Loyola of Los Angeles
Entertainment Law Review

Volume 41 | Number 3 Article 2

5-16-2021

Privacy As a Collective Norm

John Shaeffer
Fox Rothschild

Charlie Nelson Keever
University of San Francisco School of Law's Racial Justice Clinic

Privacy As a Collective Norm

Cover Page Footnote

John Shaeffer is a partner at the firm Fox Rothschild. The views he expresses herein are his own. Charlie Nelson Keever is a Staff Attorney at the University of San Francisco School of Law's Racial Justice Clinic. She is a proud alumna of Loyola Law School of Los Angeles where she served as editor-in-chief of the Loyola of Los Angeles International and Comparative Law Review.

PRIVACY AS A COLLECTIVE NORM

John Shaeffer and Charlie Nelson Keever[*]

As the economic value of aggregating personal data has grown, so too have concerns over the economic power "owning" such data gives to those who collect it. Existing legal regimes governing data privacy have struggled to strike a balance between protecting personal privacy and preserving the economic efficiencies that can be gained by permitting the collection and exploitation of personal data. This Article proposes a collective re-conceptualization of one subset of personal data: information about what we do, say, and like. This data has little value in isolation—it only becomes valuable when combined with the information about what *others* do, say, and like. When so combined, this "big data" should be viewed, not as personal property, but as a collective norm. Those who collect this data deserve compensation in exchange for the economic efficiencies that its collection provides; but complete and unlimited ownership of that data—the result of the existing "private property" framework—is too rich. The Article explains how we arrived at the existing legal regime governing data privacy, evaluates existing structures to explain why they do not and cannot work, and argues that a reconceptualization of privacy makes sense economically, culturally, and morally. This Article concludes by suggesting a regulatory structure that might better serve all interested parties when privacy is considered as a collective norm.

[*]John Shaeffer is a partner at the firm Fox Rothschild. The views he expresses herein are his own. Charlie Nelson Keever is a Staff Attorney at the University of San Francisco School of Law's Racial Justice Clinic. She is a proud alumna of Loyola Law School of Los Angeles where she served as editor-in-chief of the *Loyola of Los Angeles International and Comparative Law Review.*

I. INTRODUCTION

The United States built its privacy protection scheme on the notion that privacy is property. Privacy is thus subject to an individual's own decision-making authority. As personal property, when an individual transacts to receive something in exchange for information about what they do, say, or like, what is transferred becomes the property of its acquirer. The acquirer, as the property's new owner, is thereafter free to exploit whatever economic advantage it can derive therefrom and exclude its use by others. Treating the information that entities like Google, Facebook, or Amazon acquire in exchange for our use of their services—information reflecting what we do, say, and like—as *their* property to exploit has created an insurmountable barrier to competition against them.[1] A barrier never anticipated, and consequently not accounted for, by our existing competition and privacy laws.[2]

It is now beyond question that data concerning what we collectively do, say, and like has cultural significance and economic value. What remains difficult is determining precisely what is private and what is public in various contexts. The existing privacy regime effectively cedes to private, for-profit corporations the norms surrounding the balance of the economic and social benefits of the broad collection of what we do, say, and like against the detriments of this practice. Not only is this system ineffectual for its purpose, it is also anti-egalitarian, placing the burdens on those less privileged and allowing the privileged to reap more of the benefits.[3]

This Article proposes a shift in our mindset. What we do, say, and like is our collective contribution to the society in which we live. It is something distinct from what we internally think, feel, and believe, as well as that which fits within more traditional notions of privacy like our physical spaces, physical possessions, or sensitive information like our bank account number or medical information.

Since societies began, its members have made social contributions to their communities by doing, saying, and liking—expressing publicly what they privately thought, felt, and believed. We in the United States like

---

1. Brian Fung, *'Near-perfect market intelligence': Why a House Report Says Big Tech Monopolies are Uniquely Powerful*, CNN (Oct. 10, 2020, 8:51 AM), https://www.cnn.com/2020/10/10/tech/apple-amazon-facebook-amazon-monopoly-data/index.html [https://perma.cc/A7RY-FQZC].

2. *See, e.g.,* Ali M. Al-Khouri, *Data Ownership: Who Owns 'My Data'?*, 2 INT'L J. MGMT. & INFO. TECH. 1, 4 (2012).

3. *See id.* at 4–5.

hamburgers, listen to Taylor Swift, and elected Donald Trump as president. For better or worse, all of these things we do, say, and like become who we are. Collectively, they identify us as a society and form the basis of how we conceive of ourselves, how other societies see us today, and how historians will view us in the future.

Accepting that what we do, say, and like is both economically and culturally valuable, those who develop the tools to gather our collective contributions—phones, applications, search engines—*should* be rewarded with some measure of control and compensation. But should that reward be ultimate ownership? Should entities like Google, Facebook, or Amazon be the arbiters for the contextual demarcation of various categories of "private" data and its uses? Recognizing that such "ownership" comes with tremendous responsibility (much of which manifests in contentious litigation or adverse press), private entities now ask for rational regulation.[4] Unfortunately, even they have been unable to articulate what could be a rational approach. This Article suggests that by re-conceptualizing a subset of privacy—what we do, say, and like—as a public norm rather than individual property, a path to rational regulation can become clear.

What would a regulatory scheme look like if we re-characterized what we say, do and like as a *collective* norm rather than as an individual's property? While those who salvage this data obviously deserve compensation, nothing suggests such compensation should be *exclusive* control. Instead, not only should collective norms govern the scope of any compensation, but collective norms should be the stewards of this collective asset, demarcating what is public from what is private, and determining the uses of that which is deemed public. This determination would be similar to that made by regulatory entities like the Federal Communications Commission. Common sense suggests that a public agency accountable to the people is better positioned to identify the contextual norm for the demarcation of social versus private data.

To support this premise, this Article first defines the precise types of privacy, data, and information that it is concerned with, including so-called "Big Data." Parts III and IV discuss the legal and economic history of

4. The corporations who have most benefited from access to digital data in the form of what consumers do, say, and like no longer want the burden of authority over the data they purportedly now own. They have called for some yet-to-be-defined rational regulation, while rejecting the existing schemes, which they view as undermining the economic and social value of being able to know what we say, do, and like. Mike Isaac, *Mark Zuckerberg's Call to Regulate Facebook, Explained*, N.Y. TIMES (Mar. 30, 2019), https://www.nytimes.com/2019/03/30/technology/mark-zuckerberg-facebook-regulation-explained.html [https://perma.cc/3LBX-PVY7].

protecting a demarcation between "private" and "public" in the United States, including how initial efforts to protect privacy in the digital age and various protection schemes were influenced by historic notions of privacy in particular societies. Part V traces the proliferation of digital data collection and the economic value of what we do, say, and like. Part VI discusses the many pitfalls of an individualist approach to privacy regulation. Parts VII and VIII propose an alternative formulation of privacy, including characterizing certain personal information as a public good or as a common. Finally, Part IX suggests the broad strokes of a regulatory scheme that might better serve all interested parties when privacy is viewed as a collective norm.

With this foundation, we can begin to formulate and propose a regulatory scheme that can maximize the social, cultural, and economic value of what we do, say, and like that is consistent with prevailing norms. By reconceptualizing what we do, say, and like as a public norm to which we all contribute, we can build a better mechanism for establishing a contextual public/private demarcation that maximizes the social and economic value of our contribution while affirming the notion that there are things we simply do not want shared publicly.

II. DEFINING TERMS AND SCOPE: PRIVACY, DATA, AND INFORMATION

Parameters around three terms will drive this analysis: *privacy*, *data*, and *information*. Privacy will be discussed first, with data and information to follow. This section then concludes by considering the value of and myths surrounding large and dynamic collections of information known as "Big Data."

A. The Privacy We Are Concerned with Here

"Privacy remains operationally a 'fuzzy concept': there is no broad consensus on what exactly privacy is, and consequently on what a right to privacy should protect."[5] The German philosopher Jurgen Habermas's model for modern society is helpful. It demarcates our "lifeworld" as being "made up of the private sphere (family, private households, intimacy) and the public sphere (communicative networks that enable private persons to take part in culture and the formation of public opinion)."[6] This idea builds

5. Lanah Kammourieh et al., *Group Privacy in the Age of Big Data*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 37, 44 (Linnet Taylor et. al. eds., 2017).

6. Christian Fuchs, *Towards An Alternative Concept of Privacy*, 9 J. INFO., COMM., & ETHICS SOCIETY 220, 221 (2011). "In the words of *Vita Activa*, 'a life spent entirely in public, in

on Kant's explanation of his Enlightenment philosophy, which affords the individual a free space for thought, but expects that such thought will be contributed to society for its betterment.[7]

The U.S. has historically emphasized protecting the individual's free space, defining privacy as a negative right: the right to exclude.[8] The European formulation, the right to dignity, is a positive right, focusing on what the individual chooses to present or contribute to society, i.e., how they choose to take part in the culture and formation of public opinion.[9] These distinct formulations address different privacy problems of equal importance on both sides of the Atlantic. On one side are data security experts responsible for privacy-enhancing technologies. They focus on data processing and use. They are particularly sensitive to securing data from unknown third parties, an approach commonly referred to as "institutional privacy."[10] On the other side are those concerned with harm experienced when "technologically mediated communications disrupt social boundaries," referred to as social privacy.[11] Stated more simply, the focus is on when technology captures what we do, say, or like in both our private sphere and our social sphere. The focus of this Article is on *social* privacy.

---

the presence of others, becomes, as we would say, shallow.'" Ugo Pagallo, *The Group, the Private, and the Individual: A New Level of Data Protection?*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 159, 164 (Linnet Taylor et al. eds., 2017).

7. *Towards An Alternative Concept of Privacy*, *supra* note 6, at 230. "Privacy is in modern societies an ideal rooted in the Enlightenment. The rise of capitalism resulted in the idea that the private sphere should be separated from the public sphere and not accessible for the public and that therefore autonomy and anonymity of the individual is needed in the private sphere. The rise of the idea of privacy in modern society is connected to the rise of the central ideal of the freedom of private ownership. Private ownership is the idea that humans have the right to own as much wealth as they want, as long as it is inherited or acquired through individual achievements." *Id.*

8. Linnet Taylor et. al, *Introduction: A New Perspective on Privacy*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 1, 10 (Linnet Taylor et al. eds., 2017). "[T]he right to privacy is primarily conceived as a negative right, which protects a person's right to be let alone, while personality rights also include a person's right to represent themselves in a public context and develop their identity and personality."

9. Yola Georgiadou et al., *Location Privacy in the Wake of the GDPR*, 8 ISPRS INT'L. J. GEO-INFO. 157, 2 (2019) ("We distinguish between privacy as a negative right (freedom from interference) and privacy as a positive right (freedom to control)").

10. Ralf De Wolf et al., *Self-Reflection on Privacy Research in Social Networking Sites*, 36 BEHAV. & INFO. TECH. 459, 2 (2016).

11. *Id.*

The controversies and difficulties social privacy presents arise not from the acknowledgement that a demarcation between private and social exists, but instead the characterization of what fits within each category, and at what point the individual should lose any privacy claim to what reaches the public sphere. While Eric Schmidt, the former CEO of Google and Alphabet, notoriously once told an interviewer: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place,"[12] accepted norms do extend legitimate claims of privacy well into the public sphere.[13] To be clear, our interest here is not with the protection against the invasion of private matter such as the thoughts or intimacies shared only within the closest social relationships like families or romantic partnerships, but instead our right to control the elements of our identity that make us social beings (generally, what we do, say, and like). This type of privacy "may aptly be described not only as contextually appropriate information flow, but also as governance of personal information."[14]

Interest in privacy has existed now for well over 250 years.[15] What has changed is that we can now retain activity/data that was once lost or inaccessible due to the inability to collect, store, and retrieve the information in an efficient manner in an analog world.[16] While this change is fundamental, it is foolhardy to consider privacy anew. We cannot expect to view this new paradigm free from the bias of our past. In fact, anti-skepticism is the rational explanation for why both the United States and Europe cling to notions of privacy as an *individual* right, adequately addressed by informed consent, despite overwhelming evidence that this approach is unworkable.[17]

---

12. Haydar Jasem Mohammad, Google or Privacy, the Inevitable Trade-Off 12 (Sept. 2019) (unpublished Master's thesis, Arctic University of Norway) (on file with Arctic University of Norway) (quoting CNBC, *Google CEO Eric Schmidt on Privacy*, YOUTUBE (Dec. 8, 2009), https://www.youtube.com/watch?v=A6e7wfDHzew [https://perma.cc/FCZ9-9J9C]).

13. Benedict Rumbold & James Wilson, *Privacy Rights and Public Information*, 27 J. POL. PHIL. 3, 5 (2019) ("Even in public, norms governing . . . the 'appropriate flow of personal information' can still render certain activities violations of individuals' right to privacy.").

14. Madelyn Rose Sanfilippo et. al., *Governing Privacy in Knowledge Commons* (forthcoming Mar. 2021) (manuscript at 2) (on file with authors).

15. *See Towards An Alternative Concept of Privacy*, *supra* note 6, at 230 ("Privacy is in modern societies an ideal rooted in the Enlightenment.").

16. *See generally* Kammourieh et al., *supra* note 5, at 56.

17. ANNIKA RICHTERICH, THE BIG DATA AGENDA: DATA ETHICS AND CRITICAL DATA STUDIES 25 (2018) (Anti-scepticism "refers to the anti-Cartesian foundation of pragmatism: 'We have no alternative to beginning with the 'prejudices' that we possess when we begin doing

Consistent with the Coase Theorem,[18] we must "start our analysis with a situation approximating that which actually exists, to examine the effects of a proposed policy change and to attempt to decide whether the new situation would be, in total, better or worse than the original one. In this way, conclusions for policy would have some relevance to the actual situation."[19] It is simply wrong to conclude that strengthening privacy can do no harm.[20]

The analysis of social privacy is both economic and ethical.[21] Decisions about privacy are ethical in the pragmatic sense in that norms and values are being negotiated.[22] The level of concern over privacy varies widely with some seeking strong privacy regardless of the cost and others who are far less concerned.[23] Neither can be shown to be more objectively correct. There is no "right" answer. Rather, it is a process of negotiation and

---

philosophy . . . The prejudices 'are things which it does not occur to us can be questioned . . . Cartesian doubt 'will be a mere self-deception, and not real doubt'"); *see* Christopher Hookway, *American Pragmatism: Fallibilism and Cognitive Progress*, *in* EPISTEMOLOGY: THE KEY THINKERS 153, 155 (Stephen Hetherington ed., Continuum 1st ed. 2012).

18. Coase Theorem is a legal and economic theory developed by economist Ronald Coase that affirms that where there are complete competitive markets with no transaction costs, an efficient set of inputs and outputs to and from production-optimal distribution will be selected, regardless of how property rights are divided. Thayer Watkins, *Illustration of the Coase Theorem*, SAN JOSÉ ST. U. DEP'T OF ECON., https://www.sjsu.edu/faculty/watkins/coasetheorem.htm [https://perma.cc/BY2B-QZXA].

19. R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 43 (1960).

20. While "it is a typical American liberal belief that strengthening privacy can cause no harm[,] . . . privacy can undermine common goods (public safety, public health). That privacy is not automatically a positive value has also been reflected in criticism of privacy. Critics of the privacy concept argue that it promotes an individual agenda and possessive individualism that can harm the public/common good." *Towards An Alternative Concept of Privacy*, *supra* note 6, at 224.

21. The economics of privacy will be explored more below in the discussion on data. *See* discussion *infra* Part IV.

22. Richterich, *supra* note 17, at 4 ("Within a pragmatist framework, something is ethical because values and morals are being negotiated.").

23. "Some wish to share more about themselves, and some less." Dennis D. Hirsch, *Privacy, Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel*, 65 DUKE L.J. ONLINE 67, 67 (2016); Alessandro Acquisti et. al, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 446 (2016) ("[P]rivacy sensitivities and attitudes are subjective and idiosyncratic, because what constitutes sensitive information differs across individuals.").

renegotiation.[24] To paraphrase Slavoj Zizek, since we will not find the right approach, we must strive towards the least wrong approach.[25]

What informs this analysis is how we view our human relations in our society. Based on fieldwork performed in the 1950s, the social anthropologist Mary Douglas theorized four cultural poles—egalitarianism, hierarchy, individualism, and fatalism—with all cultures having some balance of all four.[26] How each approaches justice helps to elucidate their meaning: egalitarianism views justice as a just outcome for all; hierarchy views it as a rights-based process; to an individualist, it means "to each his due;" and a fatalist views justice as whatever power dictates.[27]

As noted above, the United States takes an individualist approach to privacy, allowing each individual to transact their privacy like a commodity but requiring informed consent. Europe's individualist approach is more hierarchical, requiring individuals to affirmatively opt into the collection of their data. A privacy fatalist sees no point in regulating personal information because any scheme will be breached. A privacy egalitarian, by contrast, considers the social: what policy is fair to all members of a society regardless of their technical sophistication.[28] While cultures with an individualist bent have a transactional view of privacy, an egalitarian culture would view what its members do, think, and say as part of the collective culture. A way to distinguish between an individualist approach and an egalitarian approach can be described "by the rallying cries 'my data belong to me, and I can use it for whatever purpose' vs. 'privacy is a human right, and its protection is in the public interest.'"[29]

---

24. Richterich, *supra* note 17, at 25 (Anti-foundationalism "between more or less reliable and well-grounded knowledge: in this sense, knowledge is not seen as universal and beyond eventual revision, but may be subject to reconsideration in light of future discoveries or developments.").

25. SLAVOJ ZIZEK, ABSOLUTE RECOIL: TOWARDS A NEW FOUNDATION OF DIALECTICAL MATERIALISM (reprt. 2015) (2014).

26. Georgiadou et al., *supra* note 9, at 10.

27. *Id.* at 10–11.

28. *Id.* at 10.

29. De Wolf et al., *supra* note 10, at 3.

Privacy, in all instances, is a relative right and not an absolute right.[30] This can be seen in Europe's codification of its right to privacy—"the right to respect for his private and family life, his home and his correspondence"—as set forth in Article 8 of the European Convention on Human Rights ("ECHR"), which expressly recognizes that privacy can be limited "in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[31] While like the United States' more narrowly drawn Fourth Amendment rights, Article 8 of the ECHR is expressly limited to actions by the state, the jurisprudence surrounding both suggests a shared contemporary public norm that one's right to privacy must be balanced with "security," "economic wellbeing of the country," and "protection of health or morals."[32] One should not, however, view this as a duality, as in the more privacy is protected, the more these more social values are compromised. Rather, each value represents different interests that any law or regulation should seek to optimize.[33] In other words, more privacy does not necessarily mean less security, and vice versa.[34] Similarly, Big Tech criticizes individualized informed consent regimes and, in particular, more onerous opt-in formulations, for failing to adequately consider their macro-economic harm in terms of lost efficiencies. While Big Tech has indicated a willingness to be regulated, in order to avoid the hammer these regulations impose on missteps, it has yet to find an acceptable balance within an individualized approach.[35] If a balance between

30. Pagallo, *supra* note 6, at 209.

31. Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence 7, 11 (2020) (Council of Eur: Eur. Ct. H.R.) https://www.echr.coe.int/documents/guide_art_8_eng.pdf [https://perma.cc/WAM5-WE9V].

32. *Id.* at 11.

33. "Antidualism stresses the need to refrain from predefined, taken-for-granted dichotomies." Richterich, *supra* note 17, at 25.

34. "The tension is sometimes presented as being asymmetric: between the *ethics* of privacy and the *politics* of security. In fact, it is ultimately ethical. Two moral duties need to be reconciled proactively: fostering human rights and improving human welfare." Luciano Floridi, *Group Privacy: A Defence and an Interpretation*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 83, 84 (Linnet Taylor et al. eds., 2017).

35. *See* Isaac, *supra* note 4.

competing norms is not achievable within the informed consent structure, maybe it is time to consider other paradigms.

Privacy is also contextual.[36] Most people would reasonably agree that what they tell their doctor is meaningfully different than what they post on Facebook. This difference, however, does not mean that individuals have no privacy interest whatsoever in what they post on Facebook. More rationally, it means that what works for one will not necessarily work for the other. "Contextual privacy is 'preserved when informational norms are respected and violated when informational norms are breached . . . . [W]hether or not control is appropriate depends on the context, the types of information, the subject, sender, and recipient.'"[37] Helen Nissenbaum, who receives much of the credit for exploring this subject, is recognized for making four key claims: "(1) privacy is appropriate flow of personal information; (2) flows conform with entrenched contextual informational norms; (3) contextual informational (privacy) norms refer to five independent parameters (subjects, senders, recipients, information types, and transmission principles); and (4) privacy is respected when an action conforms to legitimate, social and individual, norms."[38]

Significantly, the United States' approach to privacy has been contextual in that it developed in a sector-specific manner. "Laws such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Gramm-Leach-Bliley Act (GLBA) of 1999 cover data uses in narrow contexts, such as health and financial information respectively."[39] For instance, credit reporting is currently one of the most highly regulated sectors in the United States, tracing its lineage at the federal level to the Fair Credit Report Act of 1970 (FCRA).[40] Such legislation precludes financial

---

36. From an economic perspective, "[t]he value of keeping some personal information protected and the value of it being known are almost entirely context-dependent and contingent on essentially uncertain combinations of states of the world." Acquisti et. al., *supra* note 23, at 446. From a social view, "the right to privacy is properly understood as a right to 'contextual integrity' and what *this* amounts to 'varies from context to context.'" Rumbold, *supra* note 13, at 5.

37. Christian Fuchs, *The Political Economy of Privacy on Facebook*, 13 TELEVISION & NEW MEDIA 139, 142 (2012).

38. Sanfilippo et. al., *supra* note 14 (manuscript at 20).

39. MICHELLE DE MOOY, RETHINKING PRIVACY SELF-MANAGEMENT AND DATA SOVEREIGNTY IN THE AGE OF BIG DATA: CONSIDERATIONS FOR FUTURE POLICY REGIMES IN THE UNITED STATES AND EUROPEAN UNION 11 (2017).

40. Acquisti et. al, *supra* note 23, at 471.

institutions from discrimination based on personal attributes such as racial, ethnic, or other protected characteristics. However, "[t]echnological advancements have made [it] possible [now] for lending companies to mine online and offline data and make offers only to populations with credit attractiveness."[41] The disparate, sector-specific approach may be a boon for lawyers and consultants who have mastered the myriad of overlapping state and federal sector-specific approaches. As the availability of diverse data from diverse sources continues to expand, however, this sector-specific approach will become unmanageable in the absence of an omnibus solution under the auspices of a single authority well versed in privacy's contextual nature.

Finally, before considering what data/information is private, one must acknowledge the relational aspect to social privacy. "When two people—let's call them Alice and Bob—interact, and Alice learns something about Bob in the process, Bob may place his faith in Alice that she will not communicate these details to others. Bob's privacy depends, in part, on Alice's behavior: here, her willingness to abstain from speaking about their interactions."[42] Similarly, when Alice posts a picture of herself that captures Bob, she is disclosing information about Bob. Moreover, the mere fact that Bob associates with Alice discloses information about Bob. Thus, trust in some notion of privacy between Bob and Alice with respect to the information they share with each other, is undermined if they share that information across any sort of social network, including email, or simply in a public place. "[R]elational privacy recognizes that different privacy expectations attach to different people and institutions in our lives and suggests that law should take into account these different sensitivities in setting rules about such expectations (for example, by recognizing that we may have a greater interest in privacy against the government than we do against our neighbors)."[43] As will be developed below, it is largely this relational aspect to privacy that makes the current individualist approach based on informed consent so ill-conceived.

---

41. Nir Kshetri, *Big Data's Impact on Privacy, Security and Consumer Welfare*, 38 TELECOMMS. POL'Y 1134, 1148 (2014).

42. Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555, 556 (2020).

43. *Id.* at 560; Karen Levy et al., *Regulating Privacy in Public/Private Space: The Case of Nursing Home Monitoring Laws*, 26 ELDER L.J. 323, 327–29 (2019).

B. Data and Information

When we move away from privacy as a demarcation, the question becomes: What is it precisely that we want to keep private? Whether personal thoughts, credit card numbers, information about one's body, or simply personal information that one wishes to control with respect to one's social self, these are all things that can be expressed in words. As intangibles, each is distinct from our norm of protecting physical property as private, which we view as having its own unique economic value to our society in and of itself. To illustrate, there is a distinction between the value of my car, which has value independent of its connection to me, and my bank account number, which is a set of numbers with no value absent its connection to me. Unfortunately, this distinction is inevitably blurred by concepts like "intellectual property," which extends the protections we afford physical matter to things that exist in words or ideas. For example, trade dress protection is not concerned with the physical packaging itself, but with the inanimate attributes a configuration has in the minds of consumers. In the same way, copyright is not concerned with the physical manifestation of a creative endeavor, whether captured in a book, a painting or a sculpture, but the inanimate expression itself.[44] Put simply, if you steal a physical book or work of art, you have not committed copyright infringement.

Contemporary nomenclature conceives of "data" as that which can be expressed in words as opposed to physical matter.[45] Currently, data "refers to discrete, objective facts or observations about a person, event or situation that is unorganized, unprocessed and without specific meaning."[46] While

---

44. *Bobbs-Merrill Co. v. Straus*, 210 US 339, 347 (1908) ("'The copyright is an exclusive right to the multiplication of the copies, for the benefit of the author or his assigns, disconnected from the plate, or any other physical existence. It is an incorporeal right to print and publish the map'" (quoting *Stephens v. Cady*, 14 How. 528, 530 (1852)).

45. Curiously, "data" derives from the Latin plural of datum, meaning "that is given," which seems to relate only to certain readily apparent information, such as one's age, location, and race. This definition ignores what we do, say, and like; better characterized as our "achievements," which would be sublata in Latin. While we will discuss later how best to characterize data, some may suggest that "what is given" about ourselves (in other words, our attributes) are distinguishing characteristics like what the qualities that differentiate one piece of property from another. Such attributes, however, are aspects of *personhood,* which most societies distinguish from property in that one cannot sell oneself into slavery and most societies consider prostitution to be a crime. Richterich, *supra* note 17, at 4; Lauren Henry Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 TENN. L. REV. 863, 880 (2020).

46. Arjuna Dibley & Rachelle Cole, *Big Value from Big Data? Recognizing Public Value from Public Data in the Innovation Economy*, DIG. CITIZEN CONF., U. OF MELBOURNE 5 (2019).

data by itself has some value, its true value comes from its relation to other data, which is information. For example, the number of questions a student answers correctly on a test is data, but that piece of data only has meaning, or provides information, when compared to the performance of others on the same test.[47]

The EU's General Data Protection Regulation (GDPR) defines personal data as "any information relating to an identified or identifiable natural person."[48] Personal data can come in three forms: volunteered, that which one freely gives; observed; and inferred, that which is derived from relations with other data.[49] Such data can be spatial—including information from which a location can be determined—or not.[50] While securing raw data such as medical records and credit card numbers—the principal focus of institutional privacy—is no doubt valuable, it is clearly no longer sufficient to address all normative privacy concerns, as the passage of the GDPR demonstrates.[51]

Data, and the information derived therefrom, has always been of keen interest to governments, social scientists, economists, and those in the private sector.[52] Until recently, however, personal data has been a relatively scarce good "and [its] compilation was subject to controlled collection and deliberate analytical processes."[53] While the film *The Lives of Others* shows the great lengths the East German Stasi went to collect information on its citizens,[54] today only trust protects societies from becoming police states.[55]

---

47. *Id.* at 5–6.

48. Commission Regulation 2016/679, art. 4, 2016 O.J. (L 119) 33 (EU).

49. Georgiadou et. al., *supra* note 9, at 7.

50. *Id.*

51. Kammourieh et al., *supra* note 5, at 65.

52. "The history of the modern state, and the history of data are deeply intertwined. Data was, and remains, an important tool for the state to understand the public over which it has governing power, and for exercising that power." Dibley & Cole, *supra* note 46, at 2.

53. Richterich, *supra* note 17, at 4 (citing ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES AND THEIR CONSEQUENCES (2014)).

54. DAS LEBEN DER ANDEREN (Wiedemann & Berg et al. 2006).

55. "As Richard Clark (2014), a former presidential cyber security advisor and one of the authors of the American government's report reviewing the data collection and monitoring capabilities at the NSA, stated, 'we have created the potential of a police surveillance state.'" Quirine

What has changed is that what was once lost—essentially all personal data that members of past societies did not knowingly provide—is now relatively easy to collect, retain, and analyze. There are at least five steps to this complete "datafication"[56] of personal information: (1) digital data stored on networked computers; (2) consumer adoption of the internet; (3) the proliferation of smart phones; (4) the adoption of networked biometric sensors; and (5) the "internet of things," which includes home listening devices such as Amazon's Alexa or Ring, Apple's Home Pod, and Google's Home and Nest. "The spread of mobile computing and sensor technologies has blurred the distinctions between digital and physical, online and offline. All of this has led to services that simultaneously generate and capture digital trails of personal and professional activities—activities that were previously conducted in private and left little or no trace."[57]

This advance is viewed positively not only by techno adepts, "but also amongst scholars who see datafication as a revolutionary research opportunity to investigate human conduct."[58] "Traditionally, gathering population data has involved surveys conducted on the individual level with people who knew they were offering up personal information to the government. The census[, for example,] is carefully guarded by the public authorities, and misuse of its data is trackable and punishable."[59] Today, vast amounts of personal data, far beyond anything conceivable prior to the internet, is gathered, processed, and controlled by private corporations with still immature forms of public oversight.[60]

Eijkman, *Indiscriminate Bulk Data Interception and Group Privacy: Do Human Rights Organisations Retaliate Through Strategic Litigation?*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 151, 155 (Linnet Taylor et al. eds. 2017).

56. "Datafication refers to the quantification of social interactions and their transformation into digital data." Richterich, *supra* note 17, at 1.

57. Acquisti et. al., *supra* note 23, at 444.

58. José van Dijck, *Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology*, 12 SURVEILLANCE & SOC'Y 197, 198 (2014).

59. Linnet Taylor, *Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 24, 24 (Linnet Taylor et al. eds. 2017).

60. "Today's social media, search engines and the internet of things produce more data in only a brief period of time than were previously generated in all of human history." De Mooy, *supra* note 39, at 4.

C. The Value of Big Data and Its Limitations

"Big Data" refers not only to the collection of this data, but also its processing. Big Data has long been defined as "'high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.'"[61]

Big Data is less concerned with the linkage of data with an identified individual, in the way institutional privacy is, *e.g.*, securing the tie of a particular individual to a particular medical or financial record. Instead, Big Data is concerned with connecting traits and finding patterns. "By combining structured and unstructured data from multiple sources, firms can uncover hidden connections between seemingly unrelated pieces of data."[62] Simply put: "users of big data may not care about Alice at all, but only about the fact whether Alice, whoever she is, belongs to the group that regularly goes to the local church, or mosque, or synagogue, uses Grindr, or has gone to a hospital licensed to carry out abortions, or indeed shares [some other] feature of your choice."[63]

Through the use of particular algorithms, commonly referred to as Artificial Intelligence (AI) or machine learning, vast amounts of data are processed through computers to train the computers to identify patterns and links between data known about one person with another. "By extracting subsets from individual-level information or classes of similar individuals based on common habits and characteristics, technology can itself discover or "create" groups that may have consequences for members."[64] To illustrate, "Future Attribute Screening Technology (FAST) is a crime-prediction program developed by the Department of Homeland Security." "The purpose of the program is to 'rapidly identify suspicious behavior indicators to provide real-time decision support to security and law enforcement personnel'" by linking currently observed activity of a person or group with historic

---

61. Kshetri, *supra* note 41, at 1134 (quoting Definition of Big Data, GARTNER INFO. TECH. GLOSSARY, https://www.gartner.com/en/information-technology/glossary/big-data [https://perma.cc/NAU5-CPTF]).

62. *Id.* at 1146.

63. Jennifer Jiyoung Suh et al., *Distinguishing Group Privacy From Personal Privacy: The Effect of Group Inference Technologies on Privacy Perceptions and Behaviors*, 2 PROC. OF THE ACM ON HUM.-COMPUTER INTERACTION 1, 2 (2018).

64. *Id.* at 3.

data of other persons or groups.[65] Given that the value of Big Data comes from its ability to identify patterns and link traits to groups, to claim that security and privacy are protected simply by anonymizing that data seems rather shallow.[66]

One significant limitation of Big Data—among others—is that it is not neutral because not all members of a society contribute to the same extent. Data sets will be biased in favor of those less concerned about privacy who "have the necessary resources, plus the skills and an interest, to use certain digital devices and platforms. Although collected in immense quantities, [B]ig [D]ata may still represent [only] specific populations."[67] Big Data fails to capture both technologically sophisticated individuals who actively avoid contributing data, but also those who lack the means or skills to actively participate online. For example, Apple released its Research Kit in 2015, which it touted "as an efficient, effective possibility for recruiting study participants and collecting data."[68] This collection, however, is limited to Apple users who are already known to be a distinct demographic group, so much so that some online retailers know that they are typically willing to pay more for a service.[69]

The flaws of Big Data should not lead to the conclusion that we can ignore the economic or social harm in implementing legislation that undermines its value in the name of privacy. We must acknowledge that our existing preference for notice and consent schemes in the name of privacy protection can undermine the social and economic value of this data. To some, the fully informed consumer would share the views of strong privacy

---

65. Joshua A.T. Fairfield & Christopher Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 405 (2015) (quoting DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT 2 (2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf [https://perma.cc/UE3H-3CFE]).

66. With Big Data "the particular and the individual is no longer central . . . . Data is analysed on the basis of patterns and group profiles; the results are often used for general policies and applied on a large scale. The fact that the individual is no longer central, but incidental to these types of processes, challenges the very foundations of most currently existing legal, ethical and social practices and theories." Taylor et. al, *supra* note 8, at 13–14.

67. Richterich, *supra* note 17, at 46.

68. *Id.*

69. Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J. (Aug. 23, 2012, 6:07 PM), https://www.wsj.com/articles/SB10001424052702304458604577488822667325882 [https://perma.cc/EP4F-CWAW].

advocates and rationally decide that neither private corporations nor the government should know what they say, do, or like, beyond that which they explicitly direct towards those entities. If consumers were capable of comprehending the notices they receive, they would opt out of most data collection, destroying the value of Big Data.

Big Tech's concern with respect to the GDPR opt-in approach to consent is the belief that most consumers are relatively passive and if given the choice, they would prefer not to check a box regardless of its purpose. If too many were to decline to participate and refuse to contribute what they say, like, and do to Big Data, we would then return to the analog world of the last century (and likely suffer an economic recession due to the loss of efficiencies that Big Data has delivered).[70] This is surely not the case for those who subscribe to the belief that what Big Data has delivered is an illusion, but most would agree that Netflix knows better what we want to watch than the historic Nielsen system.[71] Many may not lament the destruction of Big Tech companies (those that exist because of Big Data) that a competent notice and choice system would likely cause, but if one agrees that knowing what we collectively say, do, and like has a macro economic and social value, a legislative scheme that "sticks it to Big Tech" becomes a societal self-inflicted wound.

By the same token, if there *is* societal value to data collected, societies are logically paying too much to its collectors by ceding the data collected to them as the collector's property alone. While a compelling argument can be made that the insights collectors or other users gain from the data collected own their insights, the data itself is society's and not the collector's property alone. The data is a collection of our shared activity, communication, and preferences.

---

70. Yan Carrière-Swallow and Vikram Haksar. *The Economics and Implications of Data An Integrated Perspective*, No. 10/16 INT. MONETARY FUND 1, 29 (2019) ("[A] push to tighten privacy regulations may be effective at protecting consumer rights but may generate unforeseen harm to efficiency and competition").

71. Timothy Havens, *Media Programming in an Era of Big Data*, 1.2 MEDIA INDUSTRIES J. 5, 7 (2014) ("The Netflix prize was built around improving what's known as a "collaborative filtering" algorithm, which uses such things as viewer ratings, history, and behavior to recommend content that *already exists* on the service." (emphasis in original)).

III. THE LEGAL AND ECONOMIC HISTORY OF PRIVACY IN THE UNITED STATES: A LEGAL REGIME FOUNDED IN INDIVIDUALISM

The prevailing attitudes towards privacy in Western societies—and the legal regimes derived therefrom—have their roots in the Enlightenment.[72] This is when philosophers challenged the public to emerge from immaturity and to rely on one's own understanding without the guidance of others.[73] Freedom was a prerequisite to achieving this goal, as men must be able to think freely, while still behaving obediently in civil society.[74] Such free-thinking men were not only "completely free" to pursue their thoughts, but were also "obliged to impart to the public all [their] carefully considered, well-intentioned thoughts."[75] This idea of personality separate and apart from society is a uniquely Western European one.[76]

Self-determination as championed by Enlightenment thinkers is the foundation of both America's Declaration of Independence and the French Revolution.[77] The focus of both historical efforts was to protect individuals from the State. Surprisingly, however, the word privacy appears nowhere in the U.S. Constitution. At best, the Fourth Amendment, adopted with this Constitution as part of the Bill of Rights, established a threshold for state

---

72. *Towards An Alternative Concept of Privacy*, *supra* note 6, at 230.

73. Immanuel Kant, *An Answer to the Question: "What is Enlightenment?"*, (Sept. 30, 1784), https://web.cn.edu/kwheeler/documents/What_is_Enlightenment.pdf [https://perma.cc/38T9-PMCB]. It is important to recall that these societies believed that such "enlightenment" would be pursued only by a privileged few since "[l]aziness and cowardice are the reasons why such a large proportion of men, even when nature has long emancipated them from alien guidance (*naturaliter maiorennes*), nevertheless gladly remain immature for life." *Id.*

74. *Id.*

75. *Id.*

76. It contrasts sharply, for example, with "Ubuntu, the famed African egalitarian culture, whose core definition is 'people are people through other people' [which] leaves little room for personal privacy." Georgiadou et al., *supra* note 9, at 13. Similarly, while China affords some protections for workers and consumers collectively from misuse of their data by companies, "[t]here are no comprehensive legal principles that protect privacy interests nor any effective definition of privacy exist in China and the general population of China have no knowledge of the concept of privacy." Mohammad, *supra* note 12, at 12–13 (citing Hao Wang, PROTECTING PRIVACY IN CHINA: A RESEARCH ON CHINA'S PRIVACY STANDARDS AND THE POSSIBILITY OF ESTABLISHING THE RIGHT TO PRIVACY AND THE INFORMATION PRIVACY PROTECTION LEGISLATION IN MODERN CHINA (2011)).

77. Kammourieh et al., *supra* note 5, at 54.

interference with private property. Its guarantee of an individual's right to private property free from interference is a foundational notion of liberty as defined in the U.S.

The connection between privacy and property was necessary for the nascent democracies founded in the late 18th century with capitalist economies to solidify and thrive. John Stuart Mill would later write about the value of private property to a successful economy. Specifically, "the right of each to his (or her) own faculties, to what he can produce by them, and to whatever he can get for them in a fair market: together with his right to give this to any other person if he chooses."[78] To Mill, privacy:

> [I]s a circle around every individual human being, which no government, be it that of one, of a few, or of the many, ought to be permitted to overstep: there is a part of the life of every person who has come to years of discretion, within which the individuality of that person ought to reign uncontrolled either by any other individual or by the public collectively.[79]

Much of our current thought about a right to privacy beyond personal property can be traced back to Samuel Warren and Louis Brandeis's 1890 article[80] written in response to the increasing intrusiveness of technology and the media. The authors recount how "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.'"[81] They found protecting individuals against invasion of their personal realm a "right of the individual to be let alone," which they labeled as a "'right to privacy'—the invasion of which [amounted to] a tort."[82]

---

78. JOHN STUART MILL, PRINCIPLES OF POLITICAL ECONOMY 200 (D. Appleton and Company ed. 1885).

79. *Towards An Alternative Concept of Privacy*, *supra* note 6, at 223.

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

81. *Id.* at 195.

82. Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 11–12 (2006).

Justice Brandeis would later expand on this idea, which he considered inherent in our jurisprudence, finding a constitutional foundation to the right to be left alone in the Fourth Amendment. In his view, this right not only prohibits physical trespass on one's private property, but more generally, protected against the "unjustifiable intrusion by the government upon the privacy of the individual."[83] According to Brandeis, "[t]he makers of our Constitution . . . . conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[84]

Recently, a sharply divided Supreme Court reaffirmed Justice Brandeis's expansive reading by explicitly recognizing that, while Fourth Amendment jurisprudence was "'tied to common-law[,]'"[85] "'property rights[, such rights] are not the sole measure of Fourth Amendment violations.'"[86] The Court recognized that "[w]hen an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' [the] . . . official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause."[87] While the Court reaffirmed that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,"[88] the mere fact that the information is in the possession of a third party alone is not determinative.[89] Finally, and relevant to our discussion here, the Court reaffirmed that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."[90]

---

83. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

84. *Id.*

85. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting United States v. Jones, 565 U.S. 400, 405 (2012)).

86. *Id.* (quoting Soldal v. Cook Cty., 506 U.S. 56, 64 (1992)).

87. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

88. *Id.* at 2216 (quoting *Smith*, 442 U.S. at 743–44).

89. *Id.* at 2217.

90. *Id.*

Outside the realm of the Fourth Amendment, the U.S. Supreme Court has, since 1965, recognized a constitutional right to privacy.[91] Specifically, in overturning state regulation of contraception, the Court found within the First Amendment's "freedom to associate" a penumbra protecting the "'privacy in one's associations.'"[92] Curiously, despite the tremendous focus on privacy recently, the general public's consensus that privacy is a shared norm, and the endless debate about the breadth of its protection under the federal Constitution, there has been little effort to codify this norm as a constitutional amendment.[93] By contrast, eleven states have explicitly recognized a right to privacy in their constitutions, many of which were enacted following *Griswold v. Connecticut*.[94]

While both the Fourth Amendment and the penumbra found within our right of association apply only to state actors, these articulations are evidence of a shared cultural norm. Bolstered by the foundational norm of private property, which is the cornerstone of Western capitalist society, this jurisprudence on privacy reflects a shared norm of privacy that reaches all facets of U.S. society. Significantly, as developed, this right to privacy is a negative right, the right to be left alone.[95] This contrasts with the European norm, rooted in the devastating experience of World War II, which focuses on protecting human dignity.[96] Both legal schemes, however, take as their focus the individual, the individual's property interest in their privacy, and both consider informed consent to be paramount.[97]

---

91. Griswold v. Connecticut, 381 U.S. 479, 483 (1965).

92. *Id.* (quoting NAACP v. Alabama, 357 U.S. 449, 462 (1958)).

93. One may surmise that this is largely due to this country's endless abortion debate.

94. *See Privacy Protections in State Constitutions*, NCSL (Oct. 6, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx [https://perma.cc/BNJ5-ZJBE]. The people of the State of California adopted their right to privacy in 1974, which reads, "All people are by 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." CAL. CONST. art. 1 § 1.

95. Taylor et. al, *supra* note 8, at 10.

96. Georgiadou et al., *supra* note 9, at 2; ALAN WESTIN, PRIVACY AND FREEDOM 40–41 (Ig pub. ed. 2015) (1967).

97. Fairfield & Engel, *supra* note 65, at 412.

A first articulation of a shared norm of privacy reaching all facets of the U.S. is found in the Fair Information Principles ("FIPs"), published by the U.S. Secretary's Advisory Committee on Automated Personal Data Systems in 1973.[98] FIP identifies legal guidelines for personal data compiled on computer systems. Five principles form its foundation:

> 1) [T]he existence of personal-data record-keeping systems should not be kept a secret; 2) people must have a way to find out what information about themselves is being stored and how it is being used; 3) people must have a way to prevent information about them obtained for one purpose from being used or made available for other purposes without their consent; 4) people must have a way to correct or amend records containing personally identifiable information; and 5) all organizations creating, maintaining, using or disseminating personally identifiable data must assure that the data is reliably being used as intended, and must take precautions to prevent misuse.[99]

The Privacy Act of 1974 was the first body of law to meet these standards.[100] It specifically governed the collection, use, maintenance, and dissemination of information held by federal agencies.[101] Significantly, despite dramatic changes in technology following its original adoption, most current U.S. and European regulatory schemes, including the EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), remain firmly rooted in FIPs.[102] The primary reason that FIPs fail is that the principles expect "individuals to monitor organizations in order to ensure that their information is accurate, complete, and used only for the purposes to which the individual has agreed."[103]

---

98. De Mooy, *supra* note 39, at 9 (citing U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973)).

99. *Id.*

100. *Id.* at 12.

101. *Id.*

102. *Id.* at 12–13.

103. Priscilla M. Regan, *Reviving the Public Trustee Concept and Applying It to Information Privacy Policy*, 76 MD. L. REV. 1025, 1027 (2017).

In addition to the individualist property approach to privacy that must have seemed a logical extension of Western society's preference for private property, regulatory inaction contributes to our current predicament. Beginning in 1927, the U.S. recognized the need to provide regulatory oversight over the public airway, which at the time was radio. Specifically, the Federal Radio Commission ("FRC") (the predecessor to the Federal Communications Commission ("FCC")) was established to ensure that those receiving broadcast licenses served "the public interest, convenience or necessity."[104] The idea was that:

> The public, with the government as its agent, would hand over—gratis—a license to use its airwaves to operate a radio station for a fixed period of time. In exchange, the lucky recipient of this extremely lucrative asset would operate the station as a trustee for the public that owned its spectrum.[105]

Specifically, "the broadcasting privilege will not be a right of selfishness. It will rest upon an assurance of public interest to be served."[106] Congress enacted the Communications Act of 1934 and replaced the FCR with the FCC, not only to correct deficiencies, but to broaden public powers over licensee conduct."[107]

By the 1980s, however, the FCC began to dismantle itself; first under the Carter administration with respect to radio broadcast,[108] and then under the Reagan administration with respect to television.[109] The consensus was that "consumer demand" was a sufficient check to ensure that broadcasters acted in the public's interest. Following this deregulation fervor, the Clinton administration took a hands-off approach to the infant internet.[110] In fact,

---

104. STEVE WALDMAN, THE INFORMATION NEEDS OF COMMUNITIES: THE CHANGING MEDIA LANDSCAPE IN A BROADBAND AGE 280 (2011).

105. *Id.*

106. *Id.*

107. *Id.* at 280–81.

108. *Id.* at 283–84

109. Regan, *supra* note 103, at 1025.

110. *Id.*

rather than simply relying on consumer preference, the administration enacted legislation and passed regulations to shield those playing in this arena from liability that would otherwise cripple non-digital competitors, be they broadcasters or retailers.[111] While the internet lacks the spectrum limitations of terrestrial broadcast media, and, as it developed, did not recognize national borders, the idea that public preference alone would serve as an adequate check now seems quaint and plainly naïve.

IV. THE ECONOMIC HISTORY OF PRIVACY

The progression of economic research on the issue of privacy and its impact on an economy is also helpful to understand where we are today. Building on the idea that individuals have a property interest in information they consider to be private, economists in the 1970s and 1980s began considering the impact of this property interest on the broader economy. Richard Posner, who is both a noted jurist as well as a respected economist, argued "that the protection of privacy creates inefficiencies in the marketplace, since it conceals potentially relevant information from other economic agents. For instance, if a job seeker misrepresents her background."[112] Based on this research, Judge Posner continues to believe that:

> [M]uch of what passes for the name of privacy is really just trying to conceal the disreputable parts of your conduct . . . Privacy is mainly about trying to improve your social and business opportunities by concealing the sorts of bad activities that would cause other people not to want to deal with you.[113]

George Stigler, sharing Judge Posner's view, concluded that regulation in the market for personal data was destined to be ineffectual "because individuals have an interest in publicly disclosing favorable information and hiding

111. Annemarie Bridy & Daphne Keller, *Comment Letter on U.S. Copyright Office's Second Notice of Inquiry regarding Section 512*, at 1 (March 31, 2016), https://ssrn.com/abstract=2757197 [https://perma.cc/TKQ2-PBF2].

112. Acquisti et. al, *supra* note 23, at 450.

113. Fairfield & Engel, *supra* note 65, at 416 (quoting Grant Goss, Judge: Give NSA Unlimited Access to Digital Data, PC WORLD (Dec. 4, 2014, 1:46 PM), http://www.pcworld.com/article/2855776/judge-give-nsa-unlimited-access-todigital-data.html [http://perma.cc/649V-9WTR]).

negative traits."[114] Both Posner and Stigler took what we would consider today to be a very narrow view of privacy.

Similarly, during this time before the advent of the internet and Big Data, economists also questioned the social value in the acquisition of personal data, finding, at best, "it results in a redistribution of wealth from ignorant to informed agents."[115] It was recognized, however, that certain forms of regulation could be socially *enhancing*. For example, privacy protections for health information enhance non-distorted disclosures.[116] So prior to the internet, the most favorable view of the economic value of privacy was mixed.

Research into the economics of privacy resurged in the 1990s, during the infancy of the public internet in the matter.[117] In particular, the advent of new low-cost technologies to collect and manipulate personal information would likely change the relationship between buyers and sellers. Research showed that consumers may suffer an economic cost if they chose to share less rather than more information about themselves online.[118] For this reason, a rational consumer would expect to receive a net benefit from a decision to share personal information even though they would have little understanding or control over how that information would later be used.[119] This conclusion spawned new markets for personal data.[120] At this time, however, markets seemed to have difficulty valuing personal data, and an empirical search began to determine the value of personal data as compared with

114. Acquisti et. al., *supra* note 23, at 450 (citing George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 623–44 (1980)).

115. *Id.* (citing Jack Hirshleifer, *The Private and Social Value of Information and the Reward to Incentive Activity*, 61 AM. ECON. REV. 561, 649–64 (1971)).

116. *Id.* at 451.

117. *Id.*

118. *Id.* at 452 (citing Hal R. Varian, *Economic Aspects of Personal Privacy*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (Barbara S. Wellbery ed., 1997), [https://perma.cc/47LR-8SC4]).

119. *Id.* at 452.

120. Acquisti et. al., *supra* note 23, at 452.

historical analog data.[121] Simply put, it was the comparative value of an internet eyeball measured by a click compared with an analog eyeball derived from a Nielsen rating or subscription data. It is curious that, during this time, advertising and subscription-based websites that tried to recreate the broadcast and cable television model online failed.[122]

At this time, economic researchers began to consider the question of who should hold the economic claim to the personal data collected.[123] While it was recognized that only regulation could answer this question, economically, its answer would tip the balance between the amount paid for access against the cost of protection.[124] The economic implications of changes to the cost of acquisition and the cost of protection remain a fruitful source of economic research.[125]

A third wave of economic research into privacy corresponds with the dawning of the 21st century as the internet entered its adolescence. Much of this focus is:

> [O]n issues surrounding privacy as the protection of information about a consumer's preferences or type (hence a significant number of models examine the relationships between privacy and dynamic pricing), different dimensions to privacy (and different dimensions of informational privacy) exist, and economic trade-

121. Matthew Crain, *A Critical Political Economy of Web Advertising History*, THE SAGE HANDBOOK OF WEB HISTORY 1, 7–11 (2019).

122. *Id.*; Evans, David S., *The Online Advertising Industry: Economics, Evolution, and Privacy*, J. ECON. PERSP. FORTHCOMING 1, 5 (2009) (available at SSRN: https://ssrn.com/abstract=1376607).

123. Acquisti et. al., *supra* note 23, at 452 (citing Eli M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997), https://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age [https://perma.cc/4F47-62QJ]).

124. *Id.*

125. *See, e.g.*, Rodrigo Montes et al., *The Value of Personal Information in Markets with Endogenous Privacy* (Toulouse Sch. of Econ., Working Paper No. 583, 2017), https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2015/wp_tse_583.pdf [https://perma.cc/3PNY-CR8W].

> offs can arise from different angles of the same privacy scenarios.[126]

At this time, Western economies experienced dramatic shifts. Transactions and activities that were once private due to the lack of cost-effective means to capture and compile their analog occurrence, had now moved online.[127] For the first time, economists witnessed the rise of huge corporations financed principally based on their control over both structured and unstructured data.

What drove revenues online was not targeted banner advertising of the type most akin to advertising on television and in print media, but instead the ability to target *products*, content, and price based on personal (and historically private) information about actual or potential consumers.[128] The digital economy quickly learned that online consumers did not trust what they considered online advertising, but appreciated what they perceived as the targeting of products, services, and content they wanted.[129] This discovery is the foundation of the monetization of personal and private data. Quickly, with this discovery, the economic power of online businesses funded by personal data surpassed that of businesses supported by traditional advertising (which only had the ability to target an audience of a particular demographic). Simply, data captured online had economic value far beyond ordinary advertising, and the granularity of what was now available digitally could never have been conceived in our historically analog world.[130] As a result, companies whose survival turned on outdated forms of advertising are now clearly in the decline.[131]

---

126. Acquisti et. al., *supra* note 23, at 454.

127. *Id.*

128. Crain, *supra* note 121, at 11–22.

129. *See* Acquisti et. al., *supra* note 23, at 466 ("Goldfarb and Tucker (2011a) find that obtrusive targeted ads—targeted in the sense that they are matched to the content of a website, and obtrusive in terms of visibility—are more likely to trigger privacy concerns among users in comparison to obtrusive but not targeted ads, or targeted but less obtrusive ads." Avi Goldfarb & Catherine Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 MARKETING SCI. 389, 389–404 (2011)).

130. De Mooy, *supra* note 39, at 17.

131. Evans, *supra* note 122, at 10 ("[O]nline advertising [is] a more efficient matchmaking vehicle for advertisers and viewers than offline advertising").

V. THE PROLIFERATION OF DIGITAL DATA COLLECTION AND THE ECONOMIC VALUE OF WHAT WE DO, SAY, AND LIKE

Knowing what societies, or their innumerable subgroups, do, say and like is incredibly valuable.[132] This value is both microeconomic—providing intelligence to the businesses that have it—and macroeconomic—promoting efficiencies to an economy as a whole by being able to deliver to a society what it wants.

Of all possible economic examples, the historic Nielsen rating system—the audience measurement system developed in the 1950s—is apt. Television historically presented something of an economic curiosity.[133] After purchasing a television set, consumption was free because the cost of production was borne by advertisers wanting access to its consumers. Additionally, the industry's product, a television show, has no objectively intrinsic value in the same way the performance of a BMW and a Hyundai can be compared. Instead, the value of a network television show is derived solely from consumer taste. While some would argue that a PBS broadcast of the Metropolitan Opera has more comparative cultural value, more American eyes will certainly be glued to the latest broadcast of *The Bachelor*. This makes *The Bachelor* much more economically valuable and likely more relevant to cultural norms in the U.S., whether we like it or not. An efficient market, therefore, became dependent upon knowing what consumers like. In the analog world of the 20th century, it was not possible to know what the hundreds of millions of households in the U.S. were watching at any given moment.[134] The Nielsen system became a surrogate for this data. It equipped approximately 10,000 homes throughout the country with a system that would record the viewing habits of a household and that data was then extrapolated out to the nation as a whole.[135] Hundreds of millions of advertising dollars were spent annually, predicated—and the fate of countless television shows rested—on what these few households chose to watch.

Until the 21st century, societies lacked other means to comprehensively collect these contributions and they were left with gross surrogate measures,

---

132. *Id.*

133. Shawndra Hill, *TV Audience Measurement with Big Data*, 2 BIG DATA 76, 76–77 (2014).

134. *Id*. at 77.

135. Robert Rußell et. al., *Monetizing Online Content: Digital Paywall Design and Configuration*, BUS. INFO. SYS. ENG. 62, 253–60 (2020).

such as polling or sales revenues.[136] This changed when computers, interconnected with each other, provided the means for retaining these expressions in the form of digital data. In its infancy, and through its early adolescence, the World Wide Web explored numerous alternatives for monetization. The first phase was the pay-for-a-portal model of America Online (AOL), which tried to containerize a user's entire online experience. Once access became a commodity, like the cable for your television, the private sector tried subscription models similar to newspapers or magazines. Consumers, however, equated being online to watching broadcast television, and were reluctant to pay for content when so much other content remained free.[137] Seizing upon the broadcast television analogy, online content and service providers next touted the eyeballs they could deliver to advertisers. Advertisers were not persuaded that an eyeball on the internet would lead to sales in the same way they believed eyes and ears connected with sales on television and radio. Innumerable ad-supported websites and internet marketing companies rose and fell during this tumultuous period.

Today, however, Big Data is touted as "'the world's most valuable resource.'"[138] Google contributed to this change. At the time it launched, Google was merely one of numerous search engines used to navigate the internet, with Yahoo being the prevailing leader. What distinguished Google, however, was that it wanted to be nothing more than a search engine. Google offered a place for search queries, and, at most, changed the graphic of its name. Google's simplicity contrasted sharply with its competitors. In order to be "sticky"—the buzzword of the time—Google's competitors filled themselves with loads of other content to hopefully keep users within their ecosystems.[139] These sites sought to monetize stickiness with untargeted banner ads to generate revenues. What Google understood, or discovered through sheer luck, is that most users wanted to be somewhere else and were looking for the fastest, easiest, and least obnoxious way of getting there. Rather than rely on the banner ads that cluttered other sites, Google sold the

136. Hill, *supra* note 129, at 77.

137. *See* Victor Pickard & Alex T. Williams, *Salvation or Folly? The Promises and Perils of Digital Paywalls*, 2 DIGITAL JOURNALISM 195, 200, 207 (2014).

138. Dibley & Cole, *supra* note 46, at 3.

139. Mohamed Khalifa et. al., *Online Consumer Stickiness: A Longitudinal Study*, 60 PACIS 856 (2001).

right to appear in relevant searches, meaning that users could purchase search terms (AdWord).[140]

As consumers preferred Google's model, not only did its search engine gain a competitive advantage, but it started to collect huge amounts of data about those using its service, linking searching histories to IP addresses and allowing the company to gain valuable information about those who used its service. Advertising with Google evolved from simply purchasing key words to the ability for Google to offer more robust socio-economic and demographic information to advertisers. This resulted in the development of targeted ads, which were seen as a win-win for consumers and sellers. The theory behind targeted ads was that "[t]o the extent that people can avoid seeing ads for things in which they have no interest, and instead see ads for things they might want to buy, everybody benefits."[141] "From this perspective, the online economic ecosystem is [seen as] a clear improvement over the earlier world of mass media, where a lot of advertising expenditure is wasted, precisely because it can't be targeted."[142]

This belief in the value of targeted advertising was overwhelmingly adopted by the private sector, spawning an entire industry around collecting information about consumers' perceived wants.[143] Digital ad spending for 2019 in the U.S. alone was $145.3 billion, increasing over 19% from 2018, and is triple what it was a decade ago.[144] Digital advertising now accounts for half of all advertising dollars spent in this country, with television in second place at 27.5%.[145] Virtually every connected business, from Facebook to a local grocery store or gas station, now collects data about their users and

---

140. *See Grow Your Business With Google Ads,* GOOGLE ADS (2021), *https*:// ads.google.com/home/#!/.

141. Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95, 135 (2019).

142. *Id.*

143. Fung, *supra* note 1.

144. *US Online Media Spend in 2019 and the Outlook for 2020*, MARKETING CHARTS (Feb. 5, 2020), https://www.marketingcharts.com/advertising-trends/spending-and-spenders-111801 [*https://perma.cc/F7GS-LCYH*]; Bradley Johnson, *Internet Media's Share of U.S. Ad Spending Has More Than Tripled Over the Past Decade*, ADAGE (Dec. 30, 2019), https://adage.com/article/year-end-lists-2019/internet-medias-share-us-ad-spending-has-more-tripled-over-past-decade/2221701 [https://perma.cc/L66D-7BF8].

145. Johnson, *supra* note 144.

most both sell and purchase such data from data aggregators.[146] Where historically, television and radio stations could provide you some rudimentary demographic information about their viewers and listeners, such as age, gender, and likely socio-economic status, content providers like Spotify today can provide advertisers with granular data based not only on the data they collect from their listeners, but also from other data aggregators.[147] With this data, Spotify can design unique and perhaps even previously unrecognized groups to meet a particular advertiser's need.[148]

The *actual* value of targeted advertising, however, is suspect. "[V]iewers click on less than 1% of ads displayed, and click-through rates even for ads on highly targeted services like Facebook and Twitter are in the range of 1 to 3%."[149] While targeted visual ads on websites that make use of Big Data are considered to be less obnoxious by consumers than untargeted banner ads, at least one study suggests these ads only generate twice the revenues per ad as a wholly untargeted ad.[150] Some cite privacy regulations permit consumers to opt out of data collection as a reason for the poor sell-through, arguing that ads are not as targeted as they otherwise could be. They similarly fear that newer opt-in schemes will further erode, if not destroy, the ad-supported internet.[151] Research suggests, however, that a more likely reason for poor sell-through is that "advertisers or data intermediaries—seldom possess socially optimal incentives to match consumers with products."[152] Aggregators realize that providing imperfect or incomplete data maximizes their ultimate returns. Despite concerns about low success rate, regardless

146. Kirsten Martin, *Data Aggregators, Consumer Data, and Responsibility Online: Who is Tracking Consumers Online and Should They Stop?*, 32 INFO. SOC'Y 1, 51–63 (2016).

147. Matteo Poletti, *Learning to Target Advertisements at Spotify*, KTH ROYAL INS. TECH. 1, 7 (2015).

148. "By extracting subsets from individual-level information or classes of similar individuals based on common habits and characteristics, technology can itself discover or 'create' groups that may have consequences for members." Suh et al., *supra* note 63, at 3.

149. Savage, *supra* note 141, at 105.

150. Acquisti et. al, *supra* note 23, at 464. For context, Google earns about one third of its revenues from AdSense, its service for targeting ads on websites, with the remaining two-thirds coming from search AdWord. *Id.* at 466.

151. *Id.* at 456; Savage, *supra* note 141, at 104–05.

152. Acquisti et. al., *supra* note 23, at 459.

of the reason, digital advertising remains viable because of its relative low cost and sheer scale.

In addition to the ability to target offers to potential consumers through advertising, Big Data enables the customization of products and the tailoring of prices to particular consumers.[153]

> For instance, if the price of a movie/music is outside a consumer's affordability range and if the supplier lacks the ability to price discriminate, the difference between the price the consumer is willing to pay and the marginal cost of a copy of the movie/music represents deadweight loss.[154]

Knowing a consumer's purchasing history or being able connect them to a group whose history is known, enables suppliers to manipulate price to affordability to overcome deadweight losses or to increase prices in order to recover optimal profits.[155] The economics concerns balance tradeoffs from protecting or sharing personal data.[156]

One thing that is clear is that the balance in any sales transaction has shifted. It is true that consumers have much more access to price and product information than they did previously, and are not as geographically constrained in their purchases as they once were. Sellers, however, not only know a lot more about each consumer individually—even in the case of new consumers—they also know a lot more than they used to about how people decide to buy, including their cognitive limitations biases.[157] This suggests that the actual merits of a product or service play a decreasing role in purchasing decisions.[158]

Recent economic research focuses on the impacts of varying privacy costs on effective price discrimination and the impacts of restrictions on the

153. Montes et al., *supra* note 125, at 32, 34.

154. Kshetri, *supra* note 41, at 1145.

155. *Id.*

156. Acquisti et. al., *supra* note 23, at 443.

157. Savage, *supra* note 141, at 142.

158. *Id.*

use and availability of data.[159] For example, research shows that "[a] prohibition on the collection, processing or commercial use of data would presumably increase the price of products and services for the consumers, with uncertain results that this solution would enhance the competition from rival firms," *i.e.*, price discrimination based on a customer's profile is likely economically positive to the economy as a whole.[160] Additionally, it has been shown that "[p]rice discrimination in the absence of universal transaction privacy leads to a welfare loss whenever the profiling of consumers is imperfect."[161] Stated more simply, "due to unavoidable errors in customer profiling, retailers will mistakenly quote high prices to some customers" above which they are willing to pay and vice versa, resulting in an overall loss of social welfare.[162] More troubling, however, is the fact that access to more data than a competitor can entrench monopolies, and data brokers maximize their economic benefit by not selling the same data to all rivals.[163]

While, on balance, Big Data bring efficiencies to the purchase and sale of products, it is far from the whole story of the economic, social, and cultural value that the collection, storage, and processing of what we say, do, and like has to a society. The availability of Big Data increases the efficiency of production processes and provides predictive insights into market trends.[164] In addition to enhancing economic efficiencies, the societal benefits of collecting and processing large amounts of personal information are numerous, including advancements in public health, education, welfare, and security.[165]

---

159. *See* Montes et al., *supra* note 125.

160. Andrea Giannaccari, *The Big Data Competition Story: Theoretical Approaches and the First Enforcement Cases* 3 (Eur. U. Inst. Dep't of L., Working Paper No. 10, 2018).

161. Rodney J. Garratt & Maarten R. C. van Oordt, *Privacy as a Public Good: A Case for Electronic Cash* 12 (Bank of Can., Staff Working Paper No. 24, 2019).

162. *Id.* at 32.

163. The data seller's profits are greater when it sells the full dataset to one firm only rather than selling an additional imperfect dataset to the other firm competing on the same market. Montes et al., *supra* note 125, at 30; Richterich, *supra* note 17, at 41.

164. Giannaccari, *supra* note 160, at 4.

165. De Mooy, *supra* note 39, at 24.

With the maturation of the digital economy, the collection, access, and control of Big Data resides with fewer and fewer private entities.[166] This Big Data divide is evident from the fact that Google, which remains the world's most used search engine, is now only the 25th most frequently visited website, and today's top ten websites account for 62% of all web traffic.[167] Consumers no longer need to search where they might want to go—they already know where they want to be. Similarly, most commercial websites are now hosted by Amazon's Amazon Web Services ("AWS") and most mobile data passes through Apple IOS or Google Android. These entities decide how data is fed into their algorithms that determine the content we subsequently see.[168] This content is not limited to advertisements, but also information posts they determine fit with our interests. These commercial websites use public concern over privacy to eschew efforts to develop methods for data-sharing, suggesting that others may not be as careful stewards of our personal data.[169] They know that:

> [C]onsumers are more likely to grant their opt-in consent to large networks with a broad scope, rather than to less established firms. Hence, if regulation focuses only on enforcing an opt-in approach, users may be less likely to try out services from less established firms and entrants, potentially creating barriers to entry.[170]
> This lack of data-sharing and roadblocks to nascent competitors' acquisition of personal data serves to undermine competition and further entrench their positions.[171]

---

166. "The phrase 'big data divide' emphasizes the tensions resulting from asymmetries in data access. It calls attention to the biased capacities for gaining insights into this material and assessing its implications. In addition, the term 'data monopolies' stresses that this divide not only characterizes customers' lack of agency, but the market dominance of very few internet and tech corporations." Richterich, *supra* note 17, at 41.

167. Joshua Hardwick, *Top 100 Most Visited Websites by Search Traffic (2021)*, AHREFS BLOG, https://ahrefs.com/blog/most-visited-websites/ [https://perma.cc/48L9-MT6J].

168. Richterich, *supra* note 17, at 1.

169. *Id.* at 40.

170. Acquisti et. al, *supra* note 23, at 456.

171. "[F]irms with market power often benefit from committing to privacy policies." *Id.*

In addition to the economic power this data gives those who control Big Data, their current "ownership" over Big Data enables them to influence scientific research reliant on this data. It is not uncommon for such research to either be conducted by persons employed by these entities or funded in whole or in part by them.[172] "The triple role of data collector, service provider and funding body is a defining feature of internet/tech corporations. It puts these stakeholders in a powerful position."[173] Today, these few entities get to "decide which societal actors may have access to data generated via their respective platforms, and define in what ways they are made available."[174] As noted in a 2017 report published by the Google Transparency Project, between 2005 and 2017, 329 research papers dealing with public policy issues in the interest of Google were funded by the corporation.[175] Similarly, "[o]nly Facebook has the data that can exactly reveal how fake news, hoaxes and misinformation spread, how much there is of it, who creates and who reads it, and how much influence it may have."[176]

Private entities that collect personal data as an exchange for some service, such as providing search results or access to a social media platform, have no economic interest in protecting user privacy. Instead, their interest rests in preserving trust. Virtually all human interactions rest on some modicum of trust as "trust is a transaction catalyst."[177] "The information economy[, whether it is providing a credit card with a transaction or interacting with a website,] is premised on the sharing of personal information; it is 'mediated by information relationships' to a far greater extent than prior economies."[178] We are told to be wary of "untrusted" sites, understanding that such sites may compromise data we wish to keep private. While the public tends to have a short memory, or is simply forgiving, as evident by consumers returning to Target after its big data breach, or to Facebook after its

172. Richterich, *supra* note 17, at 3.

173. *Id.* at 65.

174. *Id.* at 9.

175. *Id.* at 62.

176. Regan, *supra* note 103, at 1038 (citing Zeynep Tufekci, Opinion, *Mark Zuckerberg Is in Denial*, N.Y. TIMES (Nov. 15, 2016), https://www.nytimes.com/2016/11/15/opinion/mark-zuckerberg-is-in-denial.html [https://perma.cc/QY3R-54US]).

177. Savage, *supra* note 141, at 121.

178. Hirsch, *supra* note 23, at 83.

Cambridge Analytics fiasco, most believe that "if trust absorbs too many body blows, it can crash."[179] Simply, "online entities . . . are not competing to provide consumers with an optimal level of privacy; they are cooperating in an effort to ensure that the level of consumer trust doesn't sink so low that people stop coming online."[180]

VI. WHY AN INDIVIDUALIST APPROACH TO PRIVACY DOES NOT WORK

As discussed at length above, what falls within the concept of privacy is subject to debate, and there is really no shared definition.[181] At a minimum, privacy distinguishes what we choose to make part of our social self and what we separate therefrom. This demarcation is *contextual*.[182] That portion of our private thought, feeling and beliefs that we share—what we make social—with friends, neighbors, merchants, doctors, accountants, and lawyers, or simply the public at large in the form of a tweet or post, is likely very different in each instance.

The Enlightenment taught Western societies that an individual's private thoughts, beliefs, and desires have value.[183] This logically led to

---

179. *Id.* at 84.

180. Savage, *supra* note 141, at 98.

181. One reason for this may be that what we refer to as privacy in this context has little to do with what privacy actually means. Considering its entomology, "[t]he word private . . . comes from the L[atin] *privus* (perhaps from prce), existing for itself, single, by itself. In the old Latin it was synonymous with *singulus*. Then from *privus* was formed the verb *privo, privavi, privatum, privare*, to set free from anything, to separate from anything or any one." Thus, privacy is a demarcation and not a thing. JAMES MITCHELL, SIGNIFICANT ETYMOLOGY: OR ROOTS, STEMS, AND BRANCHES OF THE ENGLISH LANGUAGE 214 (William Blackwood & Sons, 1908).

182. *Towards An Alternative Concept of Privacy*, *supra* note 6, at 232 ("Helen Nissenbaum argues that one should go beyond the control theory and the access theory of privacy to consider privacy as contextual integrity. Contextual integrity is a heuristic that analyzes changes of information processes in specific contexts and flags departures from entrenched privacy practices as violations of contextual integrity. One then analyzes if these new practices have moral superiority and if the privacy violation is therefore morally legitimate"). HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 164, 182 (Stan. U. Press ed. 2010). Contextual privacy is "preserved when informational norms are respected and violated when informational norms are breached . . . . [W]hether or not control is appropriate depends on the context, the types of information, the subject, sender, and recipient." *Id.* at 140, 148.

183. Fairfield & Engel, *supra* note 65, at 406 ("Most dominant theories of privacy view it through the lens of individualism.").

conceptualizing what we deem "private" as property. This historic understanding of privacy as property has biased our approach to privacy in the digital age, extending its reach beyond the things we possess separate from society. Specifically, as "property," what is deemed private is a commodity that can be freely traded by individuals with informed consent.[184]

What is now clear, however, is that this approach rests on several false assumptions. First, it falsely assumes that, armed with adequate information, individuals can make rational choices. It is generally accepted that we cannot.[185] Second, it falsely assumes that an individual's personal privacy demarcations have meaning. They do not. As social beings, our personal privacy demarcation is dependent upon the privacy decisions of others, most notably our own family, friends, and acquaintances. Simply put, even if one sought maximum privacy, much of what one sought to protect could be penetrated by Big Data simply based on the more lenient privacy decisions of those with whom that person associates. Our current approach to protecting privacy is to anonymize what is collected and to require that its collection be subject to informed consent. This structure, however, simply does not work.

First, simply removing someone's name or address from data has become all but meaningless.[186] "This is due to three sea changes: the number of datasets that can be cross-referenced has grown; the data itself has become richer; and, as a result, the algorithms that succeeded in creating 'noise' in datasets to prevent re-identification are no longer effective."[187] For example, one study demonstrates "that 87 percent of the U.S. population can be uniquely identified just from zip code, gender, and date of birth."[188] Research also consistently shows that "[i]t is possible to use non-personal data

184. De Mooy, *supra* note 39, at 9 ("Regulatory regimes in the United States and Europe have taken a similar approach toward data protection since the 1970s, giving individuals the right to make decisions about how to manage their data.").

185. Jay Pil Choi et al., *Privacy and Personal Data Collection with Information Externalities*, 173 J. PUB. ECON. 113, 24 (2019) ("Currently, most countries' privacy regulation and law are based on 'informed consent' approach. This approach finds its justification on the premise that an individual's informed consent provides legitimacy for any information collection and its use. Despite its intuitive appeal, there has been wide criticism against such approach.").

186. "Anonymity is no longer central. As it becomes near-impossible, and maybe even irrelevant, we must rethink what we intend to protect when we speak of protecting privacy." Kammourieh et al., *supra* note 5, at 50.

187. *Id.* at 46.

188. Fairfield & Engel, *supra* note 65, at 390.

to make predictions of a sensitive nature such as sexual orientation and financial status."[189] Thus, while:

> U.S. federal regulations do not allow financial institutions to discriminate in the pricing of and access to credits based on personal attributes such as racial, ethnicity or other characteristics[, t]echnological advancements have made possible for lending companies to mine online and offline data and make offers only to populations with credit attractiveness.[190]

As mentioned above, the value of Big Data commercially, socially, and politically is not tying a piece of data to Alice, Bob, or Carol, but connecting them to a "type: a skier, a dog lover, a bank manager, [or] '[p]eople who bought this also bought [that].'"[191]

Big data exploits "homophily," the principle that people are likely to interact with others who are similar to them, meaning that "from people's communication networks we can identify their contacts' likely 'ethnicity, gender, income, political views and more.'"[192] "'Even if you are looking at purely anonymized data on the use of mobile phones, carriers could predict your age to within some cases plus or minus one year with over 70 percent accuracy. They can predict your gender with between 70 and 80 percent accuracy.'"[193] This is not to say we should completely dispense with the requirement that data be anonymized. Instead, "[i]n the age of Big Data and information inferred *ab extra*, the traditional right to informational privacy [, data anonymity,] no longer provides sufficient protection to the individual; it focuses solely on information collection rather than analysis, and can thus no longer be a fully effective instrument of control."[194] Stated more simply, while anonymity "may allow the individual to hide within the crowd, [it]

189. Kshetri, *supra* note 41, at 1140.

190. *Id.* at 1148.

191. Taylor et. al., *supra* note 8, at 10.

192. Taylor, *supra* note 59, at 17.

193. *Id.* at 17–18.

194. Kammourieh et al., *supra* note 5, at 46.

cannot conceal the crowd itself. We may be profiled in actionable ways without being personally identified."[195]

The addition of individualized informed consent is similarly insufficient in today's digital landscape. Informed consent has been the cornerstone of human research.[196] "This approach finds its justification on the premise that an individual's informed consent provides legitimacy for any information collection and its use."[197] Extending this principal to public and private transactions made sense when computing systems were mostly centralized and people "had little need to exercise their data-control rights on an ongoing basis."[198] The key premise is that individuals have some control over what information is collected about them and how it will be used.[199] This transactional approach—a bargained-for exchange—fits nicely with the historic notion of privacy being the personal property of an individual and, consistent with a capitalist system, that privacy should be something that each individual can exchange with limited governmental interference. This falls in line with "the general belief of economic liberalism that individual choice in markets will lead to the best global outcome."[200]

Most today, however, question the effectiveness of this approach.[201] Some suggest the problem is "that privacy notices are rarely read, and even if read, not easy to fully understand."[202] Simply educating users, however, yields diminishing returns.[203] This is because:

> [T]he idea that consumers can make meaningful choices about online privacy is practically a poster child for the behavioral economic critique of standard microeconomics. People aren't

195. Taylor, *supra* note 59, at 13–14.

196. Richterich, *supra* note 17, at 42.

197. Choi et al., *supra* note 185, at 24.

198. De Mooy, *supra* note 39, at 9.

199. Savage, *supra* note 141, at 106.

200. De Wolf et al., *supra* note 10, at 4.

201. Choi et al., *supra* note 185, at 24.

202. *Id.* at 24.

203. Fairfield & Engel, *supra* note 65, at 409.

> good at bargaining over complex, contingent, or uncertain future costs and benefits of the sort arising from online surveillance; no such bargaining occurs in fact; and it's not clear why rights in information arising from interactions between an individual and an online entity belong to the individual (to be bargained over) rather than the entity (to be exploited at will).[204]

"Most individuals understand neither the data stores they are helping to create nor the ways in which data analysts can use such information to produce actionable insights."[205] At best, "individual-centric regulatory structure[s give] modern users of digital technologies . . . [the] illusion of control through consent notices . . . [and] ad-preference" controls.[206]

There obviously exists a tradeoff between strong privacy protection and the economic and social benefits we as a society derive from Big Data. When asked, individuals usually state strong preferences for protecting privacy. Those same individuals, however, consistently fail to act in accordance with that preference, something commonly referred to as the privacy paradox.[207] True, there are some—likely well-educated and affluent—who are technologically adept and can make a rational decision here. Following known societal preferences, and in the absence of true altruism, these individuals will adopt more robust privacy protections for themselves, despite knowing that if everyone adopted the same informed approach, the economic and social benefit we achieve as a society from Big Data would suffer.[208] Accepting that Big Data provides a social benefit to society as a whole, these individuals gain all of the benefits of Big Data, while not sharing in its costs. Research shows that:

---

204. Savage, *supra* note 141, at 98.

205. Hirsch, *supra* note 23, at 75.

206. De Mooy, *supra* note 39, at 18.

207. Garratt & van Oordt, *supra* note 161, at 3.

208. "The result is a form of a prisoner's dilemma situation: while each consumer has a private incentive to opt out of intrusive marketing, when all consumers do this, price competition is relaxed and consumers are harmed . . . . If our perusal of the theoretical economic literature on privacy has revealed one robust lesson, it is that the economic consequences of less privacy and more information sharing for the parties involved (the data subject and the actual or potential data holder) can in some cases be welfare enhancing, while, in others, welfare diminishing." Acquisti et. al., *supra* note 23, at 460, 462.

> Big [D]ata is likely to affect the welfare of unsophisticated, vulnerable, and technologically unsavvy consumers more negatively. Such consumers may lack awareness of multiple information sources and are less likely to receive up to date and accurate information about multiple suppliers in a manner that facilitates effective search and comparisons. They are also not in a position to assess the degree of sensitiveness of their online actions and are more likely to be tricked by illicit actors.[209]

Even more troubling, however, is the suggestion that laws regulating privacy will always "systematically favor the interests of sophisticated consumers . . . since sophisticated consumers are on the whole more politically engaged people who pay attention to legislative policy proposals and vote their interests."[210]

> These consumers arguably think they will lose nothing from policies that allow firms to access their data … and are likely to make the necessary efforts to fight against businesses' informational advantage. Some argue that the general public outside this group may not necessarily be a 'winner' in economic or other terms in corporations' [B]ig [D]ata initiatives that rely on 'data accessibility and manipulation.'[211]

Even with respect to the sophisticated users who want to optimize personal privacy, it is doubtful whether one can participate in society today without losing some level of control over personal data, commonly referred to as the ever-increasing cost of maintaining privacy.[212] Unless one makes judicious use of cryptocurrency and tor browsing,[213] it is virtually impossible to engage in anonymous digital transactions. Because platforms like LinkedIn have become so ubiquitous in business, a candidate's failure to have a profile

209. Kshetri, *supra* note 41, at 1152.

210. *Id.* at 1143.

211. *Id.*

212. Garratt & van Oordt, *supra* note 161, at 26–27.

213. A "Tor Browser" is a web browser that anonymizes the user's web traffic using the Tor network. TOR (2021), www.torproject.org.

on the platform could be seen as a red flag.[214] Moreover, communication by its very nature is always at least a two-way transaction. Even if one always prefers the most secure, privacy protecting options, those with whom they communicate may not be as judicious.

> Engaging with social media is therefore not an individual choice. It is an inevitable outcome of being in almost any social situation. Location information is a particularly powerful example of how one person's data can affect others. Cell phones track individuals' location precisely, and by proxy, the locations of others.[215]

Today, one has essentially no choice but to pass information over a platform that others can observe. Some suggest, therefore, that no reasonable expectation of privacy can possibly exist anymore, but our social norms clearly suggest that we as a society do not agree.[216]

This latter point demonstrates the implicit failing of any individualistic informed consent approach. "By conceiving privacy as individual right, liberal privacy conceptions fail to grasp the social existence of humans."[217] Stated colloquially, "every middle schooler understands that a fundamental problem of privacy online is not what one says about oneself, but what others say."[218] While there may be some thoughts and actions that truly occur in private, most of our intimacies are shared with others. We share our thoughts, feeling, and action to varying degrees with friends, loved ones, and professionals with some varying expectation of privacy. That privacy, however, depends on the other sharing that same expectation. An extreme example of the violation of a shared expectation of privacy, which already prompted explicit regulation, is revenge porn.

An individualist approach does not address the fact that "Big Data allows governments and businesses to track the habits and movements of groups, combine and recombine people into categories, and analyze and

214. Barocas & Levy, *supra* note 42, at 583.

215. Fairfield & Engel, *supra* note 65, at 402.

216. *Id.* at 576.

217. *Towards An Alternative Concept of Privacy*, *supra* note 6, at 226.

218. Fairfield & Engel, *supra* note 65, at 396.

attempt to predict their behavior."[219] When one user consents to information-gathering, that user becomes a conduit for gathering information about their entire social network, regardless of members' consent.[220] Pushed further, when one consents to share information, certain inferences can be drawn with others who share one or more traits with that person, even if the two have never met and are completely oblivious that they both have been collected into a group.[221]

> [D]ata is no longer gathered about one specific individual or a small group of people, but rather about large and undefined groups. Data is analyzed on the basis of patterns and group profiles; the results are often used for general policies and applied on a large scale. The fact that the individual is no longer central, but incidental to these types of processes, challenges the very foundations of most currently existing legal, ethical and social practices and theories.[222]

Scholars point to this social nature of our existence as the "nail in the coffin of the individualistic, notice-and-consent model of privacy regulation."[223]

The current individualist, informed consent approach to privacy is prophylactic at best. However, Big Tech's concern that the more restrictive opt-in approaches of the GDPR and CCPA will cause economic harm is not necessarily without merit. Research suggests that even a fully informed rational consumer who makes an optimal decision with respect to their privacy may not make the decision that is in the best interest of society on a macroeconomic scale.[224] Moreover, because privacy is both contextual and relational, each individual must make innumerable discrete privacy decisions,

---

219. Kammourieh et al., *supra* note 5, at 50.

220. Fairfield & Engel, *supra* note 65, at 410.

221. "Big Data allows governments and businesses to track the habits and movements of groups, combine and recombine people into categories, and analyze and attempt to predict their behavior. Individual data is no longer only useful for gaining information about and targeting the individual, but also – and perhaps above all – for gaining information about and targeting groups." Kammourieh et al., *supra* note 5, at 50.

222. Taylor et. al, *supra* note 8, at 13–14.

223. Barocas & Levy, *supra* note 42, at 561.

224. *Id.*

which not only impact them, but others as well. It is simply irrational to conclude that each member of society in each such instance can make a fully informed, rational decision that is maximizing for each member of a society.[225]

Recognizing the inherent failings of the individualist approach, governments have suggested that Big Tech simply regulate itself. Surprisingly, Big Tech has been unable to formulate any rational proposal to get itself out of its current predicament other than to express a willingness to be regulated.[226] What is clear, however, is that efficiencies demand a holistic approach that maximizes privacy, economic efficiency, and the free flow of cultural information within a society. There is no objectively correct demarcation of what society determines to be the optimal balance between privacy and access. Any determination will necessarily be political. What is clear, however, is that leaving this decision to us as individuals is *suboptimal*, as is regulating this demarcation on an instance-by-instance basis.

VII. HOW TO TREAT OUR CONTRIBUTION TO OUR SOCIETY

"How data is [characterized] affects how it is perceived, . . . which in turn influences [our] expectations" of how it should be treated.[227] A common refrain is that Big Data has replaced Big Oil as the world's most valuable asset.[228] This comparison, along with the notion that data is discovered and mined, however, is not neutral. Instead, it supports the supposition that data is something that can (or should) be owned by its collector.[229]

Big Data shares little with oil. While oil is finite and scarce, Data is not, with increasing amounts produced and collected each day. Where oil is

---

225. "Work on relational privacy recognizes that different privacy expectations attach to different people and institutions in our lives, and suggests that law should take into account these different sensitivities in setting rules about such expectations (for example, by recognizing that we may have a greater interest in privacy against the government than we do against our neighbors)." *See id.* at 560.

226. Isaac, *supra* note 4.

227. Scholz, *supra* note 45, at 875–76.

228. Dibley & Cole, *supra* note 46, at n.6; *see also The World's Most Valuable Resource is No Longer Oil, but Data*, ECONOMIST (May 6, 2017) https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/G2SH-ZBT5].

229. Scholz, *supra* note 45, at 876.

rivalrous, with many players vying for its limited supply, multiple people or entities can simultaneously use the same data set(s) without degradation. Where oil is essentially fungible, data sets are not; a data set of movie preferences is not interchangeable with medical records. Where oil is consumed upon use, data can be used over and over again for different purposes. [230] Finally, oil is clearly a good, created over millions of years with limited input from contemporary society.[231] Big Data is not. Instead, it reflects our collective preferences, statements, and actions. Unlike oil, the value of Big Data is its ability to reflect who we are.

Irrespective of the fact that the analogy of data to oil collapses under the slightest scrutiny, the notion of data as property is longstanding and persists.[232] As private property, economists have struggled to identify its relative price.

> Should the reference point be the price one would accept to give away their data, or the amount they would pay to protect it? Or, should it be the expected cost the data subject may suffer if her data is exposed, or the expected profit the data holder can generate from acquiring her personal information?[233]

What we do know, however, is that not only is privacy contextual, "[a]ttitudes towards privacy mainly capture subjective preferences," meaning that there is no objective way to value privacy, in the way we can determine that a Mercedes Benz costs more than a Hyundai.[234] In fact, some scholars go so far as to suggest that characterizing privacy as property that can be bargained for, "create[s] a false bargain, in which individuals could accept money in return for giving up on their inalienable privacy rights."[235]

Despite these analytical difficulties, it is still helpful to consider privacy as property in some respects. The Nobel Prize-winning economist Elanor

---

230. *Id.* at 7.

231. *Id.* at 10–11.

232. "Likening data ownership to traditional property ownership is well-trodden ground." De Mooy, *supra* note 39, at 26.

233. Acquisti et. al, *supra* note 23, at 447.

234. *Id.*

235. Dibley & Cole, *supra* note 46, at 10.

Ostrom narrowed the attributes of property to two dimensions: excludability and rivalry.[236] "Excludability refers to the extent which someone can legally prevent another from accessing a good; rivalry, refers to whether one person's consumption of a good impinges on another person's consumption of that same good."[237] While excludability is the product of law, regulation, contract, or norm, rivalry refers to the product itself. These two attributes form four categories of property, under which virtually all property falls. Private property is both rivalrous and exclusionary. Property that is not exclusive and is consumable would be a common pooled resource, like the fish stock in an ocean or a common grazing land, are referred to as "commons."[238] Commons are relatively uncommon in the U.S. where "[m]arkets, private hierarchies (firms), and/or public ones (governments) are the norm."[239] Public goods are those that are neither rivalrous nor exclusionary, like the air we breathe, street lights or fire departments.[240] While such property is not subject to elimination by consumption, it can be destroyed by misuse (environmental contamination) or a lack of collective investment (failing to adequately fund a fire department). Finally, there is property that is non-rivalrous but exclusionary, such as a county club or a toll road.[241]

As discussed above, our bias has been to view what we do, say, and like as individualistic private property, which resulted in our current informed consent regulatory schemes.[242] These schemes, however, do not seem to align well with the practical economic, social, or cultural realities of Big Data. Instead, today, Big Data, the collection of what we do, say, and like, is more analogous to a country club. A few control this "property," but

---

236. VINCENT OSTROM & ELINOR OSTROM, ALTERNATIVES FOR DELIVERING PUBLIC SERVICES: TOWARD IMPROVED PERFORMANCE 7–49 (Emanuel Savas ed., 1977).

237. Dibley & Cole, *supra* note 46, at 6.

238. "'The basic characteristic that distinguishes commons from non-commons is institutionalized sharing of resources among members of a community.'" Sanfilippo et. al., *supra* note 14 (manuscript at 4) (original emphasis omitted).

239. Savage, *supra* note 141, at 117–18.

240. Dibley & Cole, *supra* note 46, at 7.

241. *Id.*

242. "The legal literature on data and property has most often started from the assumption that data has private goods characteristics, and then considers the bundle of property rights that might attach given that construct." *Id.* at 6.

their collection, use, and disposition does not consume other members' collection, use, and disposition of the same.

Much has already been written attempting to analogize our current privacy predicament—the fact that our current regulations do not adequately implement our social, economic, and cultural goals—to a tragedy of commons. Economic analysis shows that when property is rivalrous but not exclusionary, a society will tend to over-consume beyond sustainability leading to collapse, such as overfishing and deforestation.[243] Since Big Data is defined by its vastness and velocity, the notion of such data collapsing due to overconsumption does not make sense.

Others have attempted to re-conceptualize property commons relevance to privacy as a trust commons.[244] This reasoning suggests that as personal data is exploited, we will lose trust in the collectors. The privacy paradox mentioned above along with individuals' lack of understanding of how their personal data is being exploited suggests that such a social change is unlikely. However, a regulatory adoption of this analogy might lead to a scheme that fails to adequately consider the economic and social values of this resource.

Finally, what we do, say, and like has been analogized to a public good. While "public good" property in the economic sense is not rivalrous in that consumption by one does not prevent consumption by another, it does create tension between selfishness and cooperation.[245] The free-rider dilemma, which is endemic to a public good—where everyone wants the benefit but not the burden—elegantly offers an explanation for "why everyone might deeply cherish privacy, yet still contribute to privacy-damaging stores of data, just as everyone likes clean air, but individuals still pollute."[246] The public good analogy from a more legal perspective is similarly helpful. It is similar to the manner in which societies see investments in infrastructure, education, and healthcare as beneficial to the society as a whole rather than simply the individual receiving the public benefit at the moment. This notion of public good brings an egalitarian focus to the problem of how we maximize the value of property that is neither rivalrous nor exclusionary. The question becomes: what should societies' investment be here?

---

243. Hirsch, *supra* note 23, at 77–78.

244. *See* Savage, *supra* note 141, at 99.

245. Fairfield & Engel, *supra* note 65, at 414–15.

246. *Id.* at 400.

In addition to the investment a society decides to make in a particular public good, we must still decide how it can be utilized, balancing preferences to best match the norms of a society. A holistic, egalitarian approach to our privacy dilemma seems suited to address the problems that "(1) different stakeholders—including businesses, consumers, and governments—each have different, multilayered, and often conflicting objectives; [and] (2) information technologies, privacy concerns, and the economics of privacy evolve constantly, with no single study or policy intervention being able to fully account for future (and even some present) concerns."[247] This does not necessarily lead to the conclusion that more regulation is necessary, bu instead, allows us to critically examine whether our current regulations actually optimize the norms we seek. As one "school of thought holds," our currently informed consent model "inhibits technology diffusion by imposing costs upon the exchange of information," while another argues that "explicit privacy protection promotes the use of information technology by reassuring potential adopters that their data will be safe."[248]

Regardless of whether what we do, say, and like is actually property in any sense, the means by which we differentiate types of property is enlightening. It also returns us to the Coarse Theorem.[249] We must start from our present situation and realize that any change will necessarily inflict harm. The goal is not simply to minimize the harm, such as by outlawing cattle grazing because of the damage it causes a neighbor's vegetable farm. Instead, the goal is "to avoid the more serious harm."[250] "When an economist is comparing alternative social arrangements, the proper procedure is to compare the total social product yielded by these different arrangements."[251] What we know is that our current scheme of incident-specific regulations (*e.g.*, HIPPA) and a reliance on individuals' decisions maximizing social welfare (informed consent) are simply not adequate.

247. Acquisti et. al., *supra* note 23, at 478.

248. *Id.* at 469.

249. *See* Coase, *supra* note 19.

250. *Id.* at 2.

251. *Id.* at 34.

VIII. PRIVACY AS A SOCIAL NORM

This Article is not bold enough to provide complete answers. Instead, its goal is to point out the economic, social, and cultural value to what we do, say, and like, and to demonstrate the disconnect between our current regulatory scheme and the realities of Big Data (the repository of what we do, say, and like). Today, tools exist to capture virtually every aspect of our lives, and based on their adoption, we view them and the data they capture as having normative value. The issue remaining is whether the price we pay for that value is economically and socially fair.

Another property analogy is valuable here. Article 1, section 8 of the U.S. Constitution expressly empowers Congress "[t]o promote the [p]rogress of [s]cience and useful [a]rts, by securing for limited [t]imes to [a]uthors and [i]nventors the exclusive [r]ight to their respective [w]ritings and [d]iscoveries."[252] Virtually every other nation shares this norm: that society should reward those who contribute their ideas to the advancement of a nation creatively or intellectually. In this same way, those who developed the means to capture, store, and analyze what we say, do, and like should be rewarded for that effort. The reward, however, must be normatively just.

No country gives a citizen a perpetual monopoly over an idea they contribute to society. Instead, each nation has decided to bestow a reward commensurate with the contribution, typically defined by time. Here, by contrast, those who collect what we do, say, and like are given a perpetual monopoly over this data. Research shows that this data gives those who control it a distinct economic advantage over any competitor. While research shows that our contribution of what we do, say, and like has value, and further questions whether the current bargained-for exchange is economically fair, there seems to be little evaluation of whether the value societies award to those who collect this data—an absolute monopoly—is normatively justified. In other words, does awarding a monopoly fit our existing societal norms? Would most people agree that the Amazons, Googles, and Facebooks of the world *should* have a monopoly? In contrast to those who contribute unique ideas (patent) or original expression (copyright) those who collect, store, process, and control Big Data are merely *salvagers*, having found unique ways of culling value from what otherwise would have been

252. U.S. CONST. art. I, § 8.

lost.[253] Considered this way, few would suggest that a salvager of what we do, say, and like is entitled to an award greater than an author or inventor. By the same token, however, a time-limited monopoly over collected data makes little sense due the nature and value of the good.

In addition to questions about what we sacrifice for the collecting, storing, and processing of what we do, say, and like, there are serious questions about whether what we receive as a society for the private control over Big Data is fair. While not a perfect analogy, a connection can be drawn between the value of our collective actions, statements, and preferences and the radio spectrum. Historically, the analog broadcast spectrum was narrow, a limited resource, and we collectively decided to empower a public agency—the FCC—to determine how best to maximize its value consistent with our social norms, *i.e.*, the public good. Similar to our privacy, consumers, creators, and distributors not only had competing interests with each other, but also amongst themselves. Rather than simply rely on the market or the ability of targeted legislation to identify and maximize social, economic, and cultural norms, the U.S. created the FCC to address the broadcast spectrum in a holistic manner. The FCC, however, took a hands-off approach with respect to the digital realm.

Despite our preference for private property and our bias towards believing that the invisible hand of a free market will maximize our collective goals and desires, it simply has not worked with respect to Big Data. Not only have individuals, other than the technologically adept, shown themselves unable to make decisions in their own best interest, nothing suggests they can make privacy decisions that maximize the public's interest. More troubling is the notion that our existing scheme is biased, favoring the wealthy, informed, and intelligent. The privileged class derives all of Big Data's benefits while shifting the burden to those less well-off. Irrespective of this moral issue, individual privacy decisions have been proven as all but irrelevant to what data is collected about an individual. Today, our participation in society, both socially and economically, is not only dependent upon our own use of tools that compromise our privacy, but the tools used by others which also compromise our privacy irrespective of our own diligence. To remove these tools, or to prevent their use to mine what we do, say, and like, is probably no longer an option.

Regulators have thrown up their hands and suggested that those responsible for collecting, storing, and analyzing Big Data—the Amazons,

253. "The purpose of salvage award policy is to promote not only humanitarian rescue of life and property but maritime commerce as well, by preserving property from destruction." Scholz, *supra* note 45, at 880–81.

Googles, and Facebooks—simply regulate themselves. These private entities in turn have *pleaded* for regulation but have failed to propose any alternative structure to replace our individualist, informed consent approach.

What is proposed here is to replace our individualist approach with an egalitarian one. Such an approach would conceive of privacy *collectively* rather than individually, acknowledge that privacy is both contextual and relational, and consider the value of what we do, say, and like a public good. Because we, the people, create that good, we should demand that this good be placed under the supervision of *us* through a regulatory entity in the spirit of the FCC: a governing body established to determine how information about what we do, say, and like is accessed and used, guided by "the public interest, convenience or necessity."[254] Like the FCC, this body would ensure that those with access to what we do, say, and like use that information as a trustee for the public that contributes to and benefits from this public good.

IX. CONCLUSION

Precisely what such a regulatory scheme would look like, and the breadth and scope of its powers, is beyond the scope of this Article—though expanding on the ramifications of this change of focus, if valid, is plainly necessary. The point here has been simply to demonstrate that what we do, say, and like is more akin to a collective *norm* than private property. If what we do, say, and like *is* a collective norm, an individualist notice/consent model for regulation, however structured, will never make sense. It is a quixotic attempt to fit a square peg into a round hole.

What we do, say, and like is who we are. It defines us socially, economically, and culturally. Considered this way, it is not suitable to treat this good as something that we each can individually bargain away to be placed under the exclusive control of a few private companies. The current system—which relies on individual choice—is neither optimal nor sustainable. Thus, our ability to *collectively* benefit from Big Data depends on our willingness to conceive of data privacy *collectively* and—based on that understanding—to seek a better way of regulating it.

254. Waldman, *supra* note 104, at 280.