being shielded from certain forms of manipulation, coercion, and harm in spite

143. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 598 (2018); *see also* TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET: PLATFORMS, CONTENT MODERATION, AND THE HIDDEN DECISIONS THAT SHAPE SOCIAL MEDIA (2018); Anupam Chander and Vivek Krishnamurthy, *The Myth of the Neutral Platform*, 2 GEO. L. TECH. REV. 400 (2018).

144. NICK COULDRY & ANDREAS HEPP, THE MEDIATED CONSTRUCTION OF REALITY (2016).

145. David Strauss, *Persuasion, Autonomy, and Freedom of Expression*, 91 COLUM. L. REV. 334 (1991).

of our interest in accessing platforms. Consent cannot advance our interest in benefiting from the informational public sphere to the extent it subjects us to these risks.

b. Manipulation

What forms of coercion and manipulation do we have an interest in being shielded against?

It seems that any understanding of manipulation on platforms must take into account the following dimensions of digital life: (1) technology makes the storage and display of our vulnerabilities in the form of digital traces not only possible but also relentless and permanent, (2) information asymmetries and partial information are pervasive, (3) our digital choices are distorted by design constraints so that we are not always or ever fully in control of our online decisions and their consequences, (4) lock-in mechanisms psychologically enclose us right after access constraining our ability and willingness to look for outside options, and (5) most if not all of our online choices impose costs on unaware third parties.

Tal Zarsky has emphasized the importance of manipulation for understanding digital harms today.[146] He defines manipulation broadly, as influence that is unfair or unacceptable, and he considers data-driven manipulation as substantially different from all previous forms of manipulation because it is hidden, personalized, and ubiquitous.[147] Daniel Susser, Beate Roessler, and Helen Nissenbaum have similarly argued that manipulation is particularly salient in digital environments.[148] Manipulation to them is a deliberate hidden influence, and manipulating is the act of "*intentionally and covertly influencing decision-making, by targeting and exploiting decision-making vulnerabilities.*"[149] This phenomenon is

146. Tal Zarsky, *Privacy and Manipulation in the Digital Age*, 20.1 THEORETICAL INQUIRIES L. 157 (2019).

147. *See* Karen Yeung, *Hypernudge: Big Data as a Mode of Regulation by Design*, 20 INFO. COMM. & SOC'Y 118 (2017) (discussing data-driven influence and data exceptionalism).

148. Susser et al., *infra* note 149; *see also* Daniel Susser et al., *Online Manipulation: Hidden Influences in a Digital World*, 3 GEO. L. TECH. REV. (forthcoming 2019).

149. Daniel Susser, Beate Roessler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV. 1, 4 (2019).

particularly prevalent in the platform economy.

The focus of both these accounts on deliberate covert acts that are personalized and target vulnerabilities seems to capture part of what makes certain actions objectionable in the digital context; their covertness does not afford us an opportunity to understand the impacts they have on us, and to shape our lives accordingly. In Stanley Benn's view,[150] which aligns with Richard Strauss' above,[151] when platforms deliberately manipulate us and use information about us in ways that we cannot fully understand, they impair our very understanding of ourselves and of the context that surrounds us, denying us respect as persons. As Benn puts it, "*to respect someone as a person is to concede that one ought to take account of the way in which his enterprise might be affected by one's own decisions*."[152] Further, "*[o]ne cannot be said to respect a man . . . if one knowingly and deliberately alters his conditions of action, concealing the fact from him*."[153] What makes manipulative interferences particularly objectionable in the platform context is that these interferences instrumentalize us for profit or other selfish motives, impairing our ability to shape our existence in accordance with our own plans, and thereby fail to afford us the respect we are owed as persons.

To the extent manipulation is covert, can consent and disclosures solve it? A move to transparent disclosure, assuming it is feasible, risks boosting even more opaque manipulative techniques. Julie Cohen notes that, as notice and consent became established in the United States as the dominant device for regulating corporate digital tracking techniques this practically incentivized "*the quest to track internet users by less transparent means . . . pushing ever more deeply into the logical and hardware layers of consumers' devices.*"[154]

To tackle manipulation and microtargeting on online platforms, therefore, we need to first look beyond terms and conditions and disclosures at how power and money are

150. Stanley I. Benn, *Privacy, Freedom and Respect for Persons*, *in* FERDINAND D. SCHOEMAN (ED.), PHILOSOPHICAL DIMENSIONS OF PRIVACY (1984).

151. Strauss, *supra* note 145.

152. Benn, *supra* note 150, at 229.

153. *Id.* at 230.

154. JULIE E. COHEN, BETWEEN TRUTH AND POWER 56–57 (2019) [hereinafter *TRUTH AND POWER*].

channeled through existing infrastructure and data and then to open-up and regulate those bottlenecks. One such bottleneck is indeed the idealized and seamless practice of notice and consent. Other bottlenecks include data collection and profiling practices, ad-based business models, information-sorting algorithms, and the exploitative reliance on temporary contractors at scale.

c. Bias, Discrimination, Lack of Due Process

In parallel, and still beyond privacy, many scholars have uncovered and described a multitude of other hidden harms that result from the deployment of opaque automated algorithms at scale.[155] When one clicks that they have read and understand Google or Facebook's terms of service, one is in fact accepting these diffuse harms.

Mittelstadt et al. identify at least seven concerns with the use of machine learning algorithms, including as deployed by platforms such as Google or Facebook.[156] These include concerns about the biased and unfair nature of the outcomes of machine learning systems, which relate to how machine learning systems operate, but also to the training and input data used and the broader context within which machine learning is deployed; concerns with the "transformative effects" of machine learning systems such as effects on how we experience the political system and the world as mediated through these systems; and epistemological concerns relating to the evidence produced through machine learning systems including lack of explainability and interpretability of algorithms. Other harms

155. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1314 (2008); Citron & Pasquale, *infra* note 159; Jane Bambauer & Tal Zarsky, *The Algorithm Game*, 94 NOTRE DAME L. REV. 1 (2018); Brent Daniel Mittelstadt et al., *The Ethics of Algorithms: Mapping the Debate*, 3 BIG DATA & SOC'Y. (2016); Lilian Edwards & Michael Veale, *Slave to the Algorithm: Why a Right to an Explanation is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18 (2017); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection in the Age of Big Data and AI*, COLUM. BUS. L. REV., (forthcoming 2019); Frederike Kaltheuner & Elettra Bietti, *Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR*, 2 J. OF INF. RTS, POL'Y. & PRAC. (2018); Reuben Binns, *Fairness in Machine Learning: Lessons from Political Philosophy*, 81 J. MACHINE LEARNING RES. (2018).

156. Brent Daniel Mittelstadt et al., *The Ethics of Algorithms: Mapping the Debate*, 3 BIG DATA & SOC'Y. (2016).

include chilling effects on speech, filter bubbles and polarization.[157]

Danielle Citron and Frank Pasquale's work on technological due process describes algorithmic decision-making as entailing a variety of risks, including a very high tendency to perpetuate pre-existing inequalities and implicit biases through their opacity, arbitrary application, and disparate impacts:[158] "*[s]coring systems can have a powerful allure – their simplicity gives the illusion of precision and reliability. But predictive algorithms can be anything but accurate and fair. They can narrow people's life opportunities in arbitrary and discriminatory ways.*"[159] These harms in turn have prompted inquiries into novel forms of due process in opaque digital environments where individuals are unable to foresee the harms.

Karen Yeung considers some of the novel threats posed by big data and algorithms through the lens of the "hypernudge."[160] Algorithms operate through a recursive feedback loop that extends in three directions: constant refinement of the choice environment, constant data feedback to the choice architect, and constant comparison of the individual's choice environment to wider population trends. In so doing, these systems also inherently shape our cognitive environment within platforms, nudging us toward pre-designed choices and decisions.[161] Tufekci similarly provides an account of platform-related algorithmic harms dividing them into two broad groups:[162]

---

157. *See, e.g.*, Kaltheuner & Bietti, *supra* note 155, at 2; *Opinion of the European Data Protection Supervisor* (Mar. 19, 2018), https://perma.cc/85MP-R5VA.

158. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U.L. REV. 1249 (2008); Citron & Pasquale, *infra* note 159.

159. Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 33 (2014).

160. Karen Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design*, 20 INFO., COMM. & SOC'Y. 118 (2016).

161. Karen Yeung shows that like any other regulatory design mechanism, algorithms possess three "cybernetic" features: information gathering and monitoring, standard-setting, and behavior modification. *See* CHRISTOPHER HOOD, HENRY ROTHSTEIN & ROBERT BALDWIN, THE GOVERNMENT OF RISK: UNDERSTANDING RISK REGULATION REGIMES (2001).

162. *See* Zeynep Tufekci, *Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency*, 13 COLO. TECH. L. J. 203 (2015).

concerns with lack of visibility, information asymmetries and hidden influences on the one hand and concerns with inferences and profiling on the other. Many of these harms overlap closely with manipulative harms and respect for persons, as discussed.

C. Conclusions to Part III

Overall, it seems that when an individual clicks and accepts certain terms and conditions and consents to a platform's privacy policy, they are in fact agreeing to a number of hidden forms of intrusive and manipulative data collection, use and storage practices, interferences, and opaque treatments. As a result, it may lead to various harms to oneself and to others, including losses of respect and dignity, discriminatory impacts, and other systemic effects connected to commodification and the erosion of spaces for the self. In these circumstances, we must seriously question whether the emphasis on individualized notice and consent as a device which enables access and choice is appropriate and whether even the most extensive disclosure and the most freely given consent is actually sufficient to protect us from diffuse and systemic harms in the platform economy.

As said in Part I of this Article, consent's magic is that it can transform the relationship between two or more people and change the justifications each of them, as well as external observers, have for their respective behaviors. In the platform context, this hardly seems the case. It certainly seems to legitimate companies' practices, but hardly empowers individuals to make real choices in the platform economy on how to structure their relationship with these companies. The gap between what we have reason to want and what we seem to actually prefer in the platform economy, between what we get and what platforms get, points to an underlying power struggle. It is in the context of this power struggle, therefore, that notice and consent mechanisms have acquired a special importance, as a solution that appears to make practical sense on its face and that in fact acts as a free pass that promotes the political and economic interests of large data conglomerates. By accepting the terms and conditions, individuals pursue their consumer preferences and are given the right to access platform content at the cost of giving up on fundamental human interests in being treated with respect, not being discriminated and manipulated,

and not being subjected to covert harms that they cannot properly be warned of. Although some might consider these harms tolerable, the next section explains why they cannot be deemed tolerable to everyone.

IV. The Mirage of Transformation

We said that consent's transformative moral force requires the embodiment of at least three things: (a) the possibility of free, autonomous consent given under just background conditions; (b) the interests, rights, and states of affairs purportedly being transformed, can actually be transformed by the consent; and (c) the consent does not unreasonably harm third parties. Having articulated some of the things we might want to see protected in the platform economy, it seems that most of these things are not of a kind that can be alienated or transformed, and that some are diffuse and collective in kind, meaning that their disposal through individualized notice and consent can significantly harm third parties. Respect, dignity, and non-discrimination are arguably so essential that they give rise to thick institutional protection in the form of inalienable rights. Other interests, such as those in having a say over how data is collected and used or in preventing extensive commodification and datafication are collective concerns that might not be strictly inalienable but require collective governance solutions. This section examines the collective dimensions and the inalienable interests that notice and consent purportedly transform, showing that consent lacks morally transformative force in relation to these concerns and simply acts as a performative façade that normalizes the platform economy.

A. Collective Goods and Collective Governance

An important reason for doubting the transformative force of notice and consent in the platform economy is that the erosion of privacy, the commodification of personal data, and the increasing colonization by markets of spaces for the self all seem to be affecting people collectively, by on the one hand creating isolation, personalization, and the loss of a sense of community and on the other hand maintaining artificial interpersonal

connections through opaque data patterns. A concern is that managing data in an individualized way, through notice and consent, only increases these problems, accentuating isolation and the fragmented management of diffuse harms.[163] More concretely, data can be about a variety of individuals at once, and the consent of some may result in consequences that affect others. This issue arose as part of the Cambridge Analytica scandal:[164] when individuals agreed to use Kogan's quiz app and letting the app access their personal information, they also agreed to the app's access to personal information about their friends whose Facebook settings allowed it. This is what Maggie Koerth-Baker called the "*privacy of the commons*"[165] problem, defining it as:

> what happens when one person's voluntary disclosure of personal information exposes the personal information of others who had no say in the matter. Your choices didn't cause the breach. Your choices can't prevent it, either. Welcome to a world where you can't opt out of sharing, even if you didn't opt in.[166]

It has also long become apparent that the more personal data a business can link together through network effects, the more the usefulness of any datapoint within that network increases. Google search is a good example of a service whose quality increases for searchers in proportion of the data Google accumulates about other people's searches. This also means companies have an incentive to abuse the collective dimensions

163. *See* Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1 (2019); Barocas & Nissenbaum, *supra* note 11; *see also* Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904 (2013); *NETWORKED SELF*, *supra* note 135.

164. Nadeem Badshah, *Facebook to Contact 87 Million Users Affected by Data Breach*, THE GUARDIAN (Apr. 8, 2018), https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach.

165. *See infra* note 166; *see also* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968), https://science.sciencemag.org/content/sci/162/3859/1243.full.pdf.

166. Maggie Koerth, *You Can't Opt Out Of Sharing Your Data, Even If You Didn't Opt In*, FIFTHYTHIRTYEIGHT (May 3, 2018), https://perma.cc/7UNW-2WBJ.

of data by letting each user generate information about others.

The collective nature of privacy and data harms points in the direction of collective mechanisms for managing data instead of individualized notice and consent. Framing data as a commons owned by communities of people, and developing initiatives such as data cooperatives, trusts and collective management schemes give us reason to hope.[167] However, the devil in these cases is in the details: Are these initiatives giving power to people to change current incentives and commercial structures? Do they lead to a mere redistribution of value from the top or do they create opportunities to re-frame our understanding of value?

1. Liberal Rights and Collective Governance

The collective nature of privacy harms is a very powerful reason for rethinking the centrality of notice and consent, resisting an understanding of privacy as control over data, and looking to collective management solutions. However, when it comes to minimizing data collection and limiting excessive intrusions or commodification of data, there are good reasons to keep taking rights seriously. The primary reason for this is that some understandings of collective self-management do not account for the value of certain fundamental interests of persons, such as the interest in dignity and in being respected as a person and not manipulated, commodified, or harmed for profit. Data collectives can indeed function as a coherent community while having as their primary purpose the monetization and exploitation of collective data. While this may seem individually acceptable to some, allowing the data of a group to be exploited for profit can mean denying dignity and respect to members of that group including some who willingly accepted it and others. Another way of putting it is to say that if Facebook were to become a collective, or if a collective were to engage in the same data intrusive practices as Facebook during the Cambridge Analytica episode, a collective would not eliminate the disvalue of those activities for the group and its

167. *See, e.g.*, MARIANA MAZZUCATO, THE VALUE OF EVERYTHING: MAKING AND TAKING IN THE GLOBAL ECONOMY (2018); Benedetto Vecchi, *I Dati Sono un Bene Comune e Appartengono ai Cittadini*, IL MANIFESTO(Nov. 6, 2019); DECODE PROJECT, https://decodeproject.eu/ (last visited Nov. 25, 2019).

single members. Group membership does not prevent practices that violate certain inalienable rights of persons.

Liberal theorists such as Joseph Raz, Thomas Scanlon, John Rawls, and others have developed nuanced understandings of the relationship between individual entitlements and the collective good.[168] Each of them has argued that taking individual rights seriously does not entail an abdication of collective values, and, factually speaking, in most circumstances the collective good overrides individualist pursuits.[169] Raz understands morality as primarily non-individualistic and non-rights-based but still recognizes the important role that rights play in protecting the fundamental value of each person. Focusing on "interests" as a basis for rights allows him to make sense of the fact that some interests do not bear only on individuals but also on groups and that only a subset of these interests require individual rights protection. Some interests can be valued and vindicated through means such as collective organizing. Rights can also have a collective dimension, socio-economic rights are an example.[170]

B. Inalienable Rights

Another important reason for resisting consent is that some of the interests that it purportedly allows us to pursue, or the rights it purportedly allows us to transform, are constitutive of our person and thus inalienable; they are so fundamental to who we are that they cannot be disposed of through acts of the will. It is useful to explain why we have inalienable rights not to be manipulated or harmed in the platform context. The following clarifies the debate on inalienability by articulating what it means to have an inalienable right, relying on the example of our inalienable right against manipulative intrusions.

---

168. *See* RAZ, *supra* note 21, at 163; *see also* THOMAS SCANLON, WHAT WE OWE TO EACH OTHER (1998).

169. An example is John Rawls' difference principle, which posits that welfare increases, to be justified, must benefit the least advantaged at least as much if not more than the more advantaged. *See* Samuel Freeman, *Illiberal Libertarians: Why Libertarianism Is Not a Liberal View*, 30 PHIL. & PUB. AFF. 105 (2001).

170. International Covenant on Economic, Social and Cultural Rights, Dec. 16 1966, 993 U.N.T.S. 3.

1. Controversies over Alienability

Privacy as a basic fundamental right is guaranteed in equal measure to all under several state constitutions and international charters.[171] The text of the California State Constitution even stipulates that *"[a]ll people are by their nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness and privacy."*[172] Values such as personal integrity,[173] human dignity, and self-determination[174] have also been considered inalienable.[175]

A right is inalienable if it is so basic as to constitute what it means to be a human. For Immanuel Kant, the inalienability of rights is required to ensure that each person maintains their equal status as persons with equal dignity: one cannot give up one's capacity for freedom because giving away freedom means giving away humanity.[176] John Stuart Mill also recognizes limits to our capacity to trade away aspects of our freedom irreversibly; one cannot enslave oneself, for example, because it would mean giving up being a free person for good.[177] Inalienability in other words is what ensures that people are treated as humans with equal basic rights instead of as means,

171. *See, e.g.*, Universal Declaration of Human Rights art. 12, Dec. 10, 1948; International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171; European Convention on Human Rights art 8, Nov. 4, 1950.

172. CAL. CONST. art. I, § 1.

173. *See* Helen Nissenbaum's account of privacy as contextual integrity. NISSENBAUM, *supra* note 137.

174. *See Bundesverfassungsgericht [BVERFGE][Federal Constitutional Court] October 18-19, 1983, 65 BVERFGE 1 (Ger.). See also* IMMANUEL KANT, FOUNDATIONS OF THE METAPHYSICS OF MORALS (1785) (discussing the philosophical notions of dignity and self-determination).

175. Samuel Freeman, *Illiberal Libertarians: Why Libertarianism Is Not a Liberal View*, 30 PHIL. & PUB. AFF. 105 (2001); *see also* Conseil d'Etat, *supra* note 34.

176. IMMANUEL KANT, THE METAPHYSICAL ELEMENTS OF JUSTICE 98 (John Ladd trans., New York Library of Liberal Arts, 1965) (1797).

177. MILL, *supra* note 139, ch. 5. *See also* BRIAN BARRY, CULTURE AND EQUALITY 148 (2001), in relation to the right of exit inherent in the freedom to associate; Hallie Liberto, *The Problem with Sexual Promises*, 127 ETHICS (2017) (discussing the withdrawal of sexual promises).

slaves, or property.[178]

When it comes to data and privacy, inalienability has been doubted or defined narrowly.[179] One possible reason is that there is serious disagreement over whether trading away one's data or giving up aspects of one's privacy entails losing core aspects of freedom or well-being. Part of the disagreement is due to the fact that we currently live our lives in an environment that already commodifies us for various commercial purposes. The question that divides us then is whether or not such commodification is objectionable and denies us essential privacy protections. It is argued here that it does, and that a compelling understanding of privacy requires an account of what it means for aspects of our privacy to be inalienable.

2. The Right against Manipulative Intrusions

Thomas Scanlon, like Joseph Raz, offers an interest-based theory of rights which both clarifies the relationship between interests and rights and helps uncover what the inalienable core of our online rights might be about.[180] As said in Part III, interests are what people value and care about, not what they selfishly or subjectively want but what they objectively have reason to value. Scanlon defines rights as "*constraints on discretion to act that we believe [are] important means for avoiding morally unacceptable consequences*."[181] To claim a right violation for Scanlon means to claim three things: (1) that a discretionary course of action by private or institutional actors leads to unacceptable consequences, (2) that constraints over such discretion are possible, and (3) that said course of action in fact violates such constraints.[182] Scanlon believes a right has three essential components: (1) an *ends*, i.e. interests, harms,

178. Freeman, *supra* note 169, at 113.

179. *See, e.g.*, Václav Janeček & Gianclaudio Malgieri, *Data Extra Commercium*, DATA AS COUNTER-PERFORMANCE – CONTRACT LAW 2.0? (forthcoming 2019); ADAM D. MOORE, PRIVACY, INTERESTS, AND INALIENABLE RIGHTS (2018).

180. THOMAS M. SCANLON, *Content Regulation Reconsidered*, *in* THE DIFFICULTY OF TOLERANCE: ESSAYS IN POLITICAL PHILOSOPHY 151 (2003).

181. *Id.* at 151.

182. *Id.* at 152.

goals or values that makes us consider given consequences as unacceptable and given constraints as justified (e.g. the interest in privacy, the interest in the prevention of manipulative interferences); (2) a *means*, i.e. constraints the right is said to involve in order to protect the ends (e.g. notice and consent, data minimization requirements, access to judicial enforcement); and (3) a *link* between empirical beliefs as to possible unacceptable consequences and beliefs as to consequences of the constraints the right proposes. Thus, for Scanlon determining the existence and boundaries of a right is an exercise in reflective equilibrium[183] which must be grounded in a preliminary inquiry into the interests we have in constraining unreasonable actions that interfere with these interests. Given the significant empirical component of rights, Scanlon recognizes that the determination of rights necessarily entails a degree of "*creative instability*" and that rights have a protean, dynamic existence that can never be fully captured.

a. The Ends: Protection against Manipulative Intrusions

This subsection shows that data privacy is coextensive with protection from data-driven manipulative practices online, and explains what these interests are about and why they are inalienable.

In an early piece, Scanlon developed an understanding of the right to privacy, linking our interests in privacy to enforceable constraints on the power to interfere with such interests.[184] Scanlon presents his views on privacy in response to Thomson's critique of the right to privacy outlined above, yet he does not go far beyond arguing that the unitary nature of privacy can be found in a set of special interests we have in being able to be free from certain kinds of intrusions.[185] Such interests include specific interests in not being seen, overheard, etc., and also broader interests in having a conventionally defined "*zone of privacy in which we can carry out our activities without the necessity of being continually alert for possible observers,*

183. RAWLS, *supra* note 32, at 42–45.
184. *See* Scanlon, *supra* note 123; *See* Thomson, *supra* note 122.
185. Thomson, *supra* note 122.

listeners, etc." Scanlon emphasizes the importance of convention to define "*a zone of privacy immune from specified interventions*." He also notes that technological advances may require us to extend old conventions or to change them in the face of a new situation.[186]

There is something intuitively appealing in the idea that privacy's unitary nature can be found in the need to be protected against certain kinds of intrusions and interferences, and that any potential "zone of privacy" must be defined and understood within a given social context. Yet this must be qualified in two ways. First, we must tread carefully when speaking of "zones" of privacy in order not to obscure the diffuse and invisible nature of privacy violations and manipulative interferences in the platform economy. It is helpful for example to expand our understanding of privacy beyond spatiality by considering Helen Nissenbaum's theory of privacy as claims to *appropriate flows of information* about oneself,[187] or Mireille Hildebrandt's understanding of privacy as the freedom from unreasonable constraints on the construction of one's identity.[188]

Second, we need a criterion for distinguishing what is within the zone of reasonable privacy protection from what is outside of it. While Nissenbaum relies on the notion of "contextual integrity," her theory does not distinguish, other than on a case-by-case basis, between aspects of privacy that we can give up consensually and aspects of privacy that we ought not to be able to give up at all, i.e. alienable and inalienable aspects of privacy. Stanley Benn instead provides a normative criterion for this distinction which seems useful here.[189] His account grounds privacy in a Kantian understanding of respect for persons, i.e. the need to ensure that persons are treated as ends in themselves and never instrumentalized for the pursuit of someone else's aims. As seen, respect in the Kantian sense means treating a person as an end and allowing that person to choose her own ends. In the platform economy, respect means ensuring that each person is physically and mentally enabled to pursue a life of their own through a sufficient level of self-

186. *See* THOMAS M. SCANLON, WHAT WE OWE TO EACH OTHER 204 (1998).

187. NISSENBAUM, *supra* note 137.

188. *See* MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW (2015).

189. Benn, *supra* note 150.

awareness and understanding of their environment, sufficient space for independent thinking, etc. Thus ensuring that a person can flourish and make independent decisions about their life.

Data privacy seems, therefore, to be coextensive with protections against manipulative intrusions based on personal data, such as microtargeting or other behavior that undermines dignity and the capacity for self-awareness. Data surveillance and related manipulation should not be capable of being consented or opted into, to the extent they remain covert and blur the ability of individuals to make decisions regarding who they want to be, how they should vote, purchase, and more broadly how they want to conduct their lives. Protection against forms of interference that instrumentalize human life should prevail over a person's initial choice as a consumer to access a platform's gated services not knowing what might come next.

An even bolder line of argument on inalienability consists in saying that most if not all forms of data commodification lead to objectionable discriminatory treatment of persons, and that because such treatment is intolerable, no person should be allowed to accept it. A particularly salient case here is the way markets over data seem to incentivize people in need to give up their privacy while others maintain higher levels of protection, thus advantaging the rich.[190] The resulting inequalities and the surreptitious discriminatory treatment that might result from them in digital environments are important reasons for treating privacy and protection from manipulative intrusions as largely inalienable and as needing to be advanced in equal measure for all.

b. The Means: Beyond Notice and Consent

Having identified these special interests, the next step consists in asking how to design constraints that can prevent interferences with them. This question can be taken at varying levels of abstraction but is fundamentally about which institutions can ensure protection of given interests and how. As importantly emphasized by Julie Cohen, when thinking about

190. *See generally* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017).

how to protect our privacy, we must be aware that our understanding of it is in large part shaped by the universe of possible intrusions that current institutions, laws, and markets enable.[191] We must, therefore, be particularly imaginative—not take existing intrusions as to what privacy is but rather keep exploring what privacy might be, and how technology companies might respond to the introduction of new institutional, legal or technical, protections.

A Scanlonian approach to the means of data privacy protection prompts us to ask three questions about consent and its alternatives. First, whether, and to what extent, notice and consent can constitute a reasonable protection against existing and possible future interferences with our interests. Second, to the extent notice and consent is insufficient to protect us against harm, we must ask what alternatives it might be reasonable to put in place to protect them. Third, when thinking about implementing these alternatives, an important question is also who should be in charge of determining, designing and deploying these alternatives.

Regarding the first question, in the case of inalienable rights the answer is intuitive: to the extent these interests are inalienable, they cannot be given up through contractual agreements or acts of consent. Instead, to protect them we must put in place institutional protections that at least narrow the scope of the intrusive practices in question and at best render them unlawful and promote a reconfiguration of digital business models. Transparency and disclosure cannot protect platform users in this sense.

Potential answers to the second and third questions, above, will be developed further in Part V of this Article.

c. The Residual Case against Privacy Self-Management

We are left with the following two questions concerning aspects of privacy or online harms that are neither collective nor inalienable. First, if there are such aspects, what do they consist of? Second, to what extent can we legitimately disclose or consent to intrusions into these aspects of our private lives

191. *See* *TRUTH AND POWER*, *supra* note 154.

without giving up our core inalienable interest in data privacy and against manipulative intrusions?

Nothing said so far about inalienable rights amounts to saying that privacy is inalienable in its entirety. Under Nissenbaum, Scanlon's or other accounts, we may still be understood to have certain alienable interests in keeping certain information about ourselves private only as long as we choose not to disclose it. It seems legitimate to be able to alienate information in various ways: I may have a disease and choose to disclose the fact to my doctor, I may show a photo of my dress to a group of friends, I may invite a colleague into my home for lunch or tell them facts about my private life. If these disclosures were to be done by way of consent, e.g. a doctor asking about my disease, my friends asking if they can look at a photo, or a colleague asking if she can come into my house, then these would be instances where my consent would be performing its morally transformative role. However, none of these cases are cases of use or access to personal data in digital settings. The digital environment has rendered the question of alienation less straightforward.

When it comes to the Internet, there are good reasons to be able to decide how to share personal content on Facebook or Twitter, but we should distinguish between decisions about online content and decisions about online data, including metadata, geolocation and tracking data, inferred data, and behavioral data. Choosing to share information with an audience, on an online platform or elsewhere, does not mean accepting to be subjected to surreptitious targeted advertisement or inferences based on that information. While the first is a choice, the second is the result of a business model that undermines our ability to make informed choices.

Thomson relies on an example that can help clarify some misunderstandings. Her example is as follows:

> [I]f my husband and I are having a loud fight, behind open windows, so that we can easily be heard by the normal person who passes by, then if a passerby stops to listen, he violates no right of ours, and so in particular does not violate our right to privacy. Why doesn't he? I think it is because, though he listens to us, we have *let* him

> listen (whether intentionally or not), we have waived our right to not be listened to - for we took none of the conventional and easily available steps (such as closing the windows and lowering our voices) to prevent listening.[192]

For Thomson, leaving the windows open amounts to waiving a right which could be understood as a right to privacy. First, let us suppose the windows had been opened intentionally to let people listen. In that case, by inviting someone to cross a conventional boundary, to listen to my private conversation, I have waived the right to complain *about the boundary crossing itself*. When I invite my neighbor to dinner at my house, I cannot reasonably complain that my neighbor is inside my house having dinner. When I post a video publicly on YouTube, I cannot complain that people are looking at it. In these cases, I still have reasonable grounds to complain, however, when my neighbor picks up my tax returns on a table and reads them, or when YouTube starts showing me adverts based on the video's contents. A voluntary and intentional invitation to cross a privacy boundary can be understood as a waiver of the right to complain about that specific voluntary disclosure but it does not extinguish all claims to privacy within that sphere. There is in other words no window the voluntary opening of which, nor any box the voluntary ticking of which, extinguishes all of our alienable and inalienable interests in data privacy or makes any and all invasions of our data privacy interests reasonable.

As we have seen, the harm we need protection against is not only a privacy harm but includes manipulative intrusions. A mere failure to take conventional precautions against intrusions, such as leaving a window open, cannot amount to a waiver of a right to prevent intrusions in a dynamic and opaque space such as the platform economy where we cannot know which kinds of intrusions might exist let alone be harmful. Platforms are not apartments, they are more like open plans with invisible windows always open by default. Even though windows can in some cases be closed with some effort by individuals with acute vision or sophisticated tools, this may be a world to complain about, our interest in being respected as

192. Thomson, *supra* note 122, at 306.

persons and in not being covertly used or instrumentalized for others' selfish motives arguably being interfered with on an ongoing basis. Many people might never see windows being open, some people may see them, yet have a hard time closing them. All these people have reason to complain because they can envisage an alternative world where windows are not invisible or not always open by default. Yet in this hypothetical world, those who control the construction of windows prefer the world as it is, with default invisible open windows. These same entities who control the construction of windows in turn see notice and consent very favorably; it allows them to justify the status quo without incurring any liability or harm. It acts as a free pass on their otherwise illegitimate behavior.

We, therefore, should resist an expansive understanding of our alienable interests in privacy in the platform economy for at least five reasons. First, in this context there are very few aspects which we choose to disclose about ourselves that have no impact on others. Even willingly sharing certain kinds of information on platforms has effects on the information ecosystem of others, including how algorithms will make predictions about people with similar tastes. Second, choices to disclose information on platforms are not always clearly autonomous and are often induced by the behavior of others, or by psychological nudges that prompt us to keep logging in. Third, alienable privacy aspects can have discriminatory effects through data and algorithmic processing. Any information we disclose can lead to asymmetric treatments or biases. Markets over data, for instance, have the potential to lead to great inequalities. Fourth, sharing incentivizes sharing, commodification leads to more commodification, and this leads to long term alienation and harm.[193] There is harm in letting markets take advantage of individuals, even when what is being commodified is alienable if considered in isolation. Fifth, behind the shiny façade of content-sharing platforms lies a covert market for the appropriation and exploitation of personal data, and from the above discussion we have a right to inalienable protections against abuses on the latter front.

These arguments against commodification and against expansive understandings of alienable interests in data privacy

193. *See* KARL MARX, DAS KAPITAL (1867).

lead us to our discussion of platform power in Part V of this Article.

V. Consent as Disempowerment and Moving Beyond

It has been argued throughout this Article that consent cannot have morally transformative force unless three things are true: (a) consent must be largely free and autonomous and it must be given under just background conditions; (b) consent must be capable of transforming the rights, obligations, or states of affairs that it is being relied on to transform; and (c) consent must not have harmful effects on third parties. Parts III and IV have demonstrated that (b) and (c) cannot be true in the platform economy, because most, if not all, of the things consent is used to legitimate or transform are not transformable through acts of individualized consent. These things are either inalienable and constitutive of what it means to be a person with dignity, or their individualized and siloed transformation can have significant negative effects on third parties. This section extends the argument by showing that questions regarding inalienability (b) and the collectivity (c) are intimately related to the question of what it means for consent to be free, autonomous, and given under just background conditions (a). Specifically, to understand why notice and consent practices cannot have morally transformative force in the platform economy, we need to understand the power dimensions that underlie these practices.

This section offers further context on the debate on consent by framing it normatively as a question of justice, articulating why a capacious understanding of justice requires the inclusion of power considerations. It then shows why our reasons for valuing consent are weak, why arguments about paternalism miss the mark, and ends with an evaluation of platform governance options.

A. Beyond the Mirage of Transformation:

1. The Conditions for Voluntary Consent are Absent

Adding to the performative mirage of relying on consent to morally justify the curtailment of certain inalienable interests

and relationships, we must ask whether autonomous self-directed and voluntary consent of the kind described in Part I of this Article is an actual possibility in the digital ecosystem. Two sets of arguments are generally advanced to show that voluntary consent may itself be a mirage.

There are unbridgeable psychological barriers to full, informed, unambiguous and voluntary consent.

These barriers are as diverse as they are numerous. Structural complexity affects individuals' ability to make good decisions regarding their personal data.[194] Daniel Solove shows that individuals share data with hundreds of websites without realizing it.[195] Both data aggregation and the cumulative nature of harms in this space adds to the complexity of making sound choices; technology platforms process data continuously, they aggregate and disaggregate the data, add new data to pre-existing datasets, train models on old datasets and then let them run on new data, etc. The results are unpredictable, such that adding a small innocuous piece of information can have deleterious and unforeseen effects on vulnerable people.[196] Moreover, as said, there is evidence that people do not read the terms and conditions, and if they read them, often they do not understand them.[197] Further, people are biased in their privacy choices and easily affected by small changes in the choice and consent architecture.[198] We are inconsistent in that we say we care about privacy but then sign-up for a Twitter profile and post information publicly.[199] Susan Athey, Christian Catalini, and Catherine Tucker found that people with a concern about privacy have no second thoughts providing their friends' emails in exchange for pizza, and also that providing individuals with irrelevant but reassuring information about privacy protection in fact nudges them toward less privacy-friendly choices.[200] Cass

194. Solove & Hartzog, *supra* note 6, at 1888.

195. *Id*.

196. *See, e.g.*, CATHY O' NEIL, WEAPONS OF MATH DESTRUCTION (2016).

197. *See, e.g.*, Ben-Shahar & Schneider, *supra* note 56.

198. *See generally* Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, SECURITY & PRIVACY ECONOMICS 82 (Nov./Dec. 2009); SUNSTEIN & THALER, *infra* note 201.

199. *See* Harry G. Frankfurt, *Freedom of the Will and the Concept of a Person*, 68 J. OF PHIL. 5 (1971) (discussing the first and second order preferences).

200. Susan Athey et al., *supra* note 125. *See also* Acquisti et al., *supra*

Sunstein and Richard Thaler's work on nudges also provides interesting insights: for instance privacy *defaults* matter and users will hardly change them.[201] Familiarity with privacy risks[202] and the context of choice-making also affect the outcome of our decisions about privacy.[203] We also tend to be heavily influenced by other people's privacy choices,[204] and stick to bad privacy choices made in the past.[205] A small increase in the costs of one alternative can lead people to switch their attitude to privacy quite radically.[206]

There are legal and strategic barriers to full, informed, unambiguous and voluntary consent.

In addition to the psychological barriers to informed consent, legal, and strategic constraints make full transparency or meaningful disclosure are impossible. There is tension between fair disclosure on the one hand, and marketing techniques as well as trade secrets practices on the other.[207] Companies use legal terms and conditions with their users as shields to protect themselves from liability and as swords to continue to carry out objectionable practices. Companies whose business models rely heavily on data collection and analytics have an incentive to use vague, unspecific, and non-threatening language in their terms of service. This is unsurprising in light of the losses they would suffer if their users decided not to opt into these services because of their contractual terms. Further, sophisticated processing techniques such as machine learning algorithms and the use of neural networks often evade explainability[208] and companies assert overbroad trade secrecy claims over these activities.

2. Consent is about Power

---

note 57.

201. CASS SUNSTEIN & RICHARD THALER, NUDGE 34 (2008).

202. *Id*. at 24.

203. *Id*. at 36.

204. Acquisti et. al., *supra* note 57, at 511.

205. DAN ARIELY, PREDICTABLY IRRATIONAL 240 (2008).

206. Acquisti et. al., *supra* note 57, at 510.

207. Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1 (2019).

208. *See, e.g.*, David Weinberger, *Optimization over Explanation - Maximizing the benefits of machine learning without sacrificing its intelligence*, MEDIUM (January 28, 2018), https://perma.cc/L92A-6QXZ.

While these barriers are important, it is reductive to see them as exhaustive justifications for resisting consent. As discussed in Part I of this Article, we must ensure not only that the subjective conditions for informed consent are fulfilled, but also that the background conditions within which consent operates are just. For example, Bill might have consented to giving his snack to John, but if John grabs the snack in the context of an ongoing abusive relationship, or if it normalizes abuse, then his act remains unjustified and consent has no transformative value. Focusing on skillfully drawn lists of conditions for voluntary consent and disclosure, suggests that by considering voluntariness and ensuring that disclosure is accurate, we can pass judgment on the appropriateness of notice and consent in the digital context.

This approach is reductive. Confining our reasons in this way fails to take into account the power dynamics that underlie the practice of consent. The problem is not only that individuals have no valid alternatives, or are unable to choose, or lack voluntariness or understanding, but that consent is being weaponized by powerful industry actors to forward their agenda. They do this by exaggerating the liberating force of consent for individuals, by idealizing its morally transformative value, and always resisting governmental interferences and downplaying alternative regulatory protections that would be largely more effective for users. It is only by situating the practice within this corporate strategy devised to avoid governments and exploit individuals that the actual value of consent can be uncovered. The approaches of the FTC and EU data protection authorities leave us perplexed because they are based on precisely this narrow checklist approach: focused on voluntariness and idealized consent. In doing so, these authorities gloss over deeper justice concerns and fail to account for the detrimental effects on those left behind.

B. Platform Power

Corporate manipulation of users cannot be addressed through a checklist or by focusing on implausible forms of voluntariness, disclosure, and informed consent. Our insatiable desire for platform harms and our gluttonous appetite for

manipulation seem to call for an explanation that moves past traditional checklist understandings of autonomy and coercion. Underlying the psychological, factual, strategic, and legal impossibilities described above is the question of how power is exercised in digital ecosystems. Therefore, instead of playing with the conditions for disclosure and informed consent, regulators should start focusing on how data is collected, handled, and stored. Additionally, they should focus on how it is being systematically analyzed through machine learning and other proprietary algorithmic systems to make inferences about individuals, pre-empt their tastes, and influence their decisions in view of making a profit.

What is power in this context? There are three views of platforms' power. The traditional view is illustrated by the understanding of market power in traditional antitrust law. Antitrust law defines market power as "*the ability of one or more firms to profitably increase prices, reduce output, choice or quality of goods and services, diminish innovation, or otherwise influence parameters of competition*"[209] or the ability "*to raise price, reduce output, diminish innovation, or otherwise harm customers as a result of diminished competitive constraints or incentives.*"[210] The traditional view is relational and is premised on direct causation: there must be an entity exercising power and it must exercise its power by using force, coercing or otherwise directly imposing harm on others. The harms must be tangible and observable, and include price increases or narrowly understood observable quality erosions. These parameters have largely missed the intangible erosion of fundamental rights standards in the platform economy.[211]

Recent events, such as the Cambridge Analytica scandal, have led to a broadening of regulators' interest in platform

209. Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings para. 8 (EC), 2004 O.J. (C 31/5) [hereinafter "Horizontal Merger Guidelines"].

210. Dep't of Justice & Fed. Trade Comm'n, *Horizontal Merger Guidelines* (Aug. 19, 2010), https://perma.cc/P2GY-3NSA. Yet note that there are plans to amend such Guidelines. *See* Charles McConnell, US FTC considers updating Horizontal Merger Guidelines, Global Competition Review (Sept. 19, 2019), https://perma.cc/XLU2-PPSR.

211. *See* Orla Lynskey, *Regulating 'Platform Power'*, 16 London Sch. Econ., Law, Society and Economy Working Papers 1/2017 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921021.

power. A new conception of platform power seems to have emerged as a result. An example is the German Bundeskartellamt's decision against Facebook.[212] The authority's belief that antitrust and privacy laws can work in tandem to hold powerful companies with vast pools of data in check is grounded in an idea of power as ownership and control over vast amounts of personal data. The ability of a company to control vast amounts of data is indeed being increasingly perceived as harmful for both users and competitors who are unable to compete on the market for that data. The Bundeskartellamt's understanding defeats the traditional logic of market power, and places the power asymmetry between users and platforms at the forefront of regulators' attention. Such view, however, is still premised on the need to re-establish users and competitors' control over data, and on the paramount value of control and user choice.

The third more radical view does not see platform power as a tangible force that is exercised linearly by one party over another to deprive the latter of control or choice over how data is being collected or used. It is a broader vision of power as a systemic force structurally embedded in the platform economy. This cannot be fixed through small regulatory tweaks or better disclosure, but requires a radical revision of the way platforms operate and sustain themselves economically.

This vision has been developed by Shoshana Zuboff through her work on "surveillance capitalism" as an evil that has grown systemically through banal business routine. She defines "surveillance capitalism's" effects as ones that "*cannot be reduced to or explained by technology or the bad intentions of bad people,* [but that] *are the consistent and predictable consequences of an internally consistent and successful logic of accumulation.*"[213] Julie Cohen is also critical of systemic domination.[214] Cohen envisions platforms as "*infrastructure-based strategies for introducing friction into networks*"[215] which operate "*with the goal of making clusters of transactions and relationships stickier—sticky enough to adhere to the platform*

212. BKA, Prohibition Decision *supra* note 106.

213. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 192 (2019).

214. COHEN, TRUTH AND POWER, *supra* note 154.

215. *Id.* at 40.

despite participants' theoretical ability to exit and look elsewhere for other intermediation options."[216] For her: "*[t]he platform economy rewrites all parts of* [the competition] *story reshaping the conditions of entry, the scope for disruption, and the sources of manifestation of economic power. Platforms do not simply enter markets, they replace (and rematerialize) them.*"[217]

This third view of platform power understands platforms as loci of domination and control which benefit from and leverage the centralizing effects of the networks they exist within, are coextensive with and participate in creating. It goes beyond the Bundeskartellamt understanding of power, beyond a view according to which one party exerts power by selecting the options or choices available to another. As Stephen Lukes compellingly articulates it, power is about shaping the very environment within which a chooser's preferences are formed.[218] For Lukes, the core characteristic of a power relation is not an observable exercise of influence or an observable reduction in the number of options available but rather the existence of a systematic interference with what those being dominated need or have reason to want. As he notes, numbing is the primary manifestation of grave forms of power:

> [I]s it not the supreme and most insidious exercise of power to prevent people, to whatever degree, from having grievances by shaping their perceptions, cognitions and preferences in such a way that they accept their role in the existing order of things, either because they can see it as natural and unchangeable, or because they value it as divinely ordained and beneficial?[219]

It seems relevant to an understanding of platform power, therefore, that the things we have reason to want to protect, such as privacy or access to information without manipulation or discrimination, are not being afforded to us through consent, and in fact that practices of notice and consent render protecting

216. *Id.* at 41.
217. *Id.* at 42.
218. LUKES, *supra* note 35.
219. *Id.* at 28.

these things more difficult. A Foucaultian understanding of power[220] can be particularly useful in explaining this discrepancy; how the rhetoric of consent operates against our interests, its particular internal logic and rhetorical force prevents enquiry into its disempowering effects.[221] In other words, notice and consent normalizes platform power, operating as a discourse of control which subtly burdens users with intractable governance responsibilities without empowering them. It acts as a free pass for corporate action.

C. The Value of Notice and Consent within a Theory of Platform Justice

Scanlon points out that it is generally "*a good thing for a person to have what will happen depend upon how he or she responds when presented with the alternatives under the right conditions*."[222] There are good reasons to be able to self-manage privacy: it gives one a sense of responsibility, security, control over aspects of the self. Before concluding we must consider the value of notice and consent once again and determine whether a comprehensive perspective makes us prefer consent to other alternatives.[223]

Thomas Scanlon's account of what he calls the "*Value of Choice*" offers some guidance on this question.[224] Choice can have *predictive* or *instrumental* value (e.g. choosing my own meal because I know what I will enjoy eating); *representative* or *demonstrative* value (e.g. it is important that *I* be the one choosing my present for my mother's birthday, even if I often buy things she dislikes); or *symbolic* value where there is stigma

220. Michel Foucault, POWER/KNOWLEDGE: SELECTED INTERVIEWS AND OTHER WRITINGS 1972-1977, (ed. Craig Gordon, 1980).

221. FOUCAULT, THE ARCHAEOLOGY OF KNOWLEDGE AND THE DISCOURSE ON LANGUAGE, *supra* note 15.

222. Thomas M. Scanlon, The Tanner Lectures on Human Values at Brasenose College, Oxford University: The Significance of Choice 177, 178 (May 18, 23, and 28, 1986) (transcript available from the University of Utah, Tanner Humanities Center, Lecture Library). *See also* a revised account in SCANLON, *supra* note 186.

223. SCANLON, *supra* note 186.

224. Thomas M. Scanlon, *The Significance of Choice: Tanner Lectures, Lecture 2*, at 177-201 (1986). Also see a revised account in WHAT WE OWE TO EACH OTHER ch. 6 (1998).

attached to my not making certain decisions myself which might make me look incompetent, immature, etc.. (e.g. in some cultures it is important that I should be the one choosing my life partner and not my parents). These three categories of reasons for valuing choice are not mutually exclusive. By way of analogy, there are instrumental and intrinsic reasons for valuing consent as a regulatory device in the platform economy and we cannot entirely separate intrinsic from instrumental reasons. Instrumental justifications focus on the benefits that consent can bring to individual consenters.[225] The most common instrumental justification for consent is that the individual has the best information to judge whether new rights should be created.[226] Non-instrumental or intrinsic justifications focus on consent as having value regardless of consequences. These reasons are generally grounded in an understanding of consent as allowing individuals to create their own moral law, pursue projects, and choose their own paths to flourishing. Let us examine possible reasons for maintaining the centrality of consent in the platform economy.

The first argument is that notice and consent are said to promote innovation and simplicity; it is seamless, versatile and is said to efficiently promote smooth business transitions avoiding excessive regulatory interference while ensuring their legitimacy.[227] Individuals are said to have the most knowledge on what they want and consent allows them to easily make choices. This argument advances a narrow understanding of innovation and an idealized view on the ability of individuals to police their own interests. As discussed, the amount of knowledge individuals possess in such situations is subject to debate and is far from complete. Further, deregulation and self-regulation happen to favor incumbents more than they favor new entrants or consumers.[228] This has become clear in the context of antitrust enforcement where the Chicago school belief in deregulation and permissionless innovation[229] is being

225. *See, e.g.*, THOMAS HOBBES, LEVIATHAN (1651); JOHN LOCKE, SECOND TREATISE OF GOVERNMENT (1690).

226. RAZ, *supra* note 21, at 85.

227. *See, e.g.*, Erika J. Nash, *Notice and Consent: A Healthy Balance Between Privacy and Innovation for Wearables*, 33 BYU J. PUB. L. 197 (2018).

228. Yochai Benkler, *Don't Let industry write the Rules for AI*, 569 NATURE 161 (2019).

229. Richard A. Posner, *The Chicago School of Antitrust Analysis*, 127 U.

reconsidered and top down antitrust enforcement in digital matters is reacquiring popularity.[230] The FTC's new Facebook decision, discussed above, is another demonstration of the current regulatory trend.[231] Further, the ideology of innovation is far from flawless.[232]

The second argument is that notice and consent advances users' data security. Competition over security avoids the erosion of standards which might result from a state monopoly over technology. It also limits governmental interferences into users' lives by allowing private companies to handle data. This argument ignores that consent incentivizes the creation and storage of data, and that the more data is generated, the higher the security risks. Thus, insofar as notice and consent contributes to data generation, it increases instead of reducing risks for individuals.[233] Further, we know that the data stored by the industry is not immune from governmental access.[234]

The third argument is that notice and consent allow individuals to obtain access to desired services at no cost. The reality here is that consent does not allow individuals to obtain such services at no cost. Instead, consent subjects their access to a variety of covert, manipulative, and discriminatory treatments that do not serve their interests in the long run. Consent serves the interests of the platform owners and other data brokers and third-party data collectors but not the interests of users who are disempowered in the platform economy. Thus, none of these three good reasons for relying on consent seem

---

PA. L. REV. 925 (1978); ROBERT H. BORK, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF (1978).

230. *See, e.g.*, Lina Khan, Amazon's Antitrust Paradox, 126 YALE L. J. 710 (2017); Maurice Stucke, *Reconsidering Antitrust's Goals*, 53 B.C. L. REV. 551, 611 (2012); Maurice Stucke, *Should We Be Concerned About Data-opolies?* 2 GEO. L. TECH. REV. 275, 280 (2018); TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE (2018).

231. USA v. Facebook, Inc. , No. 91-cv-2184, 2019 WL 3318596 (D.D.C., July 24, 2019).

232. *See, e.g.*, Langdon Winner, *The Cult of Innovation: Its Colorful Myths and Rituals*, BLOG (June 12, 2017), https://perma.cc/M8MN-8Y6L.

233. *See, e.g.*, BRUCE SCHNEIER, DATA AND GOLIATH (2015).

234. Google reports in its Transparency Report that between January 1 and June 30 2018 it received more than 25.5 thousand government requests for individual users' information. S*ee Transparency Report: Government Requests to Remove Content*, Google https://transparencyreport.google.com/government-removals/overview?hl=en (last visited Nov. 22, 2019).

sufficient.

Looking now at the alternatives, while consent might have unique intrinsic value in that it ensures that individuals are at least symbolically informed of how they will be treated by platforms, it seems that replacing notice and consent with most alternatives would come at very little cost for individuals. For example, relying on representatives, cooperatives, or trustees could ensure access to desirable services on more acceptable terms thanks to the greater bargaining power of such representatives, trustees, or cooperatives vis-à-vis platforms.[235] Ensuring minimized collection and analytics, secure handling and storage of our data may be impossible for us to consent to directly due to trade secrecy, IP, and other proprietary arrangements. However, secure handling and storage may be possible through an intermediary, even if they acted outside the scope of our consent.[236] To the extent there is value in intermediation, it seems that the value of individualized consent is very limited.

Another alternative is the establishment of industry-wide privacy-protective interoperable standards which would promote the privacy interests of users even if they would not provide them with granular opportunities to make contextual choices. It also seems that granular and versatile opportunities to make choices can lead to more harm than good in an environment where our choices are highly sensitive to small design changes and nudging.

Overall, it seems that intrinsic and instrumental reasons for valuing consent go hand-in-hand. To the extent consent does not allow individuals to determine desirable outcomes for themselves, i.e. to the extent it has no instrumental value, it seems to also have no intrinsic value in the sense of affording to individuals respect or worth, other than perhaps mere symbolic or ideological value.

---

235. *See, e.g.*, Katrina Ligett & Kobbi Nissim, *Ground Rules and Goals for Data Co-ops* (2019) (unpublished manuscript); RADICALXCHANGE, https://radicalxchange.org (last visited Nov. 22, 2019) (showing the work currently carried out by Radicalxchange).

236. *See* COHEN, TRUTH AND POWER, *supra* note 154.

D. Clearing Doubts about Paternalism

Regarding consent's intrinsic value, it has been argued that it remains important for individuals to be directly notified or informed of what a platform intends to do with their data. Daniel Susser for example argues that notice maintains its value in spite of the flaws of notice and consent.[237] It might also be argued that it remains important that any intermediary, data cooperative, or trustee is directly entrusted by a data subject with a mandate to act on their behalf. Even if notice and disclosure remain incomplete, the symbolic or representative value attached to the notification and disclosure process might remain intact. The strength of this argument is that it might point us toward regulatory solutions that combine notice and consent with greater top down protections for individuals, but it does not suggest that the legal and regulatory status quo in the US or EU is satisfactory.

It is no doubt important to recognize the value of having the choice, of freely associating with others and of leading a life of one's own choosing. In this sense, accepting that consent's symbolic or representative value may give us reason to consider governance options that entail complementing the practice with additional safeguards is important. On the other hand, arguing that any and all interferences with choice are illegitimate and must pejoratively be understood as paternalistic is the wrong way of valuing choice.

To the extent a governance option is advanced on the ground that it avoids "paternalistic" interferences with individual choice, we should be inclined to resist such justifications. Scanlon offers a nuanced explanation of why this is:

> Legal restriction of people's freedom, "for their own good" is likely to seem justified where (a) people who make a certain choice are likely to suffer very serious loss; (b) the instrumental value of choice as a way of warding off this loss is, given the circumstances under which that choice would

237. Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't,* 9 J. INFO. POL. (2019).

> be exercised, seriously undermined; (c) the demonstrative value that would be lost by being deprived of this choice is minimal; and (d) the tendency to "make the wrong choice" under the circumstances in question is widely shared, so that no particular group is being held inferior in the argument for legal regulation. The pejorative ring of "paternalism" and the particular bitterness attaching to it stem from cases in which either the seriousness of the loss in question or the foolishness of the choice leading to it is a matter of controversy.[238]

Standard privacy terms of service are systematically skewed in favor of technology platforms that intentionally craft them to minimize disclosures and limit responsibility. There is a large and shared tendency to make the wrong choice, sign up to *phishy* websites and share data with unknown third parties by clicking "I agree," or simply accepting to browse the Internet and be tracked. Individuals who make those choices risk suffering serious loss. The instrumental value of consent as a way of limiting damage for individuals is limited at best. We have also seen that the case for the intrinsic value of consent is weak, and that alternatives such as delegation of consent to cooperatives or trusts are acceptable if not preferable to notice and consent.[239]

The purpose of this Article was not to advance alternatives to notice and consent, or explain how alternative decision-makers might be better placed than individuals to make decisions on data governance. The aim was simply to show that there are good reasons to depart from the centrality of individualized notice and consent in practice and in theory. Any political or regulatory authority, or group of individuals, charged with regulating personal data and shaping the relationship between platforms and individuals is likely to make mistakes. Yet, recognizing that alternative decision-makers are likely to make mistakes is different from saying that any decisions that

238. Scanlon, *supra* note 222, at 181.

239. *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

are not individually made are for that reason "paternalistic." Given the limitations of notice and consent as a practice, considering the role of these alternative decision-makers has become a priority. For the time being, it suffices to say that democratically determined standards and redlines regarding the generation, collection, storage and use of data need our focus more than notice and consent schemes do.

E. How to Regulate Platforms

Moving from consent to a broader perspective on how to regulate online platforms, the first question is what is regulation and how do we address the gaps that notice and consent practices have created and are leaving behind? A few points should be noted. First, the regulative power of law is to be found not only in public or regulatory laws, but also within less visible regimes such as private property and contractual arrangements.[240] Second, it is important to keep in mind that what we traditionally understand as laws are not the only force at play; technologies, or socio-technical artifacts, can constrain behavior even more than laws do. Laws in turn can act as technologies, entrenching technical defaults and reinforcing ideological interpretations of environmental constraints and affordances.[241] In 1998 Lawrence Lessig in his famous essay *The Laws of Cyberspace* dwelled on the idea,[242] that on the Internet, code shapes human behavior as much as laws, social norms and economic forces.[243] Regulators for Lessig have four "modalities" at their disposal— laws, norms, markets and code—and when it comes to the Internet, perhaps the most powerful modality is the use of code. Thus, legal and technological frameworks together shape our understanding of what platforms are and of the contexts in which notice and consent frameworks operate. Legal frameworks have transformed notice and consent into an

240. COHEN, TRUTH AND POWER, *supra* note 154 at 57.

241. Julie E. Cohen, *Affording Fundamental Rights: A Provocaton Inspired by Mireille Hildebrandt*, 4 CRITICAL ANALYSIS L. 1 (2017).

242. An idea arguably introduced by Joel Reidenberg, Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).

243. Lawrence Lessig, *The Laws of Cyberspace* (1998), https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf.

artifact that shapes digital expectations and generates resistance around cultural, legal, technological and commercial alternatives.[244]

We are currently at a crossroads. A number of competing regulatory, technological, social, and economic models are being put forward to address the question of how to govern data and how to hold platform monopolies in check. In the United States, nationalization of technology platforms is unpopular,[245] but breaking up big tech and antitrust is not,[246] nor is regulating platforms as public utilities.[247] Internationalizing regulatory standards is becoming a priority.[248] Technological solutionism is on the rise with initiatives such as blockchain-based data monetization platforms or new modes of web interaction.[249] Economists are reinventing markets for data to markets for the provision of labor by individuals to platforms.[250] Scholars have proposed a variety of solutions to the data and platform regulation puzzle. To name a few, Jack Balkin suggested treating platforms as information fiduciaries.[251] Margot

244. *See* HILDEBRANDT, *supra* note 188.

245. Jack M. Balkin, *Fixing Social Media's Grand Bargain*, HOOVER WORKING GROUP ON NAT'L SECURITY, TECH., AND L.., AEGIS SERIES PAPER NO. 1814 (Oct. 16, 2018).

246. Elizabeth Warren, *Here's how we can break up Big Tech*, MEDIUM (Mar. 8, 2019), https://perma.cc/6ZZ4-TWLP.

247. *See id.;* Frank A. Pasquale, *Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines*, Seton Hall Pub. L. Res. Paper No. 1134159 (2008); Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. R. 1621 (2018); Kevin Werbach, *The Network Utility*, 60 DUKE L. J. 1761 (2011); Tom Wheeler, *Time to Fix It: Developing Rules for Internet Capitalism*, SHORENSTEIN CTR. PAPER SERIES (2018).

248. *See, e.g.*, DAVID KAYE, SPEECH POLICE: THE GLOBAL STRUGGLE TO GOVERN THE INTERNET (2019). (Kaye makes the case for the adoption by online platforms of international standards of free speech).

249. *See* DATUM, https://datum.org/ (last visited Nov. 23, 2019) (data storage and monetization through blockchain); Mary Jo Foley, *Microsoft is Privately Testing 'Bali,' a Way to Give Users Control of Data Collected About Them*, ZDNET.COM (Jan. 3, 2019, 2:54 PM), https://perma.cc/83DE-FNJA; OPIRIA & PDATA, https://opiria.io/ (last visited Nov. 23, 2019) (the European startup); REPAY.ME, https://www.repay.me/ (last visited Nov. 23, 2019) (German startup); SOLID, https://solid.inrupt.com/ (last visited Nov. 23, 2019); THE ENIGMA PROJECT, *The Enigma Data Marketplace is Live!* (Nov. 5, 2018), https://perma.cc/87P4-B3R6.

250. *See* ERIC A. POSNER & E. GLEN WEYL, RADICAL MARKETS: UPROOTING DEMOCRACY FOR A JUST SOCIETY ch. 5 (2018).

251. Balkin, *supra* note 239.

Kaminsky envisions a "*binary governance*" framework which combines a system of individual due process rights with private-public partnerships which she calls "collaborative governance," the GDPR being an instance of such model.[252] Julie Cohen has emphasized the importance of spaces immune from the control of platforms, what she calls "*semantic discontinuity*" and "*interstitial spaces for play*,"[253] and Shoshana Zuboff speaks of a "*right to sanctuary*."[254]

In the context of this laboratory, moving beyond notice and consent requires proceeding in at least three stages.

First, it is important to consider at the outset the history and context of the harms that need tackling and the interests which need to be protected. To do so, it is crucial to understand the history, anthropology and sociology of how we have come to where we are now, and why the notion of consent can appear normatively compelling and rhetorically powerful yet practically flawed in the context of consumer contracts and voluntary privacy policies.[255] This Article described some of the harms in question as invasions of privacy, manipulation, discrimination, bias, lack of due process, political polarization and echo chamber effects. We not only need a better understanding of these harms, but we also need richer analyses of how they connect to the broader, abstract, systemically-skewed platform ecosystem and the power dynamics that underlie it. Save in exceptional circumstances, we must be skeptical about "solutions" that present themselves as "fixes," yet denote utter disregard for the historical, sociological, psychological and ideological dimensions of power which has led to the problem itself. These "solutions" frequently do little more than recreate the same problems they were designed to address.

Second, we must remain critical toward answers to the platform governance problem that tend to put most or all the responsibility for protection from harm on individuals, and/or confer broad discretion, immunity and moral cover on deep

252. Margot Kaminsky, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529 (forthcoming 2019).

253. *NETWORKED SELF*, *supra* note 135.

254. SHOSHANA ZUBOFF, *supra* note 213.

255. *See e.g.*, Sandeep Vaheesan, *We Must End Rule By Contract*, CURRENT AFFAIRS (Aug. 19, 2019), https://perma.cc/DC44-WYVM.

pocketed and technically savvy companies for the sake of protecting innovation. These suggestions are particularly problematic when they rely on the disclosure of complex information and connect broad responsibilities and consequences to implausible disclosures. Notice and consent is one such problematic solution. Other problematic solutions which must be resisted include: individualized data auctions, blockchain-based apps or other means to easily transfer data and monetize it which abstract individual choice from larger social dynamics.

Third and finally, when asking how to address data governance and the relationship between users and platforms, we must prefer comprehensive regulation that tackles structural harm. For instance, focusing on the notion of "data minimization" under the GDPR to narrow "fixes" that address legal questions in isolation.

The following is a list of strategies or developments that are welcome and in some cases should be further developed:

- The GDPR is an example of sectoral regulation which, although it focuses in our view too heavily on informed consent and privacy self-management, in fact contains a number of important shifts toward privacy protective defaults, and innovative provisions. Such privacy protection measures include: data protection by design,[256] data protection impact assessments,[257] and data minimization principles,[258] all of which require coordination between data controllers and privacy regulators, thus departing from individual control.
- The recent FTC Facebook investigation and five billion dollar fine, in spite of criticisms that the FTC did not go far enough, is a signal for the industry that privacy and behavioral advertising are no joking matter. It also provided an opportunity for FTC commissioners to demand greater enforcement powers, and to signal the need for federal privacy legislation.[259] In parallel, there

256. *Id.* at art. 25.
257. Gen. Data Protection Reg., *supra* note 8, at art. 35.
258. *Id.* at art. 5.
259. *See* Simons et al., *supra* note 82, at 6.

are signs that antitrust enforcement against technology companies is on the rise in the United States.[260]

- The Bundeskartellamt decision against *Facebook*,[261] in spite of its focus on informed consent, is also a welcome attempt at regulating technology platforms by reaching beyond disciplinary silos, and opting for a cross-sectoral and cross-disciplinary methodology that puts forward a new understanding of platform power. Further calls have been made recently for a unified approach to platform governance or the regulation of social media through a one-stop-shop. Each of these initiatives deserves individualized scrutiny.
- There have been calls for data fiduciaries, data trusts or intermediaries of various kinds that would act as buffers between users and platforms. While not all of these proposals are equally sound, recent work around data cooperatives seems to be heading in a promising direction.[262]
- Finally, if notice and consent is here to stay, which is a possibility, it is crucial that it be complemented with stringent standards of privacy compliance on the part of technology actors and that it does not remain a standalone means of governing privacy. The California Consumer Privacy Act is a very timid move toward greater empowerment of users vis-à-vis companies, which entrenches notice and consent and does not appear to go far enough. A number of Federal Proposals are also similarly removing the voluntary element in notice and choice practices in the United States. The American Law Institute's Restatement on Consumer Contracts have attempted to establish protections for consumers who opt-in to browserwrap contracts because of behavioral

260. Kiran Stacey, *Kadhim Shubber and Hannah Murphy, Which Antitrust Investigations Should Big Tech Be Most Worries About?*, FINANCIAL TIMES (October 28, 2019).

261. BKA, Federal Cartel Office (June 2, 2019) B6-22/16 (Ger.), https://perma.cc/D8PK-D82G (Prohibition Decision: Facebook Inc. i.a. - The use of abusive business terms pursuant to Section 19 (1) GWB).

262. *TRUTH AND POWER*, *supra* note 154.

biases and information asymmetries in this space.[263] More protections will be needed in future for addressing the power gaps between users and platforms, but arguably none of these protections can tackle the serious underlying problems explored in this Article.

VI. Conclusion

Loose reliance on the binary presence or absence of voluntary consent and disclosure has allowed online platforms such as YouTube, Facebook, and Twitter to engage unhindered in opaque and intrusive targeted advertising practices, profiling, and other profit-making activities that have not clearly benefited consumers and that actually covertly harm them.

Consent enables the moral transformation of the relationship between persons in a variety of circumstances, but access to information platforms does not seem one of them. As said, justifying the morally transformative force of consent in any context requires at least three elements. First, consent cannot be used to transform rights and interests that are inalienable. Second, consent must not have far-reaching effects on third parties. Third, consent must not only be voluntary and a self-directed act of the will, but it must also be given under just background conditions, meaning that we need to consider the underlying power dynamics that affect whether a person's reasons for consenting are justifiable.

In the platform economy, all three elements are missing. Regulators and legal authorities focus on the voluntariness of consent and the adequacy of companies' disclosure idealizes the practice in circumstances where it cannot have morally transformative effects. Notice and consent frameworks place the burden of data governance on individuals who are not in a position to make individualized decisions about how data is treated. They not only impose harms on people who never consented to the practices themselves, but also subordinate our core inalienable right to be protected against manipulative, discriminatory and harmful digital practices, and to the economic interests of the platforms. The idealization of such

263. RESTATEMENT OF CONSUMER CONTRACTS (Am. Law Inst., Tentative Draft 2019), https://perma.cc/9QNR-ZJGR.

practice has also had the effect of reducing the interest and appetite of administrative agencies, legislators, civil society and consumers for more adequate alternatives.

There are, therefore, many reasons to object to the centrality of notice and consent mechanisms in the United States and Europe. The time is now ripe to look beyond existing paradigms of individual control and to grapple with the core structure of corporate surveillance markets and incentives. Emerging legislative proposals at the federal level in the United States are hints that the winds might be changing, but more needs to be done not only legally but also ideologically, socially, and economically. A number of technological, political, and legal avenues for enacting change and ensuring better protection for consumers exist and deserve further attention. The longer we fail to acknowledge consent's irrelevance to data governance in the platform economy, the longer we will deny ourselves respect and protection from the ever-growing expansion of digital markets into our lives.