AGAINST PRIVACY ESSENTIALISM*

DANIEL J. SOLOVE**

What is "privacy"? This is a question that has long been vexing, but it is of profound importance, as the way privacy is conceptualized influences the outcome of cases and the way that laws and regulations are crafted, interpreted, and enforced. How privacy is understood thus makes a difference about how it is protected; and what is included and excluded from an understanding of privacy often affects whether it is even protected at all.

In this Article, I respond to María Angel and Ryan Calo's critique of my taxonomic approach to understanding privacy, which conceptualizes privacy as a plurality of similar yet different things that share family resemblances to each other. In their article, Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy, *Angel and Calo note that although "Solove's taxonomic approach appears to have exerted an extraordinary influence on the shape and scope of contemporary privacy law scholarship," this approach "fails to provide a useful framework for determining what constitutes a privacy problem and, as a consequence, has begun to disserve the community." Angel and Calo recommend an approach to conceptualizing privacy that is best described as essentialist—a quest to define clear boundaries for privacy to demarcate it from other concepts and determine what is included and excluded.*

This Article argues against privacy essentialism. This way of thinking unproductively narrows thought, creates silos, leads to the overly narrow or overly broad failed attempts at conceptualizing privacy, stunts the development of the field, and results in constricted and impoverished policymaking. Privacy essentialism leads to a dead end, and it merely provides the illusion of certainty and clarity. More importantly, privacy essentialism often leads to law and policy that ignore important privacy problems and neglects serious privacy harms because they do not readily fit within the narrow boundaries of a particular conception of privacy. Privacy law and policy are better developed with the

** Bernard Professor of Intellectual Property and Technology Law, George Washington University Law School. Thanks to Danielle Citron, Woodrow Hartzog, Matt Lawrence, Matt Sag, and participants at the workshop at Emory University School of Law for productive comments on the manuscript. The students in Tonja Jacobi's class provided very helpful and candid comments. I commend the candor, as the comments were painful to hear, but quite illuminating, and they led to significant revisions to this Article. I thank María Angel and Ryan Calo for their good spirit in conducting this debate. They eagerly encouraged this response and shared their essay with me for feedback during its development.

taxonomic approach, which is more inclusive, flexible, and evolving than the essentialist approach. The stakes of which approach is taken are enormous—often affecting whether privacy is protected sufficiently or even whether privacy is protected at all in many circumstances.

INTRODUCTION

What is "privacy"? This question has long loomed over the privacy law field. It is a question of profound importance, as it influences the outcome of cases and the way that laws and regulations are crafted, interpreted, and enforced. For example, several privacy torts turn on whether a privacy interest is violated.[1] The scope and applicability of the Fourth Amendment to the U.S. Constitution turn on whether a government activity infringes upon a

1. RESTATEMENT (SECOND) OF TORTS § 652A (A.L.I. 1977).

"reasonable expectation of privacy."[2] Countless statutes at the state and federal levels aim to protect privacy, and the things they protect against are based on an understanding of privacy. The internal practices of organizations are also affected, as their conceptions of privacy shape how they assess the privacy risks of their products and activities. The way privacy is understood thus makes a profound difference in how it is protected—and sometimes whether it is even protected at all.

For a long time, countless commentators have struggled over how to define "privacy." More than a half century ago, Professor Arthur Miller lamented that privacy is "difficult to define because it is exasperatingly vague and evanescent."[3] A quarter century ago, Professor Robert Post observed scant progress in understanding privacy. "Privacy is a value so complex," he wrote, "so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[4]

Starting in the late 1990s, and throughout the first decade of my academic career, I developed an approach to conceptualizing privacy. In my first article on the topic, *Conceptualizing Privacy* (2003), I argued that the dearth of satisfying attempts to define the concept of privacy was due to the use of the wrong method.[5] Most attempts to conceptualize privacy sought a common denominator in all things that should belong within the boundaries of the concept of privacy. But this approach produced conceptions that were too narrow or too broad or vague. Overly narrow conceptions of privacy resulted in law and policy that ignored important problems and harms because they did not fit into particular notions of "privacy." Conceptions of privacy that were too broad and vague were not readily usable; they failed to provide sufficient guidance about what to protect.

I aimed to break free from this problem by advancing a pluralistic conception of privacy based on a family resemblances method of conceptualizing. Several years later, in *A Taxonomy of Privacy* (2006), I endeavored to identify the plurality of things within the concept of privacy and explain their resemblances and differences.[6] I united and updated these articles in my book, *Understanding Privacy* (2008), where I set forth my complete theory

2. *See generally* Katz v. United States, 389 U.S. 347 (1967) (Harlan, J., concurring) (describing how Fourth Amendment protection requires the privacy expectation to be one society recognizes as reasonable).

3. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 25 (1971).

4. Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001).

5. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) [hereinafter Solove, *Conceptualizing Privacy*].

6. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

of privacy.[7] "Privacy" is an umbrella term that refers to a group of related issues that are fruitful to discuss and address together.[8] Instead of fixating on the meaning of the word "privacy," it is more productive to examine particular problems. The endless squabble over the meaning of the word "privacy" is counterproductive and leads to a dead end. Throughout this Article, I will refer to this approach as the "taxonomic approach."

In a recent article, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, María Angel and Ryan Calo critique the taxonomic approach.[9] Angel and Calo begin by contending that "Solove's taxonomic approach appears to have exerted an extraordinary influence on the shape and scope of contemporary privacy law scholarship."[10] Several other scholars have agreed.[11] Over the years, the taxonomic approach has attracted supporters and detractors, including Calo more than a decade ago.[12] Now, Calo has returned with Angel to issue the most formidable critique of the taxonomic approach to date. Their main contention is that the taxonomic approach "fails to provide a useful framework for

7. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY].

8. *Id.* at 45.

9. María P. Angel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, 124 COLUM. L. REV. 507 (2024).

10. *Id.* at 522.

11. *See, e.g.*, Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski & Maša Galič, *A Typology of Privacy*, 38 U. PA. J. INT'L L. 483, 488 (2017) (noting that the taxonomy is "arguably the most-cited and best-known classification in recent privacy literature"); David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1082 (2014) (discussing "the popularity of Solove's suggestion that privacy is a diversity of things without any common essence").

12. Some supporters include: R. JASON CRONK, STRATEGIC PRIVACY BY DESIGN xv (2d ed. 2022) ("Chapter 3, on privacy harms, would not be possible without Daniel Solove. Before his work, scholars had attempted to categorize what society considers 'privacy violations,' such as Prosser's Privacy Torts, but Solove's Taxonomy captures privacy with a comprehensive and granular empirical analysis and thus offers a sense of completeness that more theoretical categorizations lack."); Danielle Keats Citron & Leslie Meltzer Henry, *Visionary Pragmatism and the Value of Privacy in the Twenty-First Century*, 108 MICH. L. REV. 1107, 1116 (2010) ("Solove's analysis and proposed solutions to those problems have received considerable attention from scholars, media, and the courts."); Hao-Ping (Hank) Lee, Yu-Ju Yang, Thomas Serban von Davier, Jodi Forlizzi & Sauvik Das, *Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks*, *in* PROCEEDINGS OF THE CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2024), 1, 2, https://doi.org/10.1145/3613904.3642116 [https://perma.cc/ZEY4-L8C4 (staff-uploaded archive)] ("Solove's taxonomy was proposed well before modern advances in AI became mainstream in product design, and remains relevant and influential to this day."); Woodrow Hartzog, *What Is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677, 1680 (2021) [hereinafter Hartzog, *What Is Privacy?*] ("Solove's work in privacy has been extraordinarily influential for scholars, policymakers, and practitioners."). Some detractors include Jeffrey Bellin, *Pure Privacy*, 116 NW. U. L. REV. 463, 513 (2021) (critiquing Solove's approach because "[t]he absence of a clear definition of privacy combined with widespread indifference to its necessity leads to unproductive debate and bad policy"); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1141–42 (2011) (faulting Solove's theory for lacking clear boundaries).

determining what constitutes a privacy problem and, as a consequence, has begun to disserve the community."[13] They are concerned that the taxonomic approach is too "overinclusive" and "opens the door to a skeptical court devaluing a harm by painting it with the privacy brush and obscuring the true value at stake."[14]

Their article warrants a response. At the outset, I want to note that I welcome Angel and Calo's critique. I am thrilled that they have so thoroughly engaged with my work, and I see their article as an invitation to revisit the issue about how to conceptualize privacy. I thus write with gratitude at having this opportunity to put my theory to the test, nearly twenty years after I started developing it, and seeing how it holds up today. Along the way, I will address other critiques of the taxonomic approach by Professors Jeffrey Bellin, Eric Goldman, and David Pozen.

In this Article, I sharply disagree with Angel and Calo that the taxonomic approach leads to bad policy outcomes such as courts devaluing privacy harms. To the contrary, the taxonomic approach is designed primarily to prevent bad policy outcomes that are caused by underinclusive conceptions of privacy, not overinclusive ones. With an underinclusive conception of privacy, policymakers (such as courts and legislatures) as well as internal organizational compliance officials often fail to recognize many privacy harms because they do not fit into their narrow conceptions of privacy.[15]

Angel and Calo's critique stems from fundamental differences in our starting assumptions and underlying philosophy. For the most part, Angel and Calo view privacy in an essentialist manner. Their privacy essentialism involves their commitment to understanding privacy as having clear boundaries to demarcate it from other concepts and a definitive definition with a proper authoritative foundation.

In this Article, I firmly reject privacy essentialism. This approach creates silos, leads to overly narrow conceptions of privacy, stunts the development of the field, and results in constricted and impoverished policymaking.

The implications of this debate transcend the particularities of my taxonomy and Angel and Calo's critique. Regarding privacy—and probably for many other concepts—the taxonomic approach is better than the essentialist approach. The taxonomic approach is more productive for the development of law and policy as well as for discourse and understanding. How privacy is conceptualized matters significantly. The stakes are enormous—often affecting

13. Angel & Calo, *supra* note 9, at 561.

14. *Id.* at 540.

15. *See generally* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022) [hereinafter Citron & Solove, *Privacy Harms*] (explaining how the requirement of harm impedes the enforcement of privacy law).

whether privacy is protected sufficiently or even whether privacy is protected at all in many circumstances.

Part I provides an overview of the taxonomic approach to conceptualizing privacy and discusses Angel and Calo's critique, which will be referred to as the "essentialist approach." Part II discusses why the taxonomic approach leads to better legal and policy outcomes than the essentialist approach. Part III responds to challenges that Angel and Calo raise about the taxonomic approach—that it is boundaryless, lacks a legitimate source of authority, lacks any criteria for inclusion or exclusion, and cannot resolve when different privacy issues conflict with one another. Part IV examines Angel and Calo's alternative to the taxonomic approach and explains why it fails on its own terms and why it would be worse for law and policymaking. Part V discusses how Angel and Calo's essay presents a thoughtful intellectual history of the development of privacy law scholarship and thinking over the past few decades and why this history actually supports the taxonomic approach.

I. CONTRASTING APPROACHES TO CONCEPTUALIZING PRIVACY

This Part begins by briefly summarizing the taxonomic approach and discussing Angel and Calo's critique, which stems from the fact that we approach conceptualizing in different ways and have divergent views on the work that a definition of "privacy" can do.

A. *The Taxonomic Approach*

In a series of works from 2003 to 2008, I developed a theory of how to conceptualize privacy. My thinking about the meaning of "privacy" began earlier in the late 1990s, and it took me a long time to develop the taxonomic approach. In this Section, I highlight my key conclusions.

1. A Pluralistic Concept Based on Family Resemblances

Before I developed the taxonomy, I first wrestled with previous attempts to conceptualize privacy. After surveying various theories of privacy developed across many decades, I concluded that these theories were unsatisfying because they were too narrow or too broad and vague.[16]

I ultimately found guidance in a brilliant insight from philosopher Ludwig Wittgenstein: the very method of conceptualizing privacy had to be rethought. I argued:

> Most attempts to conceptualize privacy thus far have followed the traditional method of conceptualizing. The majority of theorists conceptualize privacy by defining it *per genus et differentiam*. In other

16. Solove, *Conceptualizing Privacy*, *supra* note 5, at 1094.

> words, theorists look for a common set of necessary and sufficient elements that single out privacy as unique from other conceptions.[17]

In contrast, Wittgenstein proposed a different way of conceptualizing. He argued that some concepts lack a common denominator.[18] He used the example of games and noted that there is not "something that is common to *all,* but similarities, relationships, and a whole series of them at that."[19] As Wittgenstein observed, certain concepts involve "a complicated network of similarities overlapping and criss-crossing: sometimes overall similarities, sometimes similarities of detail."[20]

Drawing from Wittgenstein's notion of family resemblances, I contended that privacy should be understood in a pluralistic manner, as protection from many different problems that are related yet distinct. These problems should not all be treated the same. Existing attempts to define privacy with a common denominator are doomed to fail because no common denominator can capture the many things that are often being referred to when the term "privacy" is used. A common denominator extensive enough to address the many meanings of privacy would be so broad and vague that it would include nearly everything. Narrower common denominators would be too restrictive, omitting important things that should be included. My pluralistic conception aimed to escape from this Hobson's choice.

2. Privacy Lacks a True Fixed Meaning

Privacy has been quite challenging to conceptualize because it lacks a fixed meaning and is culturally and historically contingent. Privacy is an evolving concept. What privacy meant to people in prehistoric times is far different than what it means today: "[T]he matters that have been considered public and private have evolved because of changing attitudes, institutions, living conditions, and technology. The matters we consider private are shaped by culture and time and have differed across societies and epochs."[21]

Following Wittgenstein, I view meaning as emerging from use.[22] I thus reject essentialist conceptions, which require some form of ultimate authority or first principles. Under the taxonomic approach, the term "privacy" has no particular magic. It is not a Platonic concept with a clear right or wrong meaning. There is no grand arbiter, no god from on high who will reveal the true meaning of "privacy."

17. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 14.

18. LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS 31 (G.E.M. Anscombe trans., Basil Blackwell 3d ed. 1967).

19. *Id.*

20. *Id.* at 32.

21. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 50.

22. WITTGENSTEIN, *supra* note 18, at 20.

3. A Pragmatic Account

Another key part of the taxonomic approach involves the purpose of the term "privacy." Drawing from pragmatist philosophy, I argue that particular terms have purposes, and they are useful in so far as they are suited for their purposes. Trying to use particular terms for purposes for which they are ill-suited will create problems and lead to obfuscation rather than illumination.

"Privacy" is an umbrella term that is helpful to refer collectively to a group of related things, but beyond this, the term "privacy" serves little additional use. In *Understanding Privacy*, I noted that:

> [T]here are many times when using the general term "privacy" will work well, but there are times when more specificity is required. Using the general term "privacy" can result in the conflation of different kinds of problems and can lead to understandings of the meaning of "privacy" that distract courts and policymakers from addressing the issues before them.[23]

A pragmatic understanding of privacy focuses on usefulness as its key guiding star. To the extent that understanding the similarities between privacy problems is helpful, then it is useful to see the different problems in my taxonomy together. To the extent that there are differences, they should be acknowledged and understood.

4. A Taxonomy of Privacy

"Privacy" lacks clear borders. The taxonomic approach to understanding privacy is bottom-up and open-ended. In my first article developing the taxonomic approach, I analogized privacy to a web of related yet different things: "[T]he act of conceptualizing privacy should consist of mapping the typography of the web."[24]

I attempted to do this mapping in an article called *A Taxonomy of Privacy*.[25] My goal in understanding privacy was to facilitate the development of law and

23. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 45–46.

24. Solove, *Conceptualizing Privacy*, *supra* note 5, at 1130.

25. When I began the mapping project, which was first published in my article, *A Taxonomy of Privacy*, *supra* note 6, I had originally conceived of it as a mapping of a landscape. An earlier title of the piece was "*A Cartography of Privacy*," but I decided that readers would be more familiar with the term "taxonomy" and might be confused by my rather unconventional use of "cartography." Upon reflection, I think the term "cartography" more accurately describes the taxonomic approach. When I united my articles and further developed my theory in my book, *Understanding Privacy*, *supra* note 7, I retained the term "taxonomy" because this piece had become widely known under this moniker. But I described the project in the following way: "There is no overarching conception of privacy—it must be mapped like terrain, by painstakingly studying the landscape." SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at ix. This, in my view, is the most accurate description of the taxonomic approach. I view "privacy" as akin to a landscape, and I aimed to observe and describe it like a cartographer.

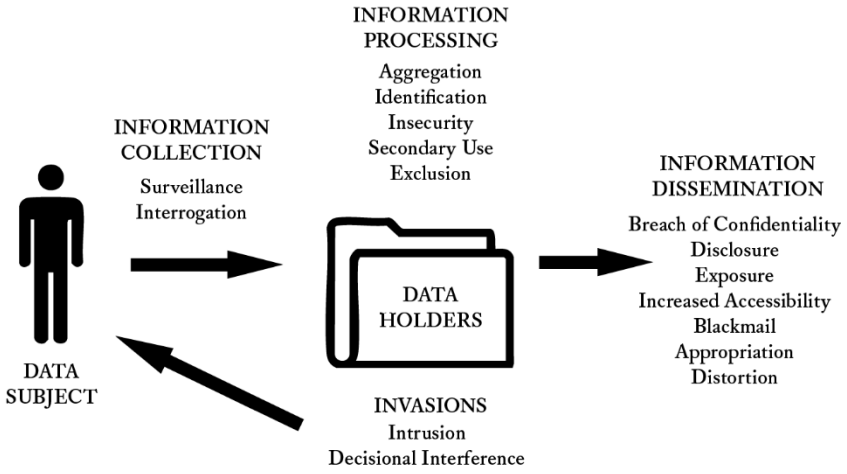
policy. I thus focused on situations where certain activities are causing disruptions and interventions might be needed.

The lack of a grand source of authority presents a challenge: Which sources should we use to determine privacy's meaning? I endeavored to identify "privacy problems that have achieved a significant degree of social recognition."[26] I approached this project with "a bottom-up cultural analysis, using historical, philosophical, political, sociological, and legal sources."[27] I focused primarily "on the law because it provides concrete evidence of what problems societies have recognized as warranting attention," but I also stated that my aim was "not merely to take stock of where the law currently stands today, but to provide a useful framework for its future development."[28] Additionally, I noted that the taxonomy is "but a snapshot of one point in an ongoing evolutionary process."[29]

I developed a taxonomy of privacy which consisted of four general categories of problems: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasions. Under each of these categories are sixteen different types of problems that were related yet distinct. As I explained, a "privacy interest exists whenever there is a problem from the related cluster of problems we view under the rubric of privacy. A privacy problem disrupts particular activities, and the value of protecting against the problem stems from the importance of safeguarding the activities that are disrupted."[30]

26. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 102.
27. *Id.*
28. *Id.*
29. *Id.* at ix.
30. *Id.* at 75–76.

Figure 1: The Taxonomy of Privacy



The goal of the taxonomy is to track privacy problems that can emerge throughout the "information life cycle," which refers to how information is generated, collected, processed, and disseminated until it ultimately is deleted or destroyed.[31] Many accounts of privacy focus on various parts of the information lifecycle, such as collection or dissemination, but they neglect other parts. The taxonomy demonstrates that privacy problems emerge during all parts of the information lifecycle, and these problems are different even though they have notable similarities.

A key dimension of the taxonomic approach is to study and understand the problems in a bottom-up manner. The project is not to try to force from the top down a rigid categorical structure. Instead, the taxonomy is to be used as a helpful way to see similarities and differences in problems and to better understand where privacy problems can arise and why they are problematic. Focusing on privacy this way is helpful in moving past some rather stultifying and limiting notions that have wormed their way into many privacy conceptions.

For example, consider *surveillance*, one of the privacy problems in the taxonomy under the category of *information collection*. Surveillance is a form of collecting information about people through watching, audio recording, or data gathering. I examined the effects of surveillance, which bring benefits as well as problems. The goal for policy is to maximize the benefits and mitigate the problems, ultimately achieving a normatively desirable balance.

I noted that surveillance causes at least two major problems: (1) chilling lawful and desirable activities such as speech, reading, exploration of ideas,

31. Meg Leta Ambrose, *It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten*, 16 STAN. TECH. L. REV. 369, 405–08 (2013).

discourse, and association; and (2) providing too much power to the watchers, leading to the potential for abuse. The goal of policy should be to acknowledge these problems and find ways to mitigate them. In some cases, the benefits of surveillance might outweigh mitigation efforts. In other cases, the problems might outweigh the benefits. But a productive discussion about how to modulate the costs and benefits can only occur if the problems are recognized and addressed.[32]

Crabbed notions of privacy impede this process. Many courts and policymakers assert that privacy involves only activities in private places, and thus any surveillance in public is not within the ambit of privacy protection. This manifests in the law through determinations that there is no reasonable expectation of privacy under tort law or Fourth Amendment jurisprudence when surveillance occurs in public.[33] Statutes exempt public surveillance or fail to protect publicly available information.[34]

This narrow notion of privacy loses sight of the problems. Surveillance in public can result in chilling and abuse. The problems of surveillance are thus present regardless of whether it occurs in public or private. Attempts to define privacy with a strict public/private binary lose sight of these problems.[35] In contrast, the taxonomy keeps the focus on the problems. It shows that privacy involves much more than a public/private distinction. Privacy involves how data is collected, how it is used, and how its collection and use affect people and society.

The taxonomy's categories "are not final and immutable."[36] I acknowledge that the taxonomy "is not meant to be the final word. It cannot be, because privacy is evolving."[37] The taxonomy was designed to be a beginning, not the end; a living project that evolves.

B. *The Essentialist Approach*

Angel and Calo contend that "the long-dominant social-taxonomic approach to privacy and privacy law is no longer serving the field."[38] The crux of their critique is essentialism. They reject the pragmatic open-ended nature

32. *Id.* at 174.

33. *See* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 235–37 (2002).

34. Daniel J. Solove & Woodrow Hartzog, *The Great Scrape: The Clash Between AI Scraping and Privacy*, 113 CALIF. L. REV. 1521, 1563 (2025) [hereinafter Solove & Hartzog, *The Great Scrape*]; Justin Sherman, *People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs*, LAWFARE (Oct. 30, 2023, at 15:03 ET), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs [https://perma.cc/3WXX-TMPU].

35. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 112.

36. *Id.* at 105.

37. *Id.* at 196–97.

38. Angel & Calo, *supra* note 9, at 511.

of the taxonomic approach and find it lacking firm authority. The main fault they advance is that the taxonomic approach lacks clear boundaries, which they assert makes its conception of privacy too expansive. According to Angel and Calo, the taxonomic approach has "ambiguous criterion of inclusion."[39] Angel and Calo write: "Unburdened by a need to define privacy, the past two decades have seen a Cambrian explosion in the arguments and issues at the heart of mainstream privacy scholarship."[40]

Additionally, Angel and Calo fault the taxonomic approach for failing to provide a sufficient source of authority to define privacy. They argue that the taxonomic approach is based on "social recognition" and "vague resemblance[s]."[41] They are concerned that privacy is too big a tent and can include "whatever information-based harm the right people are talking about."[42]

Moving beyond their essentialism, they turn to consequentialist concerns. They argue that "social taxonomy fails to provide a useful framework for determining what constitutes a privacy problem and, as a consequence, has begun to disserve the community."[43]

Angel and Calo advance two reasons that the taxonomic approach has been a disservice. First, they argue that "[s]ocial recognition alone cannot furnish a principled approach for determining whose voices are heard and valued when it comes to identifying new privacy harms."[44] They use the examples of information-based discrimination and algorithmic manipulation that "have come to be recognized as privacy harms in the past few years."[45]

Second, they contend that the taxonomic approach fails to "provide a framework for recognizing or addressing the internal tensions between conflicting values included in the growing privacy family."[46]

I will discuss each of these points in detail later on. Ultimately, the crux of their critique is that they prefer the essentialist approach—the traditional method of conceptualizing privacy—a singular concept with clear boundaries to what counts as privacy and a definitive source of authority for inclusion.

II. THE CONSEQUENCES OF THE APPROACHES

I most fervently disagree with Angel and Calo when it comes to the consequences of the taxonomic approach. They claim that the taxonomic approach fails to provide "courts, lawmakers, and scholars" with a "framework"

39. *Id.* at 548.
40. *Id.* at 511.
41. *Id.* at 553.
42. *Id.* at 560.
43. *Id.* at 561.
44. *Id.* at 529.
45. *Id.* at 531.
46. *Id.* at 529.

to resolve tensions among privacy problems.[47] They further argue that "[a]n overinclusive theory of privacy also opens the door to a skeptical court devaluing a harm by painting it with the privacy brush and obscuring the true value at stake."[48]

Far from creating these problems, the taxonomic approach does exactly the opposite—it serves as a framework that aids in the recognition and addressing of privacy problems, increases the appreciation of privacy harms, and helps clarify the values at stake. Moreover, Angel and Calo's essentialist approach has led to the exclusion of harms, a lack of recognition of problems, silos, and incomplete policymaking. Angel and Calo are advocating for an intervention that will likely create far more problems than it will solve; it will likely impoverish the discourse and lead to worse laws and regulations.

Angel and Calo want gatekeepers for the concept of privacy. They contend that only with the appropriate authority should something be granted admittance.[49] In contrast, the taxonomic approach views privacy as a landscape without walls or clear lines. Anything is welcome to the extent that it has a family resemblance to other things in the landscape. The goal of the taxonomic approach is problem-solving, not figuring out who or what should be admitted to an exclusive club.

The taxonomic approach aims to shift the focus from the gates to what is inside. Strict gatekeeping involves far too much conversation at the gate trying to persuade the gatekeeper about admittance, much like the old man in Kafka's parable, *Before the Law*, who spends his entire life outside the gate to the Law pleading to be granted admittance.[50]

The most interesting and important questions involve how particular privacy problems should be understood and addressed. The fact that these problems are all given the general label of "privacy" is not of paramount importance. All that the label "privacy" is doing is indicating that there are meaningful similarities that warrant treating different problems in similar ways, at least partially. When there are similarities, there can be helpful benefits of comparison. Tools to solve one problem might work on another problem. Ways of thinking about one problem might help with another problem.

The practical effect of Angel and Calo's view is exclusion. They repeatedly criticize the taxonomy for being too inclusive. Despite their discussion of the importance of diverse views in the field, their approach is exclusionary; it will excise issues from the discourse about privacy and expel scholars who are not talking about what they deem to be "privacy" issues.

47. *Id.* at 541.

48. *Id.* at 540.

49. *See id.* at 540–41.

50. Franz Kafka, *Before the Law*, *in* THE COMPLETE STORIES 3, 3–4 (Nahum N. Glatzer ed., 1971).

A. *The Dangers of Too Narrowly Defining Privacy*

Angel and Calo never pinpoint exactly what is wrong with a big tent for privacy. They argue that "[b]y uncritically broadening the concept of privacy, most Americans are missing out on a global conversation around data protection, information governance, and harm mitigation."[51] This claim is vague and ultimately unhelpful. Angel and Calo fail to justify how a narrower conception will inspire this "global conversation." They provide no evidence or examples to support claims such as this one and others.

In contrast, the dangers of too narrowly defining "privacy" are quite real and harmful. As I argued in *Understanding Privacy*, "[c]ourts and policymakers frequently struggle in recognizing privacy interests, and when this occurs, cases are dismissed or laws are not passed. The result is that privacy is not balanced against countervailing interests."[52]

1. The Perils of Silos

The landscape of privacy problems is best understood together rather than in siloed fashion. For example, data security, long a part of the privacy landscape, broke off from privacy in the early 2000s, and the effects of this were problematic, often hindering the protection of personal data.[53] The more that privacy and data security were treated together, as related rather than siloed domains, the better.[54] I fear that the Angel and Calo approach will lead to more silos and excluding issues from privacy. It is generally far better to err on inclusion rather than exclusion.

Silos emerge when the focus on issues has been bifurcated. Different people focus on different things. The result is the parable of the blind men and the elephant.[55] In one version of the parable:

> Six blind men approach an elephant in order to learn more about it. The first man touches the side of the elephant and concludes that an elephant is like a wall. The second man feels the tusk, and deduces that the elephant is like a spear. A third man grabs the squirming trunk, and resolves that the elephant is like a snake. The fourth man reaches out and pats the huge leg, thereby determining that the elephant is like a tree. The fifth man touches the ear, and thus infers that the elephant is like a

51. Angel & Calo, *supra* note 9, at 513.

52. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 7–8.

53. *See generally* DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 128–57 (2022) (outlining how the separation of privacy and data security within organizations has led to serious data breaches).

54. Lauren Henry, *Information Privacy and Data Security*, 2015 CARDOZO L. REV. DE-NOVO 107, 114 (2015) ("[I]nformation privacy and data security can be siloed into very different parts of professional practice.").

55. *Blind Men and an Elephant*, WIKIPEDIA, https://en.wikipedia.org/wiki/Blind_men_and_an_elephant [https://perma.cc/YD52-7QVR] (last modified Sep. 3, 2025, at 03:00 ET).

> fan. Finally, the sixth man seizes the swinging tail, and judges an elephant to be like a rope. And, so the story goes, each man vehemently argued for the truth of his perception.[56]

Courts and policymakers often recognize certain dimensions of privacy in some contexts but then fail to recognize them in others. This failure is due in part to siloed thinking—not seeing how the themes of privacy play across different laws and doctrines.

2. Constricted Judicial Conceptions of Privacy

Courts have adopted crabbed understandings of privacy to exclude important things from protection. In its Fourth Amendment jurisprudence, the U.S. Supreme Court has long determined whether the Fourth Amendment provides protection based on the existence of a "reasonable expectation of privacy."[57] A broader conception of privacy means greater Fourth Amendment protection, and a narrower conception means less protection. The Court has often adopted a very narrow and impoverished conception of privacy that has resulted in many problematic searches being left completely outside the protection of the Fourth Amendment.[58] I have long criticized the Supreme Court (and other courts) for conceptualizing privacy narrowly in an approach I have called the "secrecy paradigm."[59] Under this conception, privacy is understood as hiding secrets, and something is no longer private if it is exposed in any way to the public. In contrast, the family resemblances approach would include the whole landscape of related problems and would be more inclusive.[60]

56. C.R. Snyder, Carol E. Ford & Robert N. Harris, *The Effects of Theoretical Perspective on the Analysis of Coping with Negative Life Events*, *in* COPING WITH NEGATIVE LIFE EVENTS: CLINICAL AND SOCIAL PSYCHOLOGICAL PERSPECTIVES 3, 12 (C.R. Snyder & Carol E. Ford eds., 2013).

57. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J. concurring).

58. *See generally* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 93–145 (2011) (explaining the Supreme Court's Fourth Amendment jurisprudence, how it does not always comport with societal expectations of privacy, and how, in an increasingly digital age, it allows unacceptable intrusion into our lives); United States v. Knotts, 460 U.S. 276, 285 (1983) (no reasonable expectation of privacy when tracking device monitored movement in public); Florida v. Riley, 488 U.S. 445, 450–51 (1989) (no expectation of privacy in anything that can be viewed on one's property by police officers in a helicopter flying in legal airspace); Smith v. Maryland, 442 U.S. 735, 745 (1979) (no expectation of privacy in phone records); United States v. Miller, 425 U.S. 435, 445–46 (1976) (no expectation of privacy in bank records); California v. Greenwood, 486 U.S. 35, 39–41 (1988) (no reasonable expectation in trash one discards, even if in opaque plastic bags).

59. DANIEL J. SOLOVE, THE DIGITAL PERSON: PRIVACY AND TECHNOLOGY IN THE DIGITAL AGE 8 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON].

60. I have argued that ironically, Fourth Amendment jurisprudence would better protect privacy if it focused less obsessively on privacy—and the text of the Fourth Amendment does not even use the word "privacy" and instead restricts "unreasonable searches and seizures" which is a much broader approach. Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1535–37 (2010).

In my previous work, I have pointed out that in other contexts, the Supreme Court had embraced broader understandings of privacy. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[61] the Supreme Court held that there was a privacy interest in criminal history compilations sought under the Freedom of Information Act ("FOIA").[62] The Court noted that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[63] In my taxonomy of privacy, I called this dimension of privacy "aggregation," and I noted:

> *Reporters Committee* is one of the rare instances where American law has recognized that aggregation can make a material difference in what is known about an individual. Most courts adhere to the secrecy paradigm, which fails to recognize any privacy interest in information publicly available or already disseminated to others.[64]

The taxonomic approach points out broader understandings of privacy that are recognized even by the very same courts that in other contexts are adopting narrower understandings. The U.S. Supreme Court would later broaden its conception of privacy in Fourth Amendment law. In 2018, in *Carpenter v. United States*,[65] the Court held that there was a reasonable expectation of privacy in GPS data despite that it involved people's movements in public: "A person does not surrender all Fourth Amendment protection by venturing into the public sphere."[66] The Court observed: "[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[67] The Court further noted that location tracking "provides an all-encompassing record of the holder's whereabouts" and the data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[68] The Court finally recognized the problem of aggregation under the Fourth Amendment.

Beyond the Fourth Amendment, consider the U.S. Supreme Court case, *TransUnion v. Ramirez*.[69] TransUnion, a credit reporting agency, falsely labeled

61. 489 U.S. 749 (1989).
62. *Id.* at 774–75.
63. *Id.* at 764.
64. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 120.
65. 138 S. Ct. 2206 (2018).
66. *Id.* at 2217.
67. *Id.* (internal quotations and citations omitted).
68. *Id.* (internal quotations and citations omitted).
69. 141 S. Ct. 2190 (2021).

plaintiffs as terrorists in their credit reports, a violation of the Fair Credit Reporting Act ("FCRA").[70] The U.S. Supreme Court denied standing to plaintiffs whose reports had not yet been disclosed to others.[71] Despite having a valid cause of action to sue for a FCRA violation, the Court reasoned that the plaintiffs had not suffered a concrete injury because their files had not been disclosed.[72] Because there was no disclosure of the information, the Court apparently did not perceive any privacy harm.[73] In an article I wrote with Professor Danielle Citron, we argued that the Court overlooked many other privacy harms.[74] We contended that privacy involves "data quality harms" where errors and false information in people's records can make them "lose out on loans or jobs that they might have obtained if their data were accurate."[75] We also noted that "a reasonable person would certainly be justified in feeling emotional distress at being labeled a potential terrorist."[76]

In data breach cases, many courts make conclusory statements that the law doesn't recognize pure emotional distress as sufficient for cognizable harm. These courts often fail to consider the extensive body of privacy tort cases that contradict this claim.[77] We argued, "[T]he privacy torts, recognized in the vast majority of states, allow plaintiffs to recover for the disclosure of private information or the improper intrusion into private matters resulting in emotional distress."[78] Perhaps the failure of these courts to recognize data breach harm was due to the silo effect—these courts simply did not know about the privacy torts cases or think of them as relevant.

Big tent privacy helps courts recognize the foundations for protecting against privacy harms in more situations. The problem is not courts having too capacious an understanding of privacy but having an overly constricted one.

3. Exclusion in Policymaking and Compliance

Angel and Calo's quest to narrow privacy will likely result in excluding various privacy problems in policymaking and corporate compliance. Beyond

70. *Id.* at 2201.

71. *Id.* at 2214.

72. *Id.*

73. *See id.*

74. *See* Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion v. Ramirez, 101 B.U. L. REV. ONLINE 62, 68–69 (2021).

75. *Id.* at 69.

76. *Id.*

77. *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018) (arguing that courts have come out inconsistently by recognizing intangible and risk-oriented harms in other areas of law but have failed to do so in data breach cases).

78. *Id.* at 746.

pushing to broaden judicial conceptions of privacy, I have also argued to broaden conceptions of privacy for legislatures as well as organizations.[79]

Of course, the law could regulate various privacy problems separately with dozens and dozens of different laws. But many commentators have criticized the U.S. sectoral approach to privacy as an overly complicated patchwork.[80] And it is far from clear that narrowly defining privacy will lead to policymaking to address all the problems; most likely, if something is not included in the privacy tent, there will not be other tents to welcome it. Instead, it will be left out.

Many privacy laws require organizations to engage in privacy risk assessments.[81] Such assessments depend upon an understanding of privacy; a narrow conception will lead to failing to identify and mitigate risks. As Professor Ari Waldman has documented, the managers and engineers at many companies have overly narrow conceptions of privacy when doing a privacy impact assessment or privacy by design.[82] Waldman's interviews of engineers in technology companies revealed impoverished and crabbed conceptions of

79. *See generally* Daniel J. Solove, *Privacy by Design: 4 Key Points*, *in* 5 PRIV. IN GER. [PinG]: DATENSCHUTZ UND COMPLIANCE 191 (2015) (Ger.) (advocating for intentionally designing products, programs, and services with privacy in mind).

80. *See* Christopher G. Bradley, *Privacy for Sale: The Law of Transactions in Consumers' Private Data*, 40 YALE J. ON REGUL. 127, 131 (2023) ("Despite wide acknowledgement of its importance, the actual law of privacy remains famously unclear and incomplete: it has been described as a 'patchwork,' a 'hodgepodge,' a 'kludge,' and a 'smorgasbord'—a 'piecemeal' and 'scattershot' law, '[held] together with duct tape,' but left with 'gaps.'"); Felicia Jafferies & Amanda Graham Brazinski, *Navigating the Patchwork of U.S. Privacy and Cybersecurity Laws*, REUTERS (Oct. 9, 2023, at 20:57 ET), https://www.reuters.com/legal/litigation/navigating-patchwork-us-privacy-cybersecurity-laws-key-regulatory-updates-summer-2023-10-09/ [https://perma.cc/PE4Y-2HPG] ("The increasing patchwork of privacy and cybersecurity statutes, rules, and regulations on the state and federal level will likely result in further compliance costs to entities."); Daniel Castro, Luke Dascoli & Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws*, INFO. TECH. & INNOVATION FOUND. (Jan. 24, 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/ [https://perma.cc/8Q6T-E5GK] ("In the absence of a federal privacy law, a growing patchwork of state laws burdens companies with multiple, duplicative compliance costs."); Natasha Singer, *An American Quilt of Privacy Laws, Incomplete*, N.Y. TIMES (Mar. 30, 2013), https://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html [https://perma.cc/GLA6-242X (staff-uploaded, dark archive)] ("The American system involves a patchwork of federal and state privacy laws that separately govern the use of personal details in spheres like patient billing, motor vehicle records, education and video rental records.").

81. *See, e.g.*, Regulation (EU) 2016/679, art. 35, 2016 O.J. (L 119) 53; CAL. CIV. CODE § 1798.185(a14)(B). Nearly all U.S. state privacy laws require privacy risk assessments. *See* CTR. FOR INFO. POL'Y LEADERSHIP, COMPARISON OF U.S. STATE PRIVACY LAWS: DATA PROTECTION ASSESSMENTS 1–2 (Feb. 8, 2024), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comparison_us_state_privacy_laws_dpa_feb14.pdf [https://perma.cc/249E-H8RV].

82. *See* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 132–34 (2021) [hereinafter WALDMAN, INDUSTRY UNBOUND]. S*ee generally* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659 (2018) [hereinafter Waldman, *Designing Without Privacy*] (presenting the findings of a study of how designers of technology integrate privacy and user needs in the design process, including some fields where these considerations are hardly factored in at all).

privacy.[83] As Waldman notes, "many technologists did have a conception of privacy. I noticed two running themes during the interviews: privacy-as-notice-and-choice and the conflation of privacy and security."[84] Many engineers believed that "consumer privacy must be relatively narrow" which "misses the privacy concerns associated with data tracking and is, therefore, limited to notice-and-choice."[85] Waldman noted that a common narrow understanding of privacy was "control" over one's data or viewing protecting privacy as primarily about encrypting data.[86]

Turning to privacy legislation and regulation, I have devoted considerable scholarly attention to critiquing narrow approaches to privacy that view it as about individual control over personal data.[87] Several other scholars have also pointed out the limitations of understanding privacy as individual control.[88] Oddly, Professor David Sklansky critiques the taxonomic approach and wrongly claims that most scholars embrace control as the central meaning of privacy. He writes:

> Despite the popularity of Solove's suggestion that privacy is a diversity of things without any common essence, most discussions of privacy today—certainly most discussions by people who think of themselves as "privacy scholars"—*do* treat privacy as having a core meaning. The core meaning of "privacy" for these scholars is control over the use and dissemination of personal information.[89]

I find this assessment of the field to be quite inaccurate, and to no surprise, Sklansky's claim is not backed up by even one citation to a scholar writing after

83. WALDMAN, INDUSTRY UNBOUND, *supra* note 82 at 132–34.

84. Waldman, *Designing Without Privacy*, *supra* note 82, at 682.

85. *Id.* at 683.

86. *Id.*

87. *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 B.U. L. REV. 1021, 1023–24 (2024) [hereinafter Solove & Hartzog, *Kafka in the Age of AI*]; Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 978–79 (2023) [hereinafter Solove, *Limitations*]; Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 627 (2024) [hereinafter Solove, *Murky Consent*]; Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–82 (2013); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1398 (2001); SOLOVE, THE DIGITAL PERSON, *supra* note 59, at 93–97.

88. *See, e.g.*, Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1476–91 (2019); Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIA. L. REV. 559, 563 (2015) ("[F]ree choice is not the shibboleth of privacy in the information-sharing context."); Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 461–62 (2020) (critiquing approaches to privacy that seek "to facilitate individual choice"); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1660–64 (1999) (critiquing the "autonomy trap"); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1379 (2000).

89. Sklansky, *supra* note 11, at 1082.

1990. To the contrary, many scholars have rejected control over information as the core meaning of privacy.[90] It has been policymakers who have embraced control over information and enshrined it into law. As other academics and I have argued, the obsessive focus on privacy as individual control has led to colossal failures in privacy law.[91]

In many other instances, narrow conceptions of privacy have led to unfortunate omissions and exceptions in privacy laws. For example, the California Consumer Privacy Act[92] focuses obsessively on data transfer (through sale or sharing), and it fails to protect against many harms caused by the collection and use of personal data when it is not sold or shared. A multitude of states have followed in California's footsteps, enacting consumer privacy laws that are similar in focus.[93] The vast majority mainly address data transfer. But data transfer is just one dimension in the lifecycle of personal data, as reference to the taxonomy makes quite clear. The taxonomy demonstrates concretely what these laws are missing and how their focus is too narrow to address privacy problems comprehensively.

Another example of overly narrow conceptions of privacy is the many privacy laws that exempt publicly available personal data.[94] The taxonomy demonstrated how even publicly available personal data can cause the same types of privacy harms as nonpublicly available personal data: "With increased accessibility, a difference in quantity becomes a difference in quality—it heightens the risk of the harms of disclosure."[95] Many policymakers fail to see any harm in publicly available personal data because it is not "private" under their narrow conception. They view privacy narrowly "as a binary status—information is either completely private or completely public."[96] But especially in today's age of AI, massive quantities of publicly available personal data are being gathered and analyzed by sophisticated algorithms to make inferences about the intimate details of people's lives.[97] Because the taxonomic approach

90. *See supra* notes 4–7 and accompanying text.

91. *See, e.g.*, Solove & Hartzog, *Kafka in the Age of AI*, *supra* note 87, at 1023–24; Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617, 673 (2021); Richards & Hartzog, *supra* note 88, at 1463; Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 401 (2014); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 34 (2011); Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551, 564–67 (2023); Solove, *Murky Consent*, *supra* note 87, at 596–97; Solove, *Limitations*, *supra* note 87, at 993.

92. Ch. 55, 2018 Cal. Stat. 1807 (codified as amended at CAL. CIV. CODE §§ 1798.100–.199.100 (2020)).

93. JORDAN FRANCIS, FUTURE OF PRIVACY F., ANATOMY OF STATE COMPREHENSIVE PRIVACY LAW: SURVEYING THE STATE PRIVACY LAW LANDSCAPE AND RECENT LEGISLATIVE TRENDS 33–34 (2024).

94. Solove & Hartzog, *The Great Scrape*, *supra* note 34, at 1563–64.

95. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 150.

96. *Id.*

97. Solove & Hartzog, *The Great Scrape*, *supra* note 34, at 1530–31, 1573.

seeks to understand problems from the bottom-up, it avoids the pitfalls of being trapped within constricted notions of privacy that are antiquated in light of modern technology.

Overall, there are countless instances where courts, policymakers, technologists, and corporate officials have failed to recognize and address privacy problems based on an expressed or unexpressed overly narrow conception of privacy. I can't think of instances where an overly inclusive conception of privacy has resulted in less protection. Nor have Angel and Calo provided any examples.

B. *The Purpose of the Term "Privacy"*

A major part of my dispute with Angel and Calo boils down to how much work we expect the umbrella term of "privacy" to do. I do not think it can do much work other than to serve as an umbrella. There is nothing wrong with a generalized umbrella term like "privacy," but it is a mistake to rely too heavily on it and try to use it for more than just having a broad sense of the landscape. Generalities are useful to a point, but they are at best an impressionistic painting of the world, as they fail to capture things with sufficient detail, complexity, and nuance.

Angel and Calo contend that "[o]nly by distinguishing privacy can privacy law reach its full potential as a discipline and a body of law."[98] Distinguishing privacy in an essentialist manner is far from necessary; in fact, it gets in the way of the development of the law. Ultimately, essentialism generates debates over inclusion and exclusion, diverting attention away from more productive problem-solving. A key point in the taxonomic approach is that the debate over defining the precise boundaries of privacy is not fruitful and gets in the way of discussing and tackling problems.

Among the things Angel and Calo say that the taxonomic approach has done is that "it has freed scholars to explore and engage in broader discussions around concepts such as informational capitalism and the role of information in racial, gender, and other forms of discrimination."[99] Good. They also declare that "[n]ovel data-exploitation practices—from data mining to the application of machine learning and artificial intelligence to consumer and government decisionmaking—have become fundamental to privacy discourse, resulting in a Cambrian explosion of topics."[100] This seems appropriate, as data mining and AI often involve privacy issues.[101]

98. Angel & Calo, *supra* note 9, at 513. Unfortunately, they do not explain what they have in mind when they say "full potential."

99. *Id.* at 522.

100. *Id.*

101. *See* Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. 1, 5–6 (2025) [hereinafter Solove, *Artificial Intelligence*].

The taxonomic approach does not eschew rigorous theoretical analysis of issues; instead, the taxonomic approach invites such analysis but channels it away from unproductive attempts at definition of a general umbrella term to a more productive examination of particular problems. Instead of focusing obsessively on the gates to the privacy tent, the taxonomic approach focuses on the actual problems. Rather than spending so much time determining whether certain issues should be admitted into the tent or be left outside, one should use analogical reasoning to determine whether there were resemblances notable enough to include.

Angel and Calo are quite concerned about an overinclusive concept of privacy, but they fail to point out where the taxonomy is overinclusive. Instead, they point to things that were not included in the original taxonomy but were later recognized. For example, they discuss algorithmic manipulation (which they also refer to sometimes as "digital manipulation") and its inclusion as a privacy problem in the academic discourse about privacy: "Today, many scholars understand digital manipulation as a privacy problem or as a danger against which privacy can protect—so much so that it made its way into Solove and Citron's 2022 typology of privacy harms."[102]

If Angel and Calo agree that algorithmic manipulation should be included, then this isn't a good example of overinclusivity. They should be pointing to things that should be subtracted, not added. But perhaps they do not believe algorithmic manipulation should be included. If this is their claim, then I would disagree. Incorporating algorithmic manipulation into the taxonomy of privacy has had a positive effect on the development of law and policy. In recent years, legislatures have begun to include protections against "dark patterns" in privacy laws.[103] A "dark pattern" is "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation."[104] One can never know whether separate laws to address manipulation would have arisen had privacy laws not started to include the issue, but we should accept this development as a win.

Angel and Calo's discussion of algorithmic manipulation is thus a great example of how the taxonomic approach works rather than how it fails. Scholars started discussing the issue along with other privacy problems because of similarities. Legislatures started addressing the issue in privacy laws. This is how the open-ended taxonomy should evolve, and it is an example of how the law has begun to evolve in the same direction.

102. Angel & Calo, *supra* note 9, at 534.

103. *See, e.g.*, California Consumer Privacy Act, ch. 887, sec. 1, 2024 Cal. Stat. 7486 (codified as amended at CAL. CIV. CODE § 1798.140(l) (2024)).

104. *Id.*

Professor Woodrow Hartzog captures the goal of the taxonomic approach by noting: "By getting us past the threshold question of what privacy is, Solove's work provides room for scholars and lawmakers to tackle bigger phenomena."[105] Precisely. The debate over the meaning of "privacy" reminds me of William James' famous anecdote about the squirrel and the tree:

> The corpus of the dispute was a squirrel—a live squirrel supposed to be clinging to one side of a tree-trunk; while over against the tree's opposite side a human being was imagined to stand. This human witness tries to get sight of the squirrel by moving rapidly around the tree, but no matter how fast he goes, the squirrel moves as fast in the opposite direction, and always keeps the tree between himself and the man, so that never a glimpse of him is caught. The resultant metaphysical problem now is this: *Does the man go round the squirrel or not?* He goes round the tree, sure enough, and the squirrel is on the tree; but does he go round the squirrel?[106]

James explained that the entire debate turned on what "going around" means. If it means going around the squirrel in a circle, then the man went around the squirrel. If going around meant being on all four sides of the squirrel, then he did not.[107] The debate was fruitless, James argued. Instead, we should focus on "practical consequences."[108] And when we do focus on practical consequences, the virtues of erring on the side of inclusion win out over erring on the side of exclusion.

III. UNDERSTANDING THE TAXONOMIC APPROACH

Angel and Calo argue that we must "move beyond the comfortable habit of labeling whatever information-based harm the right people are talking about as a 'privacy problem.'"[109] In this Part, I address the ways their critique fails to appreciate the virtues of an open-ended conception of privacy. Their critique often is based on a misunderstanding of Wittgenstein's family resemblances, the way that a pluralistic conception of privacy works, as well as the nature of messy conceptual boundaries.

105. Hartzog, *What Is Privacy?*, *supra* note 12, at 1687.

106. William James, Lecture II - What Pragmatism Means, Lecture Series at the Lowell Institute and Columbia University (Nov. 1906–Jan. 1907), *reprinted in* WILLIAM JAMES, PRAGMATISM: A NEW NAME FOR SOME OLD WAYS OF THINKING 34 (1907).

107. *Id.*

108. *Id.*

109. Angel & Calo, *supra* note 9, at 560.

A. *Conceptual Boundaries and Family Resemblances*

1. Blended Privacy Problems and a Sharp Carving Knife

When it comes to their conception of privacy, Angel and Calo's essentialism sometimes has a binary nature. They are concerned about "what constitutes a privacy problem and what does not,"[110] what is inside the privacy tent and what is outside. Although I do not believe that Angel and Calo see privacy strictly as a binary, their essentialist demand for clear criteria for inclusion in the privacy tent creates challenges for issues that only partly involve privacy dimensions. These situations are complicated because privacy is often marbled throughout them or sometimes mixed into them in ways like fluids stirred together. I will call these "blended privacy problems."

Angel and Calo would surely recognize that problems are often not purely about privacy and that blended privacy problems exist. But such problems greatly challenge their project of drawing clear boundaries around the concept of privacy.

Under the taxonomic approach, labeling a problem a "privacy problem" does not mean that it is *only* a privacy problem. It just means that it has some similarities or family resemblances to other privacy problems. Placing it under the umbrella of privacy does not mean that it must be exclusively a privacy problem or be identical to other privacy problems. Instead, its being under the umbrella—or in the "tent" as Angel and Calo often refer to it—means that there is utility in focusing on the similarities. By looking at the similarities and overlap between distinct problems, fruitful thought and policy can develop. Similarity is not to be conflated with sameness, and the taxonomic approach can be misapplied if differences are ignored.

Angel and Calo want a gate to clearly separate what is inside from what is outside. Hybrid issues are difficult for gatekeeping because they belong partially inside and partially outside. Under the taxonomic approach, this problem does not present a headache. But for the essentialist approach, hybrid issues are hard. For example, Angel and Calo argue that "lumping questions of fairness into discussions of surveillance can potentially dilute both."[111] But what is wrong with discussing fairness and surveillance together? The Fair Information Practice Principles, the backbone of contemporary privacy law, are about fairness—hence the word "Fair." Surveillance involves fairness, as surveillance is unequally distributed.[112] Certainly, the fact that surveillance can

110. *Id.* at 509.

111. *Id.* at 556.

112. *See generally* SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS (2021) (describing how the lack of legal protections for privacy harm marginalized communities); SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS (2015) (examining the history of surveillance of Black people in the United States); Michele Gilman & Rebecca Green, *The Surveillance*

involve fairness does not mean that surveillance and fairness are the same thing. But just because surveillance and fairness are not the same thing does not mean that they have nothing to do with each other. Additionally, the FTC has long enforced the FTC Act Section 5's prohibition on "unfair" acts or practices in countless privacy cases.[113] Far from a stranger to privacy, fairness has often been deeply involved in privacy issues. Privacy is marbled throughout with various matters like fairness, and privacy and different matters overlap and intertwine. They cannot be readily separated.

In another example of a hybrid issue, recent discussions of AI have shown the complicated and nuanced relationship between AI and privacy. They are different yet also have extensive overlap.[114] AI involves privacy, yet also many other things such as copyright, safety, and free speech. This means that privacy law sometimes will be a useful tool to regulate AI, but not always. It means that some AI issues are about privacy and others are not. There is no bright line where privacy and AI begin and end, as if they are the borders between countries. Ultimately, the world is too complex for simplistic demarcations, so I do not think it is possible or even useful to try to somehow carve out AI as entirely separate from privacy.

2. The Lack of Clear Boundaries

At times, Angel and Calo appear to imply that the lack of clear boundaries to the concept of privacy allows nearly any information or technology problem to be considered as a privacy one. Privacy could become the "law of everything," as Nadezhda Purtova warned about EU data protection law based on its expansive definition of personal data.[115] In an earlier article, Calo warned that the overuse of the "privacy" label "risks its diffusion into a meaningless catchall."[116]

In a related critique to Angel and Calo's, Professor Jeffrey Bellin also faults the taxonomic approach for lacking clear boundaries: "Legal scholars take full advantage of the unchallenged freedom to fit more and more conceptions of privacy into this boundaryless theoretical space."[117] He argues: "Privacy

Gap: The Harms of Extreme Privacy and Data Marginalization, 42 N.Y.U. REV. L. & SOC. CHANGE 253, 281 (2018); KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017) (arguing that poor mothers in the U.S. have been deprived of the right to privacy).

113. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 160–63 (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599 (2014).

114. *See* Solove, *Artificial Intelligence*, *supra* note 101, at 15.

115. Nadezhda Purtova, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, 10 LAW, INNOVATION & TECH. 40, 41 (2018).

116. Calo, *supra* note 12, at 1137.

117. Bellin, *supra* note 12, at 466.

pluralism changed the game, turning ambiguity into a virtue, not a vice. Privacy emerged undefined and undefeated."[118]

Similar to Angel and Calo, Bellin assumes that the lack of clear boundaries in a Wittgensteinian family resemblances approach means that privacy is undefined. But this ignores the fact that the family resemblances approach is, indeed, a form of definition—it is just a different form than the traditional *per genus et differentiam* method. Rather than attempting to fully understand the family resemblances approach, Angel, Calo, and Bellin just dismiss it.

Like Angel and Calo, Bellin makes the claim that the lack of boundaries turns privacy into everything: "[W]hen privacy means everything it also means nothing."[119] I agree, as I even made a similar claim: "Privacy seems to encompass everything, and therefore it appears to be nothing in itself."[120] Under the taxonomic approach, privacy certainly does not encompass everything, so Bellin is arguing against a flawed understanding of the family resemblances approach.

Like Angel and Calo, Bellin wants an essentialist conception of privacy: "A viable definition of privacy should possess two characteristics. It should capture everything that truly constitutes privacy, and it should leave out everything else."[121] Bellin ultimately settles on a definition of privacy focused on disclosure: "We can think of a *right to privacy* as the *ability to prevent disclosure of information about ourselves*, and *privacy* as the *absence of information about us in the minds of others.*"[122]

"Precision matters," Bellin declares.[123] "Using the wrong term clouds important policy debates and increases the chances of miscalculating complex tradeoffs."[124] But precision was also at the heart of the taxonomic approach. A pluralistic understanding of privacy is more precise because the umbrella term of "privacy" is simply too broad and imprecise to capture the multifarious privacy problems. In the taxonomic approach, disclosure is one of the many privacy problems in the taxonomy.[125] But the term "privacy" encompasses more. It is more imprecise to arbitrarily narrow a broad term to exclude things just for the sake of narrowing it. Omitting many things does not make privacy more precise; it just makes it more restricted. Moreover, it is not more precise to describe something foggy as clear; the description should reflect the actual situation.

118. *Id.* at 468.

119. *Id.* at 471.

120. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 7. I invoked Jorge Luis Borges's wonderful parable, "Everything and Nothing" to elaborate on this point. *Id.* at 6–7.

121. Bellin, *supra* note 12, at 496.

122. *Id.* at 471.

123. *Id.* at 508.

124. *Id.*

125. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 140–46.

According to Bellin, "The absence of a clear definition of privacy combined with widespread indifference to its necessity leads to unproductive debate and bad policy."[126] Bellin notes that privacy does not always win when balanced against conflicting values; he aims to "break the cycle."[127] But no matter how clear the definition of privacy is, it will not break the cycle because it cannot tell us how to balance the value of privacy against conflicting values. Privacy issues are contextual, and whether privacy wins or loses depends upon the context.[128] Bellin wants the umbrella term of "privacy" to do far more work than it is capable of. But terms like this just cannot do the work Bellin demands. For example, the term "freedom" cannot solve all debates about freedom, no matter how precisely the term is defined. Instead, for policymaking, various situations must be analyzed.

Just because a concept lacks clear boundaries does not mean that it lacks boundaries. Wittgenstein uses the term "blurred edges" and "indistinct picture" to describe the boundaries of categories.[129] Author Herman Melville captures it most eloquently: "Who in the rainbow can draw the line where the violet tint ends and the orange tint begins? Distinctly, we see the difference of the colors, but where exactly does the one first blendingly enter into the other?"[130] The fact that boundaries are unclear does not mean that they do not exist.

In a similar way to Bellin, Angel, and Calo, Professor Eric Goldman argues that the "taxonomical approach to defining 'privacy' has no natural boundary."[131] He contends that "[v]irtually every policy question could have privacy implications, so the privacy umbrella keeps expanding to account for those implications."[132] He declares: "We don't want privacy experts making policy decisions about topics outside their swimlanes. They lack the requisite expertise, so they will make serious and avoidable policy errors."[133] However, I am not arguing that every policy question has privacy implications. But to the extent that a policy question does have privacy implications, it would seem that the rest of Goldman's critique does not follow. If privacy is implicated, then at least the privacy dimensions are within the swim lanes of privacy experts.

126. Bellin, *supra* note 12, at 513.

127. *Id.* at 514.

128. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010) (developing a theory of privacy as "contextual integrity").

129. WITTGENSTEIN, *supra* note 18, at 29.

130. HERMAN MELVILLE, BILLY BUDD, SAILOR 102 (Harrison Hayford & Merton M. Sealts, Jr. eds., Univ. of Chi. 1962) (1924).

131. Eric Goldman, *Privacy Law Is Devouring Internet Law (and Other Doctrines) . . . To Everyone's Detriment*, TECH. & MKTG. L. BLOG (May 9, 2023), https://blog.ericgoldman.org/archives/2023/05/privacy-law-is-devouring-internet-law-and-other-doctrines-to-everyones-detriment.html [https://perma.cc/D7RN-8FSG].

132. *Id.*

133. *Id.*

3. Everything "Privacy" Is Not the Same

A key virtue of the taxonomic approach is the recognition that not all privacy issues are the same. The essentialist approach reduces all privacy issues to a singular essence. But as the taxonomy demonstrates, "privacy" involves many similar yet different things. It would seem that a compelling way to demonstrate the overinclusiveness of the taxonomic approach would be to point to examples of things in the taxonomy that should not be included. Yet, Angel and Calo fail to do so.

The essentialist approach aims to impose a top-down, pre-fabricated definition onto everything. This approach is similar to actions of Procrustes, who tried to fit everyone into his bed, lopping off limbs or stretching them so that they fit. With privacy, this approach has often led to definitions with notable omissions. As I have argued above, essentialist definitions of privacy have resulted in policymakers and courts failing to recognize and address problems. I provided concrete examples here as well as in my previous work. In contrast, the essentialists have not pointed to actual instances where a broader open-ended approach has resulted in bad policy or case outcomes. As the many examples I examined demonstrate, we should resist the Procrustean urge to cut and divide in order for something to fit into a pre-defined box. Privacy problems are better understood and addressed by examining them from the bottom up through analogical reasoning.

B. *Social Recognition, Analogical Reasoning, and Authority*

Angel and Calo argue that the taxonomic approach to identify privacy problems in the taxonomy based on "social recognition" provides an inadequate authoritative foundation. This critique grows out of an earlier article by Calo, *The Boundaries of Privacy Harm*, where he criticizes the taxonomic approach and demonstrates his essentialist concern for authority: "A working definition of privacy harm gives us a 'limiting principle' that guards against dilution and may reveal other important harms. It also means having a 'rule of recognition' that permits the identification of novel privacy harms as they emerge."[134] For Calo, there must be authoritative sources to determine what is included in privacy's tent. "But what happens if someone disagrees with these sources?" Calo asks.[135] "How does one go about *denying* that a given harm is a privacy harm?"[136] He continues: "Conversely, how does one go about arguing that a new harm should be included as a privacy harm, before the right sorts of authorities have recognized it as such? We would have to wait until they do."[137]

134. Calo, *supra* note 12, at 1136.
135. *Id.* at 1141.
136. *Id.*
137. *Id.*

More than a decade later, Calo and Angel declare that "[t]he time has come to be wary of social recognition as the 'sacred canon[] of objective truth' and the sole gatekeeper for the privacy field."[138] They argue that "[t]he criteria for what makes the problem a privacy problem . . . should be something other than social recognition or a vague resemblance."[139]

The taxonomic approach, however, does not claim to be objective truth. It is Angel and Calo who want this. Because there is no gatekeeper with a grand ledger book, the best one can do is offer a convincing interpretation—to articulate resemblances, to use analogical reasoning, and to make strong arguments—and then evaluate the consequences. There are no "right sorts of authorities" because such authorities do not exist. Anyone can refer to whatever sources they want and make an argument about why their sources are illuminative. Anyone can make arguments about whether it is useful to add new problems to the taxonomy or suggest changes or deletions. Privacy is a societal construction,[140] and the most suitable way to understand privacy is through societal interpretation. Just as there are no definitive objectively true interpretations of a literary text, there are no such interpretations of privacy. But still, compelling arguments can be made that certain interpretations are better than others. Ultimately, this is the best scholars can do.

Angel and Calo do not argue that any of the problems in the taxonomy should be excluded. In fact, they mention new problems not included in the taxonomy (algorithmic manipulation and information-based discrimination) and argue that they could be included and then turn around to argue that the taxonomy is flawed because it might include them.[141] Despite lamenting the weak source of authority in the taxonomic approach, Angel and Calo fail to provide any alternative sources of authority or any indication of what types of authority would be acceptable. Even when they advance their own conception of privacy, they provide no source of authority for it. Using social recognition as a basis of authority is arguably better than using nothing at all.

The taxonomic approach relies on social recognition to a degree, but it also uses analogical reasoning, much like the way that common law precedent works.[142] Cases that are similar to each other are to be decided similarly. Although not all cases are identical, the common law's reasoning focuses on how

138. Angel & Calo, *supra* note 9, at 531.

139. *Id.* at 553.

140. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 958 (1989).

141. They also fault me for excluding them.

142. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 46; CASS R. SUNSTEIN, LEGAL REASONING AND POLITICAL CONFLICT 61 (2d ed. 2018); Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741 (1993) (providing a comprehensive examination of analogical reasoning).

to weigh the similarities or differences between cases.[143] Using a common law approach to recognizing problems for the purpose of legal and policy responses is far from arbitrary.[144]

Angel and Calo engage in a lengthy discussion about how information-based discrimination and algorithmic manipulation came to be included in the taxonomy.[145] For a justification for the inclusion of these problems in the taxonomy, I would point Angel and Calo to their own discussion. However, they are not satisfied with this analysis as a basis for inclusion; they want a higher authority—the "right" sources. They fail to provide such sources; they do not even attempt to advance any guidance about how to identify such sources.

In my view, there is no higher authority. The best we can do is to engage in societal interpretation. For my taxonomy, I looked to various cultural, legislative, judicial, historical, literary, anthropological, and other informed sources. Privacy is a social and cultural concept. It is not separate from society and culture; it is a facet of human thinking and behavior. Nevertheless, my interpretation is far from objective truth. I used a broad array of sources from the humanities rather than the opinions of everyday people.

Some scholars have attempted to understand privacy by studying the actual beliefs and attitudes of people by interviewing them; they have interviewed lay people, corporate privacy officers, and regulators.[146] Although I do not reject this interview-style approach, I developed the taxonomy by focusing on academic and legal literature rather than direct discussions with people. I was not aiming for a populist understanding; I aimed to develop a

143. EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING 3 (1948); Grant Lamond, *Precedent and Analogy in Legal Reasoning*, STANFORD ENCYC. OF PHILOSOPHY ARCHIVE (2016), https://plato.stanford.edu/archives/spr2016/entries/legal-reas-prec [https://perma.cc/QJ8R-MTWR].

144. MELVIN ARON EISENBERG, THE NATURE OF THE COMMON LAW 3 (1988) ("[T]he most basic institutional principle of the common law is that rules announced in earlier cases should be consistently applied and extended if they are substantially congruent with applicable social propositions, but should not be consistently applied and extended if they are not substantially congruent with social propositions.").

145. Angel & Calo, *supra* note 9, at 522–29, 532–36.

146. JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY (2001) (using interviews of low-income mothers who receive welfare); DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS (2014) (using interviews of teens about their use of social media); ALICE E. MARWICK, THE PRIVATE IS POLITICAL: NETWORKED PRIVACY AND SOCIAL MEDIA (2023) (using interviews of marginalized people about privacy); KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015) (using interviews of various corporate employees and executives about privacy); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011) (using interviews of chief privacy officers about corporate privacy management); Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 758 (2016) (using interviews of state attorneys general about privacy enforcement).

pragmatic philosophical one for the purposes of law and policymaking. I thus looked most closely at sources in law and regulation.

Ultimately, there are no definitive answers about what is included or excluded from the taxonomy. I attempted to craft the taxonomy based on what I had read and studied. My taxonomy was limited and imperfect because my knowledge was limited and imperfect.

The taxonomy is an open project. Angel and Calo have shown how information-based discrimination and algorithmic manipulation "have made it into the taxonomy"—even when they were not initially included.[147] They seem to want an ultimate answer as to whether these things should be included, but they can't point to any better source of authority on this matter beyond the social recognition they find to be inadequate.

C. *The Nature and Purpose of Definitions and Conceptions*

The taxonomic and essentialist approaches diverge greatly in how they understand the purposes of the term "privacy." The essentialist approach focuses on the term "privacy." In contrast, the taxonomic approach views the term as quite limited in purpose. "Privacy" works as an umbrella term to refer to a group of related things, but it cannot do much additional work. The real work is done by the taxonomy itself.

Understanding something transcends mere definition. For example, knowing the definition of "animal" does not mean that one understands animals. To understand animals, one must study animals and learn the different types and how they are similar and different. A definition of "animal" may help us distinguish animals from plants, but it will not help us understand how a tiger compares to a lion or how a cat compares to a dog. Similarly, the word "privacy" itself contributes only mildly to an understanding of what constitutes privacy—and often has led to more obfuscation and confusion. This is why the taxonomic approach aims to advance beyond the umbrella term of "privacy" to develop an understanding of specific privacy problems.

Angel and Calo have different expectations about what definition can give us. Angel and Calo often speak of "privacy" as if it has a true meaning that corresponds to some type of Platonic ideal. In my view, there is no true meaning of privacy. Conceptions are mental constructs that are more akin to tools—they should be evaluated in terms of their usefulness. "Privacy" does not have an inherent meaning that transcends history and culture. Meaning emerges from use, and use changes over time.

147. *Id.* at 529.

D. *The Clash of Values*

Angel and Calo contend that the taxonomic approach inhibits the ability to resolve conflicts between different privacy interests. They argue that "[t]he social-taxonomic approach also omits, and arguably impedes, the development of a sophisticated framework for interrogating the tension *between* the various values under the privacy umbrella."[148]

This argument assumes that everything under the umbrella label of "privacy" cannot be compared or contrasted, as well as cannot be in conflict. But under the taxonomic approach, "privacy" consists of many things, not just one thing; and these things can conflict with each other.

Angel and Calo invoke Professor David Pozen's discussion of "privacy-privacy tradeoffs" and develop it into one of the central pillars of their argument for why my taxonomic approach leads to bad results.[149] In his essay, Pozen argues for the recognition that, in some cases, privacy interests can conflict with other privacy interests.[150] Pozen begins by noting what he calls privacy's "*pluralistic turn*," and states, "Professor Daniel Solove's work is exemplary in this regard."[151] He discusses my taxonomy for several pages, listing it in full. By and large, his discussion of the taxonomy is an accurate description. He concludes that "[t]he very breadth of the taxonomy underscores the need to start balancing privacy against itself."[152]

For the most part, I am on board with Pozen's argument. But he makes one key misunderstanding of the taxonomic approach that ultimately leads Angel and Calo astray. Pozen states: "Pluralistic theories of privacy . . . maintain that there are many different valid understandings of privacy and that none has priority over the others."[153] However, the taxonomic theory does not imply that all problems are equal; in fact, it demonstrates the opposite.

In a chapter in *Understanding Privacy* about the value of privacy, I contended that "[p]rivacy problems impede certain activities and the value of privacy emerges from the value of preserving these activities. Privacy, therefore, does not have a uniform value. Its value must be worked out as we balance it against opposing interests."[154] Just because different issues are labeled "privacy" issues does not mean they all have the same value. Questions of value must often be determined contextually.

Pozen makes a useful contribution by stating that sometimes privacy interests conflict. Pozen expresses some concern over the expansiveness of my

148. *Id.* at 511.
149. David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 221 (2016).
150. *Id.* at 222.
151. *Id.* at 225.
152. *Id.* at 228.
153. *Id.* at 242–43.
154. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 78.

taxonomy, and he argues that "[t]he more sorts of privacy claims that there are, the greater the risk that there will be conflicts among them."[155] But he does not make claims much stronger than this. Indeed, this is a risk, but so what?

Angel and Calo see "privacy-privacy tradeoffs" in a different way than Pozen. For Angel and Calo, the fact that two forms of privacy in the tent are in conflict is paralyzing. According to Angel and Calo, "holding a giant umbrella over myriad, sometimes-conflicting values exacerbates the dilemma of privacy-privacy tradeoffs while giving no clues about how to unpack or reconcile internal tensions between family members."[156] For Angel and Calo, when conflicting values are "part of the privacy family," it "renders these types of tensions harder to recognize and resolve."[157] No, it does not. Nothing is stopping the resolution of the tension. Whether conflicting values are in the same tent or in a different tent really doesn't matter. Every family knows that not all family members get along. For Angel and Calo, family disputes must be resolved by kicking someone out of the family.

Angel and Calo claim that "[l]abeling everything as 'privacy' diminishes scholars' capacity, not to mention the capacity of lawmakers and courts, to balance information harms, one against the next."[158] Angel and Calo wrongly assume that bringing everything under the same tent makes them identical and of equal value. But the taxonomic approach recognizes the differences between the privacy problems in the tent. The fact that things fall under the same tent does not mean that they are the same; it just means that they have significant similarities that are productive to recognize and address together. Focusing on similarities does not logically exclude also recognizing and addressing differences. The taxonomic approach does not aim to hide differences or make them harder to recognize; in fact, the taxonomy explicitly highlights differences and distinctions between different privacy problems and does not seek to meld them all into a single monolith. Everything in the taxonomy is not the same; they are merely *related*. Similar does not mean the same.[159]

155. Pozen, *supra* note 149, at 227.

156. Angel & Calo, *supra* note 9, at 541.

157. *Id.* at 546.

158. *Id.* at 551.

159. Angel and Calo invoke discussions of privacy by feminist law scholars in the 1980s, especially Catharine MacKinnon who argued that privacy was long used to further patriarchal society, hide the abuse of women, and exclude women from the public sphere. *Id.* at 542–44; Catharine A. MacKinnon, *Privacy v. Equality: Beyond* Roe v. Wade, *in* FEMINISM UNMODIFIED 93, 102 (1987). In *Understanding Privacy*, I discussed MacKinnon's views but also mentioned the views of other scholars such as Professors Anita Allen, Ruth Gavison, and Judith DeCew who have contended that privacy has also played an important role in protecting women. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 81–82, 97. More recent work by Professor Danielle Citron has also emphasized how "intimate privacy" is essential rather than harmful to women. *See generally* DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE (2022). Ultimately, there is no reason why both claims cannot be true. Privacy can be used in ways to harm women, but it

Further, it is important to recognize that privacy is not the only conception with internal conflicts. Consider "free speech," where the speech of some people can inhibit the speech of others and even silence them.[160] At a more general level, "liberty" and "freedom" conflict with themselves. Various things under the "liberty" tent often conflict with other things under the same tent. To address these conflicts, legal minds engage in a normative analysis of each situation and determine how the law should attempt to navigate the tension. John Stuart Mill was able to propose ways to resolve tensions within liberty by privileging self-regarding acts.[161] Ultimately, the resolution of conflicts does not depend upon labels because the conflicts are not about labels. They are about values.

The taxonomic approach is not designed to answer questions about how to resolve tensions between conflicting values. As I argued in *Understanding Privacy*, "declaring that an activity is problematic does not automatically imply that there should be legal redress, because there are many valid reasons why the law should not get involved or why countervailing interests should prevail."[162] Furthermore, the "question of when and how the law should regulate can be answered only in each specific context in which the question arises."[163] Resolving questions of value depends upon a larger theory of the good. Slapping different labels on values in tension does not resolve the conflict.

IV. AUTHORITY AND SOCIAL RECOGNITION

Angel and Calo critique the taxonomic approach as lacking in adequate authority: "The criteria for what makes the problem a privacy problem, however, should be something other than social recognition or a vague resemblance."[164] What, then, should be the criteria? The best critique of a theory is to advance a better theory, so it is important to examine what Angel and Calo propose as an alternative to the taxonomic approach. They actually offer two alternatives—an essentialist definition of privacy and what they call a "functional" approach. In this Part, I examine each in turn.

also can be used in ways to help women. We do not need different terms for every use of privacy. Privacy is often used as a tool to achieve other ends. Think of it like a hammer. Suppose Baxter uses a hammer to pound in a nail, but Maxwell uses it to murder someone by bashing them on the head. Both Baxter and Maxwell are using a "hammer." We can acknowledge that Baxter's use of the hammer is good and Maxwell's is bad without having to relabel one of the hammers as something else.

160. CITRON, *supra* note 159, at 124 ("When digital communications are involved, plaintiffs and defendants may have privacy *and* free speech rights at issue."); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 8–9 (2014) (discussing how victims of online hate speech and harassment stop speaking online and shut down their blogs and social media accounts); MARY ANNE FRANKS, FEARLESS SPEECH: BREAKING FREE FROM THE FIRST AMENDMENT (2024).

161. JOHN STUART MILL, ON LIBERTY 13 (Norton ed. 1975).

162. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 102.

163. *Id.* at 103.

164. Angel & Calo, *supra* note 9, at 553.

A. *Angel and Calo's Essentialist Conception of Privacy*

To counter the taxonomic approach, which understands privacy as a plurality of different things that bear a family resemblance to each other, Angel and Calo offer their own conception of privacy, one rooted in a single definition: "[T]o qualify as a privacy problem, we think, a given phenomenon must involve: (1) an observation that (2) exposes individuals to unbalanced information relationships and (3) that renders them vulnerable and/or powerless."[165] This definition of privacy is flawed for several reasons.

First, their definition fails their own critique of the taxonomic approach, which they argue "raises critical questions about authority, legitimacy, and whose voices should be heard and valued when it comes to identifying new privacy harms."[166] Yet, when it comes to their own efforts, they merely assert a definition of privacy without any indication of its authoritative pedigree. For the part of their definition involving vulnerability and power, they cite only a few scholars, including myself, Ryan Calo himself, Gianclaudio Malgieri, Jędrzej Niklas, Nora McDonald, Andrea Forte, Julie Cohen, Neil Richards, Woodrow Hartzog, and Ari Ezra Waldman.[167] These scholars are not new or diverse voices. Most are legal academics who have long been in the privacy tent.[168]

If social recognition and family resemblances are insufficiently authoritative for Angel and Calo, then it is surprising that they supply no foundation in authority whatsoever for their definition of privacy. As flawed as social recognition or resemblance might be, surely they are better than nothing at all.

Second, Angel and Calo chastise the taxonomic approach as vague and too broad. Yet, their conception of privacy is exceedingly vague and potentially very broad, depending on how key components of it are defined. In some interpretations, their conception of privacy would seemingly encompass most information-based harms.

165. *Id.* at 553 (footnote omitted).

166. *Id.* at 511.

167. *Id.* at 553, nn. 263–64.

168. Angel and Calo could readily have drawn from a much more diverse array of scholars for vulnerability and power, such as Oscar Gandy, Jr., Mary Anne Franks, Khiara Bridges, Anita Allen, Simone Browne, Alvaro Bedoya, and others. *See, e.g.*, BRIDGES, *supra* note 112; Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 426 (2017); SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018); OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (2d ed. 2021) (originally published in 1993); SKINNER THOMPSON, *supra* note 112; BROWNE, *supra* note 112; Alvaro M. Bedoya, *Privacy as a Civil Right*, 50 N.M. L. REV. 301 (2020); ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988); Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 YALE L.J. F. 301 (2022). They cite some of these scholars elsewhere in their essay but oddly fail to include them in support of their conception of privacy.

The key part of their definition must be "observation" because the other components are nearly limitless. What is an "unbalanced information relationship"? Most of life involves relationships between humans, machines, or organizations. The requirement of "relationships" thus does not do much limiting work at all. Most relationships involve information, as it is hard to have a relationship without any information being known or exchanged. Rarely are relationships entirely balanced. Do Angel and Calo mean any information asymmetry, even if slight? And why must there be an imbalance for privacy to be violated? Suppose a person discloses on social media highly offensive personal secrets about their ex-spouse. Under Angel and Calo's definition, it is unlikely that this disclosure would be a privacy violation because the spouses share information about each other, so they might not be in an "unbalanced" information relationship.

Angel and Calo also fail to define "vulnerable" or "powerless." By "powerless," they surely do not mean completely powerless, as it is rare that people are totally powerless. Angel and Calo must have some kind of power inequality in mind, but it is not clear where the line is. Nearly all relationships involve power and rarely is power equally distributed. Most relationships will be unbalanced and will render people vulnerable or reduce their power to at least some degree.

The main work in Angel and Calo's concept is done by the word "observation." Without this element, their conception would involve nearly everything. But what is an "observation?" Surprisingly, given Angel and Calo's strong desire for clear boundaries, they do not define "observation."

In today's world of AI and digital technologies, it is not readily apparent what "observation" means. Does "observation" imply that a human is observing? Can a machine observe? Can a surveillance camera really observe? Or must a human be watching? According to the Merriam-Webster dictionary, observation means "to watch carefully especially with attention to details or behavior for the purpose of arriving at a judgment."[169] The Cambridge Dictionary defines observation as "the act of watching something or someone carefully."[170] Neither definition seems to be very precise, and neither helps much in answering the key questions about the meaning of "observation" in today's age of digital technologies and AI. In fact, the definitions add ambiguity to "observation" because they indicate that the observation must be done "carefully." When is observation careful? What does observation entail? Clearly, it involves watching people. Does an "observation" encompass the collection of personal data by a machine? Does it encompass the analysis of

169. *Observation*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/observe [https://perma.cc/K3NM-KGRN].

170. *Observation*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/observation [https://perma.cc/HEL8-J7FV].

personal data? The aggregation of personal data? Using personal data to make inferences about people? Using personal data to make decisions about people? The transfer or sharing of personal data?

If Angel and Calo are attempting to define "observation" broadly to encompass not just data collection but also all forms of data processing, use, analysis, retention, and so on, then the word "observation" is not doing much work in maintaining the boundaries of privacy. It is unclear what, if anything, in my taxonomy would not fall under their definition, which would be incredibly broad. If observation means "doing anything with information," then their definition means doing something with information in an unequal information relationship that involves vulnerability and power on the part of individuals. The two problems that Angel and Calo use as examples of the overbroad taxonomy—information-based discrimination and algorithmic manipulation—both would seemingly fall into their own definition.[171] But so would nearly everything.

But I doubt this is what Angel and Calo want. They are critiquing the taxonomy for being too inclusive. Therefore, their definition of "observation" is probably narrower—perhaps they mean information gathering or surveillance. But if narrowed in this way, their definition risks being too narrow. Indeed, I placed "surveillance" as one of sixteen different types of privacy problem in my taxonomy, as it is much narrower than the umbrella term "privacy."[172] Most of the Fair Information Practice Principles (which have long been heralded as the basic building blocks of privacy law) are not about observation.[173] These principles involve transparency, data quality, restriction of secondary use, purpose specification, data minimization, and so on. They are mainly about the processing, use, and transfer of data. It is doubtful that "observation" includes data analysis, aggregation, inference, or other activities, as they do not fit with the definition of the word.

The most glaring omission from Angel and Calo's privacy tent is disclosure. Under Angel and Calo's view, the act of disclosing personal data about someone is not a privacy violation because it does not involve observation. Ironically, according to Professor Bellin's essentialist definition, privacy is disclosure. Who is right? Angel and Calo? Bellin? How are we to decide? Like Angel and Calo's definition, Bellin's definition also does not rest on any authoritative sources. The taxonomic approach has the dexterity and breadth to include both observation and disclosure; in contrast, essentialist conceptions force us to choose. In today's digital age, it seems obvious that privacy problems

171. Angel & Calo, *supra* note 9, at 524.

172. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 106–12.

173. Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 953 (2017); Robert Gellman, Fair Information Practices: A Basic History (Jan. 26, 2021) (unpublished manuscript) (on file with author).

involve data collection through observation or other means, the disclosure of personal data, and the use and analysis of personal data. Privacy is implicated throughout the entire data lifecycle. The essentialist conceptions focus narrowly on particular parts of the data life cycle and omit the others. Privacy law and policy should not be limited by these narrow and incomplete conceptions; they should address the entire data life cycle, not just part of it.

Attempts to define privacy *per genus et differentiam* have all failed because they end up being too narrow and too broad.[174] Angel and Calo try to navigate the difficulties of the *per genus et differentiam* approach by having a fusion between a narrow part (observation) and a broad part (unequal information relationships that render people vulnerable or powerless). The problem is that their definition of privacy is really just shifting from the vague label of "privacy" to other vague terms such as "observation," "vulnerability," "powerless," and "unbalanced information relationships." These undefined terms are just as vague as "privacy." If interpreted narrowly, they will exclude many things that are routinely and rather uncontroversially considered to be about privacy, such as the use, analysis, disclosure, and sharing of personal data. Their definition would exclude from law and policymaking a recognition of many of the most important problems of privacy we face today—the gathering of massive quantities of personal data in computer databases, the extensive analysis of this data and production of inferences by algorithms, the disclosure through sales of this data and otherwise, and the multifarious uses of this data. All of these things seem to be beyond "observation," which appears to focus very narrowly on data gathering. With this definition, courts will likely fail to recognize many privacy harms and decide cases in a worse way than by using the taxonomic approach.

Consider the problem of deep fakes, which are "audio or visual material digitally manipulated to make it appear that a person is saying or doing something that they have not really said or done."[175] Deep fakes fall outside of the boundaries of many traditional conceptions of privacy. Deep fakes do not involve true information about people—they are false. They are not revealing any true private facts about people, not disclosing secrets, and not breaching confidentiality. They do not involve observation, so they would not fit into Angel and Calo's conception. But deep fakes bear many similarities to privacy problems. In the taxonomy, many deep fakes would be a form of "distortion," a type of problem that involves "the manipulation of the way a person is perceived and judged by others."[176] It is fruitful to examine and discuss distortion along with other privacy issues:

174. Solove, *Conceptualizing Privacy*, *supra* note 5, at 1085–96; SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 14.

175. Mary Anne Franks & Ari Ezra Waldman, *Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions*, 78 MD. L. REV. 892, 893 (2019).

176. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 7, at 160.

> Distortion, like disclosure, involves the spreading of information that affects the way society views a person. Both distortion and disclosure can result in embarrassment, humiliation, stigma, and reputational harm. They both involve the ability to control information about oneself and to have some limited dominion over the way one is viewed by society.[177]

It is thus not arbitrary that so many privacy laws include protections against distortion. Many privacy laws give individuals a right to correct inaccuracies in their records.[178] Correct records is also one of the Fair Information Practice Principles, which have influenced privacy laws around the world.[179] One of the four privacy torts that developed based on Warren and Brandeis's article, *The Right to Privacy*, is the tort of false light.[180] Deep fakes often create harms that are similar to the types of harms that many privacy problems cause—embarrassment, reputational injury, loss of control over one's personal information, and dignity harm, to name a few. Of course, deep fakes might not be purely about privacy, but they bear enough resemblance that it is fruitful to include them in the tent.

Additionally, deep fakes are a form of "appropriation," another type of privacy harm in the taxonomy.[181] Appropriation of name or likeness is one of the four privacy torts inspired by Warren and Brandeis's article.[182] In fact, the tort was the first privacy tort created after the article.[183] The harm of appropriation is exploitation of a person's identity.[184] In most appropriation

177. *Id.*

178. *E.g.*, 5 U.S.C. § 552a(d)(2); 20 U.S.C. § 1232g(a)(2); Commission Regulation 2016/679, art. 16, 2016 O.J. (L 119) 1 (EU).

179. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS xx–xxiii (1973).

180. RESTATEMENT (SECOND) OF TORTS § 652E (A.L.I. 1977)

181. For more on deep fakes and an attempt to classify them in the taxonomy, see Benjamin L.W. Sobel, *A Real Account of Deep Fakes*, 124 MICH. L. REV. (forthcoming 2026). Sobel concludes that deep fakes fit most closely with appropriation but ultimately do not fit precisely into any category of the taxonomy. While I find some of his account of the problem of deep fakes compelling, he views the problem of deep fakes a bit too singularly and focuses mainly on a small percentage of deep fakes that do not fit. The result diminishes the recognition of harm with other deep fakes. The best approach, in my view, is to explore deep fakes in a more bottom-up way and recognize that they can cause many different problems and might not neatly fit into one category.

182. RESTATEMENT (SECOND) OF TORTS § 652C (A.L.I. 1977) [hereinafter TORTS § 652C].

183. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 23–24 (8th ed. 2023).

184. TORTS § 652C, *supra* note 182, cmt. a (the appropriation tort protects "the interest of the individual in the exclusive use of his own identity"); *see also* JESSICA LAKE, THE FACE THAT LAUNCHED A THOUSAND LAWSUITS: THE AMERICAN WOMEN WHO FORGED A RIGHT TO PRIVACY 57–69 (2016) (discussing the history of one of the earliest appropriation cases that led to the enactment of the first privacy tort law in New York in 1903); Jonathan Kahn, *Bringing Dignity Back to Light: Publicity Rights and the Eclipse of the Tort of Appropriation of Identity*, 17 CARDOZO ARTS & ENT. L.J. 213, 213–14 (1999) ("[A]ppropriation of identity involves the personal right to privacy . . . . [P]rivacy rights protect and vindicate less tangible personal interests in dignity and integrity of the self.").

cases, the interest is not about concealing secrets or even protecting against damaging facts. Many appropriation cases involve uses of a person's name or likeness that are not embarrassing or reputationally harmful. The problem is that people's identities are commandeered by others and used in ways beyond people's control, which is exactly what deep fakes do.

Ultimately, deep fakes might not fit precisely into one category of the taxonomy. Professor Benjamin Sobel points to deep fakes that have a disclaimer that they are fakes or that are obviously fakes. He contends that this category of deep fakes would fall outside of the distortion category in the taxonomy.[185] Although deep fakes that are not convincingly deceptive might not be a form of distortion, they still are a form of appropriation. Consider deep fakes depicting victims naked or having sex—perhaps the most common type of deep fake. Professors Mary Anne Franks and Ari Ezra Waldman aptly contend that "digitally manipulated pornography turns individuals into objects of sexual entertainment against their will, causing intense distress, humiliation, and reputational injury."[186] This type of injury—turning people into objects of entertainment against their will—is at the core of the harm of appropriation and therefore privacy.

Deep fakes thus have substantial similarities to appropriation. If deep fakes are deceptive, as most are, then they also are a form of distortion. These similarities are helpful because they aid us in understanding the problems with deep fakes. The consequences of including deep fakes in the privacy tent are that they will be discussed alongside other privacy issues. Existing privacy laws might be used to address the problem, or new privacy laws might be crafted to address the problem. Privacy scholars might write about the problem, as noted privacy scholars Danielle Citron and Ari Waldman did.[187]

Although there are many reasons why including deep fakes would be productive, it remains unclear what the benefits would be of exclusion. Angel and Calo have not explained why excluding issues like this would improve thinking about issues or how it would lead to better law and policy.

Ironically, despite their quest for precision, clarity, and clear boundaries, Angel and Calo's attempt at an essentialist definition fails to achieve these goals and ends up performing worse than the taxonomic approach. Angel and Calo's conception creates the illusion of clear boundaries. At least the taxonomic approach directly acknowledges it is open-ended, has blurry boundaries, and is expansive. The taxonomic approach also advances ways to determine whether particular problems should be included in the privacy tent—social recognition,

185. Sobel, *supra* note 181, at 29–37.

186. Franks & Waldman, *supra* note 175, at 893.

187. Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1753–54 (2019); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OP. PSYCH. 105, 105–09 (2020).

family resemblances, and analogical reasoning. In contrast, Angel and Calo supply no real criteria, no indication of which sources should be consulted, and no approach to determining what should be included or excluded beyond their own assertions.

In contrast to the essentialist approach, the taxonomic approach is more democratic about the determination of the boundaries. As Angel and Calo note in their essay, others can use the taxonomic approach without being tethered to the particularities of my taxonomy.[188] Anyone can propose additions or subtractions.

Additionally, the taxonomic approach is more flexible and evolving. Angel and Calo's essentialist conception appears to be a definitive conception of privacy, one that does not appear to be open to any change over time. The taxonomic approach recognizes that privacy is historically and culturally contingent and that the concept of privacy is evolving. In contrast, Angel and Calo do not indicate how their concept would evolve, and they state their conception without any historical or cultural context, as if it is the definitive meaning of privacy beyond culture and time. The taxonomic approach rejects such thinking; privacy is a dynamic concept, forged by social practices, attitudes, and changing technologies.

B. *The Functional Account of Privacy*

Angel and Calo alternatively propose what they call a "functional" account of privacy. Angel and Calo write: "Recent scholarship has embraced a *functional* account of privacy that defines the field in terms of the specific set of problems privacy exists to address. Rather than define privacy per se, socially or otherwise, this approach interrogates what privacy is 'for.'"[189]

Angel and Calo point to various academics who make arguments that privacy advances values such as respect, love, trust, liberty, autonomy, selfhood, identity, and freedom, among other things.[190] However, when discussing what privacy is for or why privacy matters, these scholars are arguing about the *value* of privacy, not about the *definition* of privacy.

Many things advance these interests beyond privacy. For example, privacy may be necessary for freedom, but this does not mean that privacy is freedom or that freedom is how to distinguish privacy from other things. I struggle to follow Angel and Calo's functional approach—it seems to rest on conflating what privacy *is* with what *values* or *aims* privacy facilitates.

188. Angel & Calo, *supra* note 9, at 521.

189. *Id.* at 554.

190. *Id.* (citing Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013); NEIL RICHARDS, WHY PRIVACY MATTERS 141 (2021)).

There are many things beyond privacy that lead to identity, freedom, and selfhood. Angel and Calo beg the question when they say that we can define privacy based on what it is for. Many things contribute to democracy and freedom, so either under their view everything that leads to democracy and freedom is privacy (which is absurd and would make privacy about nearly everything) or that privacy is X, which contributes to democracy and freedom. But that begs the question: What is X?

The functional approach—looking at what privacy is for—would make privacy about everything, as privacy can facilitate nearly anything, both good and bad. Privacy is essential for democracy. It is also helpful to criminals. Privacy even facilitates things it can conflict with, such as free speech.[191]

Ultimately, the functional approach is not a definition of privacy. It does not address the issue of conflicting values. Nor does it tell us much about what should be admitted into Angel and Calo's privacy club and what should be excluded.

V. THE GROWTH OF THE PRIVACY LAW FIELD

Despite my disagreements with Angel and Calo's thesis, I find their discussion of the development of scholarship about privacy law to be quite insightful. They chronicle how thinking about privacy has evolved and how different scholarly ideas relate to each other. This kind of work is fruitful, as it leads to a richer understanding of the various problems scholars have been trying to tackle. Understanding the evolution of thinking about privacy is a useful and productive endeavor, as such thinking has evolved as more scholars have entered the field and technology has advanced at an exponential pace.

Angel and Calo note that the "big-tent taxonomic approach" has "facilitated the growth and proliferation of privacy scholarship."[192] Despite constituting a plurality of different things, privacy is still a coherent concept and a coherent focus for law, policy, and scholarship. Privacy is a *field*, not just a topic.[193]

Privacy law scholarship can enrich judicial, legislative, and policymaker understandings of privacy and facilitate a more robust recognition of privacy problems. For this to happen, practitioners, policymakers, advocates, and academics must engage in a shared discourse and have productive interdisciplinary conversations.

191. NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 3 (2015).

192. Angel & Calo, *supra* note 9, at 529.

193. As a field, privacy law is still in the process of developing and being recognized. In practice, most large law firms now have sizeable privacy law practice groups, and many professionals in law and other areas now call themselves "privacy professionals."

This discourse has been greatly aided by the big tent of the privacy field. We are living in the digital age, and so much of the world today revolves around personal data and technology. For many people exploring these issues, often the closest home—and sometimes the only home—has been privacy. And so, they came to the privacy tent. So far, the discussion has been fruitful, interesting, and impactful. Professor Woodrow Hartzog aptly observes that under the taxonomic approach:

> [P]eople in politics, commerce, and society can work to solve complex information problems without constantly relitigating privacy's meaning. Instead of squabbling over the binary boundaries of privacy, people who understand privacy as more of a vague umbrella term can leave the line-drawing question for another day and get to work identifying problems created by specific conduct, articulating the values implicated by those problems, and crafting solutions to the problems that serve those values.[194]

Angel and Calo acknowledge that the big tent helped facilitate many of these developments. Ironically, their essay makes compelling arguments to support the taxonomic approach. They note how the field has grown, how the big tent has nurtured many scholars, enabled a rich tapestry of ideas to flourish, and resulted in a productive discourse. Angel and Calo write: "This pluralist, pragmatic approach opened the door to a shift in emphasis from defining to doing, as well as the broadening of privacy to encompass information-based harms such as discrimination and algorithmic manipulation."[195] This sounds like a success.

I thus strongly resist Angel and Calo's call to raise the gates. I do not see a problem. Instead, Angel and Calo urge a return to an approach that has long failed. They have not shown how the essentialist approach will enrich scholarly conversations, increase diversity of scholars and perspectives, or improve law or policymaking.

Ultimately, the essentialist approach stems not from any actual problems but from a deep-rooted desire for certainty, clarity, and authority. But these things are illusory. We live in a world of fog.[196]

194. Hartzog, *What Is Privacy?*, *supra* note 12, at 1681.

195. Angel & Calo, *supra* note 9, at 552.

196. I am reminded of the wonderful and hilarious essay by William Prosser about fog. William L. Prosser, *Lighthouse No Good*, 1 J. LEG. EDUC. 257 (1948) (analogizing legal confusion and obscurity to fog).

CONCLUSION

I greatly appreciate Angel and Calo's thoughtful engagement with my work. Although I disagree with them, their article raises many interesting points, and I have enjoyed this opportunity to think further about these issues.

Where Angel, Calo, and I share common ground is that we have a strong conviction that a deep theoretical understanding of privacy matters. Our disagreement stems from method; they adhere to the essentialist approach, and I believe the essentialist approach is doomed and that the taxonomic approach is better.

Although the taxonomic approach involves a bottom-up analysis of similarities and differences, it is not anti-theoretical. Theory is essential to understanding privacy problems. The taxonomic approach shifts theorizing about privacy from an obsession over the umbrella term "privacy" toward the more specific things under the umbrella.

Angel and Calo certainly demonstrate that it is fruitful to revisit the taxonomy. My thinking about privacy began about twenty-five years ago, and I published the first part of the taxonomic approach in 2003 and the taxonomy in 2006. A lot has happened in nearly twenty years, and I would not propose an identical taxonomy today. For the most part, I would probably continue to include the problems I included. Some problems might be further distinguished, split into two or more separate problems. I would probably add problems. Over the past twenty years, as Angel and Calo have quite compellingly documented, many new voices have entered the field. They brought many thoughtful insights, so of course, all these new voices would further enrich the taxonomy were I to update it today.

In the end, Angel and Calo's critique reminds me of Franz Kafka's story, *A Hunger Artist*, where a person at a carnival starves himself.[197] Toward the end of the story, he is asked why he performs his starvation act. He is not starving to entertain people. Instead, he says that he does not eat because he has not found the food he liked. *A Hunger Artist* is a fitting story to describe Angel and Calo's quest for an essentialist conception of privacy. They want food that does not exist. They want firm sources of authority and clear boundaries, but they are unable to propose a concept with these things despite their valiant efforts. They thus push away the food the taxonomic approach has offered, despite their recognition that it is quite nourishing.

At the end of Kafka's *A Hunger Artist*, after the artist has perished, a panther is placed in his stead. The panther is content to eat the food it is given. This, perhaps, is the closest thing to a happy ending in Kafka. We can be hunger artists or panthers, and I humbly cast my vote for the panthers.

197. FRANZ KAFKA, *A Hunger Artist*, *in* FRANZ KAFKA, THE COMPLETE STORIES 268 (Willa Muir & Edwin Muir trans., 1971).