DRAFT PAPER UNDER REVISION – DO NOT CITE OR DISTRIBUTE

Theorizing Privacy's Contestability: A Multi-Dimensional Analytic of Privacy

Deirdre K. Mulligan, University of California at Berkeley
School of Information
(dkm@ischool.berkeley.edu)
&
Colin Koopman, University of Oregon
Department of Philosophy
(koopman@uoregon.edu)

§1: In Defense of Contestability

The concept of privacy, despite its centrality for contemporary liberal democratic cultures, remains remarkably contested. Privacy claims are asserted to defend a diverse range of interests, from an equally diverse set of harms, in nearly every realm of daily life. Given the frequency and intensity with which privacy is invoked, many find the uncertainty and disagreement about its meaning and purpose jarring. Some argue that the extent of disagreement evidences privacy's waning utility and meaningfulness for contemporary life.[1] Others, while believing privacy important are frustrated by the lack of clarity about its meaning—particularly its purpose and justification. Businesses and engineers who, in part due to repeated privacy failures, find themselves tasked by regulators with designing privacy into products and services claim that the ambiguity, and at times social schizophrenia, of privacy combined with a lack of principles, mechanisms, and models hampers such efforts.[2] Surely a concept called upon to protect individuals' thoughts, bodies, and relationships, and viewed as essential to civil society, democratic governance, as well as the textures of moral life should have a settled meaning, or a set of settled meanings with clear relations. If it is conceived as a requirement for technical systems, surely it should be well understood, defined and modeled. Yet, this is not the case.

There is scant agreement amongst scholars within and across disciplines, practitioners, and policy makers about what privacy entails, what privacy applies to, what justifies privacy, and what privacy means. The scholarly literatures on privacy law, privacy policy, and the morality of privacy present an almost dizzying array of diverging and often conflicting theories, conceptualizations, and analyses of privacy. These scholarly debates reflect much wider and more heated contestations over privacy in contemporary culture. Thus, sociologist Alan Westin, in a landmark 1967 book that helped usher in a new age of thinking about privacy penned this

---

[1] The most famous or infamous statement to this effect was made by Scott McNealy, former CEO of Sun Microsystems, who proclaimed, "You already have zero privacy—get over it." Amitai Etzioni, "Privacy Isn't Dead Yet," New York Times, April, 6, 1999, p. editorial.

[2] See, Stuart S. Shaprio, "Privacy by Design: Moving from Art to Practice," COMMUNICATIONS OF THE ACM VOL. 53 NO. 6 pp. 27-29 JUNE 2010, (explaining the gaps between privacy and design, "Supporting the translation of abstract principles, models, and mechanisms into implementable requirements, turning this into a repeatable process, and embedding that process in the system development life cycle is no small matter. Security has been at it a lot longer than privacy, and it is still running into problems. But at least security has a significant repertoire of principles, models, and mechanisms; privacy has not really reached this stage yet.") Id. at 29; Deirdre K. Mulligan and Jennifer King, "Briding the Gap between Privacy and Design," 14 U.Penn. Con. L.J. 989 (2012) (providing an overview of the rift between privacy by design as envisioned by regulators and privacy by design tools for use by system and product designers).

disturbing thought: “Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists.”[3] Philosopher of law Judith Jarvis Thomson, in a 1975 article expressing some skepticism about the coherence of the very concept itself, wrote that: “the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.”[4] More recently, legal theorist Daniel Solove in a 2008 book reflecting on privacy concerns arising due to another wave of socially-destabilizing technologies, claims that privacy “is a concept in disarray.”[5] Summing up the general tenor of much of the discussion about privacy over the past few decades, legal theorist Robert Post wrote in 2001: “Privacy is a value so complex, 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.”[6] Focused attention to privacy as a potential subspecies of engineering is a relatively recent development. Recent work examining the concepts of privacy used in computer science research documents a similar disarray. However, in contrast to law and ethics where competing notions of privacy are acknowledged and debated, within sub-disciplines of computer science researchers use competing definitions of privacy often with little explicit or implicit recognition that one definition, among many, is being chosen, or how researchers in other sub-disciplines conceive of the problem.[7] While this leads to a range of technical solutions, it’s unclear how well any assemblage of them aligns with what individuals would recognize as privacy in a given context.[8]

---

[3] Westin 1967, 7
xxxWestin, Alan. 1967. *Privacy and Freedom*. New York: Antheneum, 1967.
[4] Thomson 1975, 295
xxxThomson, Judith Jarvis. 1975. “The Right to Privacy” in *Philosophy and Public Affairs* 4, no. 4, Summer, 1975: 295-314
[5]Solove 2008, 1
xxxSolove, Daniel. 2008. *Understanding Privacy*. Cambridge: Harvard University, 2008.
[6] Post 2001, 2087
xxxPost, Robert. 2001. “Three Concepts of Privacy” in June, 2001 89 Geo. L.J. 2087.xxx: 2087-2098.

[7] Seda Gurses and Claudia Diaz, “Two tales of privacy in online social networks,” under submission, IEEE Security & Privacy (2013) (discussing privacy as surveillance, as boundary negotiation (social privacy), and as controls over institutional use of data (institutional privacy)) (http://www.cosic.esat.kuleuven.be/publications/article-2270.pdf).; see Mulligan and King discussing HCI work that explores privacy as control and privacy as boundary negotiation.

[8] Accord, Gurses and Diaz, (discussing range of tools flowing from multiple concepts, but limitations from fragmented approach).

It is not an overstatement, we think, to say that the very concept of privacy is today everywhere contested. These contests run in multiple directions and at varying levels of complexity. Troublingly, at times contests over privacy's meaning are under appreciated and eclipsed by arguments about whether privacy is relevant at all, for lack of tools to adequately distinguish one competing concept of privacy from another. The easiest contests to discern and address center on the applicability of some concept of privacy in a given situation: whether it ought to apply, and if so, how.

Our interest lies in other sorts of contests—those that go to the heart of the concept of privacy itself. These contests over privacy are essential to its work in the world for it is what W.B. Gallie called an "essentially contested concept"—one whose proper use "inevitably involves endless disputes that "*cannot be settled by appeal to empirical evidence linguistic usage, or the canons of logic alone.*"[9] A concept is essentially contested where disputes about its "essence or central meaning" are both paramount and central to the term itself. In claiming privacy as an essentially contested concept we therefore contend that contests about privacy and the ambiguity of meaning they simultaneously rely upon and beget are essential to its meaning.[10]

Given that privacy cuts so much to the heart of our moral, political, legal, and cultural self-understandings that we cannot but disagree over its meaning, application, implementation, and justification, this may hardly seem a bold claim. For of course, the attendant debates surrounding privacy, while often frustrating, are prime evidence of our culture productively negotiating what privacy means and requires in rapidly changing social contexts. However, the

---

[9] W.B. Gallie, Essentially Contested Concepts, 56 Proc. Aristotelian Soc'y 167 (n.s. 1955-56). We are not the first to attach Gallie's concept to privacy, however, we are the first to fully plumb its significance. See, Colin Bennett & Rebecca Grant, Visions of Privacy: Policy Choices For The Digital Age 5 (1996) (stating that "privacy is a deeply and essentially contested concept"); James B. Rule, "Privacy Codes and Institutional Record Keeping: Procedural versus Strategic Approaches, 37 Law , &, Soc. Inquiry 119, 123 (2012) (Privacy is, thus, one of what philosophers term "essentially contested concepts" whose implications for practice are bound to be disputed in any real-world setting.); Lawrence Lessig, *Understanding Changed Readings: Fidelity and Theory*, 47 Stan. L. Rev. 395 (1995).

[10] As Jeremy Waldron explained "contestedness is part of the very meaning of the expression in question: it is part of the essence of the concept to be contested." Jeremy Waldron, "Vagueness in Law and Language: Some Philosophical Issues," 82 Cal. L. Rev. 509, 529 (1994) (explaining that essentially contested concepts such as freedom do not prevent people from taking a stand on meaning but rather they demand a recognition that others may have equally strongly held, yet different perspective on the concepts meaning, "anyone who says that "freedom," for example, has a perfectly clear meaning and that he cannot see why so many people get it wrong, shows that he himself does not understand the most striking rule for the use of "freedom" in the modern world - namely, that it is a verbal arena in which we fight out our disagreements about the nature of human agency and autonomy.) Id.

implications of this claim are large and warrant examination and action. Waldron is again useful here, he explains with respect to the term "art" that "the definitional dispute enriches the wider debate in which the disputed concept is deployed…The dynamics of that debate - putting forward views, citing and assembling examples, responding to rival views with arguments and counter-examples, modifying one's view to meet exceptions, explaining why it is still coherent even after modification, developing schools of thought which evolve partly in response to internal dynamics and partly in response to rival pressures, locating each view in a history and heritage of disputation, opening one's aesthetics in various ways to contributions from other spheres of life and thought, relating one's aesthetics to rival conceptions of the good life for those endowed with talent, and so on - results in any modern claim about the nature of art being considerably richer and more subtle than it would have been if the claim had issued straightforwardly from an historically unchallenged consensus."[11] As with art, we would not advance privacy, or our understanding of it, by winnowing out competing definitions or creating more precise meanings. The persistent disagreement surrounding privacy and the debates that ensue are necessary for continued understanding and deployment of privacy in political and social debates. As Waldron so aptly framed it "knowing where we stand may not be the point of the provision. Instead, the point may be to ensure that certain debates take place in our society…"

For privacy we believe this is so: the debate it promotes, rather than its resolution in any given instance, is what is of most value to society. The contestability of privacy, in this narrative, is not a flaw to be rooted out or winnowed down, but rather an essential element that keeps privacy robust in the face of ongoing change. Through these iterative contests society affirms privacy's continued relevance, and enriches and deepens our understanding of its value.[12]

Privacy's disorder—its ambiguity, its vagueness, and the underlying contestability—makes it a difficult notion to work with. Such difficulties have prompted many legal theorists, philosophers, and privacy practitioners to ask: *how* can the contemporary contestability of privacy be overcome? Despair in the face of disarray is certainly understandable given the

---

[11] Jeremy Waldron, Vagueness in Law and Language: Some Philosophical Issues, 82 Cal. L. Rev. 509, 532 (1994)

[12] Accord Waldron, ("We do not agree on many things in our society, but perhaps we can agree on this: that we are a better society for continuing to argue about certain issues than we would be if such arguments were artificially or stipulatively concluded.") Id. at 540.

importance of privacy for contemporary liberal culture. While appreciative of the difficulties privacy in all its messiness poses, we argue that despair is neither a rationally warranted response nor a culturally, politically, or legally viable way of moving forward amidst our uncertainty, and that efforts to reduce contests about privacy's meaning and application are misguided and counterproductive. We propose an alternative method for addressing privacy's predicament.

While we share the frustration that motivates efforts to reduce or simplify privacy, we argue that enriching our capacity to leverage privacy's richness and vitality—not attempting to pare it down—is both the pragmatic, and intellectually honest, response. Our work is motivated by a simple claim that privacy's contestability, along with the vagueness and ambiguity attendant to any contest within a space of conceptual plurality, should be regarded as an asset rather than a liability. While embracing contestability, our work repositions privacy's so-called disarray, finding it not to be an inherent property of the concept itself, but rather a result of insufficient effort to explicate its complexities.[13] Through our work we aim to shift the conversation about privacy, from ruminations about its disarray to critical examinations of the full array of privacy's workings.

Privacy's contestability is only a positive feature, to the extent that tools (theoretical, legal, technical) are available to expose the multiplicity of our many concepts of privacy in their contest with each other, and facilitate their productive use. Such tools ideally will make concepts of privacy analytically available for nuanced interrogation, both individually and in relation to one another.

Below we propose a privacy analytic to advance this goal. Our multi-dimensional analytic allows privacy's many meanings to be deftly leveraged, and in doing so create a bridge between privacy theory and privacy practice. With efforts, like our analytic, scholars and practitioners can work to reveal and leverage the inter-related array of privacies currently perceived as disarray. While the array may surely be more difficult to handle than a single unified theory or concept, it does not signal incoherence. It is a source of responsiveness, generativity, and dynamism. Fruitful deployment of privacy to serve our ever-evolving needs

[13] We are distinguishing between disarray which results from a lack of understanding of the various concepts of privacy, and contestability which requires both a concept with an open texture and the actual existence of multiple competing concepts.

requires tools that allow us to tap into the latent power of the multiplicity of privacy rather than be stymied by it.[14]

Our analytical framework for understanding and engaging privacy has several potential benefits. Positively, such a framework advances our ability to deploy privacies across many situations as the need arises. The analytic of privacy we propose makes privacy understandable, such that we can do what we need with and for privacy.[15] Through delineation, categorization, and relationship modeling we can push back on misguided, if understandable, efforts to whittle down privacy to some essential core and simultaneously bring privacy pluralism more effectively into practice. Thus, our sense of the positive value of a multi-dimensional approach is that it is useful for analyzing the operations (both intended and actual) of privacy in many settings or, in other words, clarifying and realizing the functioning of privacy in law, system design, and a range of other practices. Our analytic can function both descriptively and prescriptively to assist our understanding of privacy problems as well as helps structure regulations, policies, and design choices meant to address them. A few examples illustrate this point.

Descriptively, one might use our analytic to map privacy complaints lodged by users of social network sites—this could provide a deeper understanding of the range of harms perceived as privacy violations and how those harms both resemble and diverge from each other. Another descriptive effort could involve the creation of a relational map of the contemporary theoretical landscape of privacy—this would help with an examination of the connections between claimed privacy harms and privacy theories. Prescriptively, one might use the analytic much as a computer security professional uses threat modeling—the analytic provides a structured approach to support the systematic identification and clarification of the risks to privacy the technical designer, legislative drafter, or privacy professional (for example) cares about (or should care about).

---

[14] We take Pamela Samuelson's efforts to map the plurality of the public domain as a similar exercise aiming to offer "deeper insights about public domain values", the "many positive functions" it plays in society, and "how and why to preserve and protect" it. Samuelson at 826-827. Need citexxx

[15] James B. Rule notes the gulf between commitments to privacy as a value and determining what is necessary to protect it in any given instance. James B. Rule, "Privacy Codes and Institutional Record Keeping: Procedural versus Strategic Approaches, 37 Law , &, Soc. Inquiry 119 (2012) ("The emerging law on privacy of institutionally held personal data may indeed be part of what Selznick terms a "realm of value," but affirming the validity of values in such broad terms does not help much in adjudicating specific claims and counterclaims that make up the flux of privacy controversies.") Id. at 124.

From both of these descriptive and normative perspectives, interrogating the nuances of what is meant to be protected by privacy in a given setting—who poses a threat to it, the actions they might take and from whom it ought to be protected, for example—is essential to considering the kind and scope of protections that could be usefully deployed and the justifications that support them. The absence of such a multi-dimensional approach has led to technical systems and legal codes that purport to protect privacy but fall short. This explicates our primary positive interest here: uncovering the richness of what individuals experience and theorists conceptualize as privacy wrongs or violations, and thereby facilitating more meaningful debate and action around privacy.

Our multi-dimensional analytic responds to a number of potentially pernicious effects of contestability.[16] First, to the extent that contestability stymies action (legislative, regulatory, and standard setting) to protect privacy that is decreed too fickle, too personal, and too underdetermined, our analytic allows participants to more finely map areas of disagreement and consensus. Second, it is routinely observed that wrongs experienced on the ground as privacy violations go orphaned because there is little connecting extant theories of privacy to its current realities, and experiences of harm to legal remedies.[17] The relationships between distinct concepts of privacy while claimed are, at best, thinly documented. The absence of an overall framework in which to situate distinct concepts, consider their interrelations and their relations to claimed violations, stymies efforts to apply, leverage, and extend privacy protections. Third, it is expected that privacy may wither. Bandied about but never richly mapped, privacy becomes easy to devalue and less likely to evolve and extend. Precisely when contests over privacy are most severe—where there is both a perceived need for privacy and a lack of agreement on what might count as fulfilling that need—the absence of a detailed understanding of the many contours of the concept may be its downfall. Addressing these concerns about privacy's ambiguity and vagueness provides an additional motivation for our efforts here to more fully analyze privacy's plurality.

---

[16] Samuelson notes the key drawback to maintaining a diversity of definitions of the public domain is that it exposes those who rely on the term to legal liability from misunderstanding of the subtleties of the definition in a specific context. At 831.

[17] Reidenberg, Hastings privacy symposiumxxx

Providing rigor to our understanding of what we mean when we talk about privacy is essential given its heightened importance in an increasingly networked, informationalized, and programmed society. James B. Rule noted, "Widespread convictions that the state should act to protect (any essentially contested concept)…normally mask profound clashes of public sentiment as to what policies in fact would serve such broad values. It is always much easier to agree that "something must be done" to protect widely regarded values than it is to recognize what practices authentically serve those ends."[18] What we mean by privacy and what we can demand of the government and ourselves in its name will be of increasing importance as the social embedding of computers, networks, and other informational technologies, and changing social and organizational expectations of data use escalates the contestability of privacy itself. Our analytic seeks to facilitate a richer analysis of operative concepts of privacy. Our belief is simply that we cannot use privacy to its capacity if we do not fully understand its rapidly evolving contours.[19]

---

[18] James B. Rule, "Privacy Codes and Institutional Record Keeping: Procedural versus Strategic Approaches, 37 Law , &, Soc. Inquiry 119, 122 (2012).

[19] William Prosser sought to update legal conceptions of privacy in the middle of the twentieth century; see Prosser, William L., 1960, "Privacy" in *California Law Review* 48, no. 3, Aug., 1960: 383-423. Today we again find ourselves at a series of impasses with respect to understandings and operations of privacy in our society. Following Prosser in the project of keeping track of our evolving we of course depart here from his four-part typology of privacy torts. Two recent examples reveal the inevitable evolution of privacy threats and the need for new privacy theories (beyond Prosser, but also beyond others) to satisfactorily address them.

First, the "mosaic theory" of privacy endorsed in Justice Alitos's concurrence in *U.S. v. Jones* and favorably noted in Justice Sotomayor's concurrence in that case, is, as other scholars have noted, a new theory of privacy under the Fourth Amendment developed to respond to the feasibility of twenty four hour surveillance of the population in public areas made possible by advances in technology. See for further discussion Orin Kerr, 2012, "What's the status of the mosaic theory after U.S. v. Jones?", January 23, 2012 http://www.volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/.

Second, the work of scholars such as Sweeney, Malin, and Narayanan and Shmatikov reveals the potent threat to privacy posed by sharing so called anonymized data sets given the growing availability of auxiliary data and tools to support cross-correlation. See, Latayna Sweeney, "Weaving technology and policy together to maintain confidentiality," J. of Law, Medicine and Ethics, 25 (2-3): 98-110 (1997); Bradley Malin and Latanya Sweeney, "How (not) to protect genomic data privacy in a distribute network: using trail re-identification to evaluate and esign anonymity protection systems," J. of Biomedical Informatics," 37 (3): 179-192 (2004); Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset), In Proc. of *29th IEEE Symposium on Security and Privacy*, Oakland, CA, May 2008, pp. 111-125. IEEE Computer Society, 2008. Relatedly, Cynthia Dwork has revealed the equally troubling fact that statistical databases can breach the privacy—ie reveal something about an individual that was not known before—even of individuals whose records are not contained within them. In response to the risks posed by auxillary information Dwork proposes a new goal for privacy "the risk to one's privacy…should not substantially increase as a result of participating in a statistical database," she terms this new concept *differential privacy*. This idea embraces a statistical property that offers a strong privacy guarantee consistent with maintaining the utility of socially beneficial databases. See Cynthia Dwork, "Differential Privacy," International Colloquium on Automata, Languages and Programming (ICALP) 2006, p. 1–12.

§2: Toward Pluralism and Contextualism in Service of Contestability

Our aim is to leverage the positive benefits of privacy's ambiguity to support robust contests over the forms and meaning of privacy society desires and needs today and for the future. To do so, we must understand and relate concepts of privacy at play in theory and practice. This requires an analytic grid that disentangles concepts of privacy along multiple dimensions. Such an analytic should facilitate the process of faithfully documenting the plurality of axes along which privacy travels. Our analytic is thus meant to express a picture of privacy as a *tapestry*, in which many different kinds of fibers are interwoven with one another to form different kinds of complex patterns. Though the full tapestry presents privacy in all its nuance and detail, each region presents a different and internally coherent (or not) picture of privacy. Our claim that there are many 'dimensions' of privacy is thus the claim that there are many kinds of threads (in terms of color, thickness, material, etc.) contributing to the overall fabric of what we know as privacy.

Our focus on privacy's contestability builds directly on a spate of recent efforts in the direction of pluralism and related contextualism about privacy. These efforts are united in their central bid for the idea that privacy is not one thing but many things operating in many contexts. While existing approaches focus on distinguishing many concepts of privacy and many contexts for privacy, our approach is geared toward exposing relationships—similarities and differences—amongst and across these many concepts (in contexts) such that we can better interrogate—and yes, facilitate—contests over privacy, whether they be legal disputes, policy battles, or technical designs countering one another.

Our argument is that privacy should not be reified or concretized at a *wholesale* level but rather left to flexibly operate at the *retail* level allowing various concepts of privacy to be deployed as situations demand. If this is the case, then the most pressing question we face concerns *how* we can approach privacy in such a retail manner. This question concerns what sort of methodology or analytic can assist us in assessing and understanding privacy given a starting assumption that privacy is multiple in its multiple contexts.

The approach we develop below teases apart pragmatic components of the workings of privacy. It contrasts with existing taxonomies that typically begin and end on the semantic level, our taxonomy digs further to give meaning to the term *meaning* itself. We unpack meaning by

decomposing the many elements implicated in existing attempts to conceptualize privacy. This involves a shift from thinking about privacy solely as having many meanings to focusing on constituent elements of those meanings and the contexts in which they operate. Collectively, the many elements of privacy we distinguish help to reveal the complex, multi-threaded intersections and divergences that form the tapestry of privacy.

Philosophically, this point can be made by way of another pragmatist view to the effect that linguistic meaning (or conceptuality) is one aspect of a fuller complex assemblage of human practice (or practicality). This approach is inspired by philosophical pragmatism. It draws on Ludwig Wittgenstein's pragmatist theory of "meaning as use"[20] as well as work by the classical American pragmatist John Dewey and contemporary neopragmatist Robert Brandom.[21] The point of all these pragmatisms is that the content of the concept of privacy is not a mental affair, but rather a practical affair such that privacy has whatever meaning it does in virtue of its complex functionality in the midst of its contexts of operation. Simply put, pragmatism is designed to counter attempts to remove meanings from context—pragmatism pushes philosophers back onto the rough road of words in action and off the smooth ice of abstractions.

Adopting this approach here, we focus on privacy as it is used in practice, as well as how it is articulated in theory, thus shifting the field of analysis to a combined semantic plus pragmatic analysis. Our taxonomy unpacks the semantic understandings of privacy by bridging semantics and pragmatics, or meanings and practices. It maps privacy along a plurality of dimensions both dissecting meaning and adding dimensions that relate contextual experiences of privacy as practiced.

Our work here is in important ways aligned with the work of other privacy scholars to defend privacy against essentialist efforts, and to ground and structure privacy discussions in meaningful and detailed understandings of its many contexts. It will be useful to situate our work vis-à-vis existing precedents of pluralist (i.e., anti-essentialist) and contextualist (i.e., embedded) defenses of privacy.

---

[20] On a pragmatist theory of meaning see Solove (2008, 42ff.) and on "meaning as use" see Wittgenstein (1953, §43).

[21] See my discussion in Koopman 2009, Chapter 4, Dewey (1938), and ; for another related (but importantly different) approach to the priority of pragmatics for semantics in a pragmatist vein see Brandom (1994). xxxKoopman, Colin. 2009. *Pragmatism as Transition: Historicity and Hope in James, Dewey, and Rorty*. New York: Columbia University Press, 2009.

Unpacking Privacy's Many Meanings: Semantic Pluralism

A central precedent for our interest in the plurality of privacy itself is philosopher and legal scholar Anita Allen's argument that, "A plurality of notions and opportunities for privacy must be permitted to flourish."[22] Allen's expressly pluralistic approach accepts that we lack not only a widely-endorsed definition of privacy but also that we do not even have "consensus about what would constitute an adequate definition."[23] If we choose one from among the existing privacy theories we foreclose inquiries that might disclose the changing contours of the privacies we find ourselves in the midst of. Privacy pluralism facilitates the concept's resilience in the context of changed social, technical, and ethical conditions. Recognizing the value of this approach, a number of theorists have followed Allen's lead in exploring the plurality of privacy.[24]

Another important pluralistic precedent for our efforts here is Daniel Solove's recent contribution toward a pluralist approach to privacy.[25] Solove's work helps us understand *how*

---

[22] Allen 1999, 756 check quote

[23] Allen 2003, 489 (xxxcheck quote).

xxxAllen, Anita. 1999. "Coercing Privacy" in *William and Mary Law Review* 40, no. 3, Mar. 1999: 723-757.

xxxAllen 2003 "Privacy" cited above in note 1

[24] See Kasper (2005), Moore (2003), Bennett (2008, 2ff.), Lipton (2010), Gill et. al. (2011), and Hemsley, Patin, and Nahon (forthcoming).

xxxMoore, Adam. 2003 cite.

xxxBennett, Colin. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: MIT Press, 2008.

xxxHemsley, Jeff, Patin, Beth, and Nahon, Karine (forthcoming). "Information Movements in Networked Spaces: A Model of Networked Private and Public Spaces" presented at *Internet Research 12.0*, Seattle, WA, October, 12, 2011.

xxxLipton, 2010.xxx

> "An exception is the work of Jacqueline D. Lipton who sets forth six discrete aspects of privacy incurions: (1) actors-relationships; (2) conduct; (3) motivations; (4) harms-remedies; (5) nature of information; and (6) format of information, with the goals of creating "a larger-scale outline of privacy" and the interrelationships between the aspects of incursions. Jacqueline D. Lipton, "Mapping Online Privacy," *104 Nw. U.L. Rev. 477 (2010).* For our purposes, however, Lipton's work falls short because it doesn't bridge theory and practice. "

xxxKasper xxx cite

[25] See Solove (2008). A useful summary review article is offered by Citron and Henry (2010). An insightful criticism of Solove's contextualist approach is developed in Calo (2011). For a recent and instructive application of his pluralism to the torts of privacy see Solove and Richards (2010), the concluding sentence of which well states the spirit that also animates our efforts here: "If the tort law of privacy is to survive in the twenty-first century, it must finally emerge from Prosser's shadow and regain some of Warren and Brandeis's dynamism" (2010, get citexxx, p. 38 of PLSC doc version).

exactly privacy can be understood pluralistically. Solove undertakes a semantic analysis of privacy, that is, an analysis of privacy's *meanings* or *understandings* or *conceptualizations* which shows these meanings to be many, or plural.[26] Solove states that, "A conception of privacy is an abstract mental picture of what privacy is and what makes it unique and distinct."[27] Beginning here, Solove distinguishes six different theoretical conceptions of privacy prevalent in the contemporary literature:[28] the right to be let alone (or seclusion), limited access, control, personhood (or self-development), secrecy, and intimacy.[29] Building on methodologies drawn from philosophical pragmatism, [30] Solove cautions against common efforts to narrowly, reductively, or rigidly specify privacy.[31] Using philosopher Ludwig Wittgenstein's famous "family resemblance" metaphor for linguistic meaning Solove argues that there is no single

---

xxxSolove, Daniel J.. 2008. *Understanding Privacy*. Harvard: Harvard UP, 2008.
xxxCitron, Danielle Keats and Henry, Leslie Meltzer. 2010. "Visionary Pragmatism and the Value of Privacy in the Twenty-First Century" in *Michigan Law Review*, Vol. 108 Issue 6, Apr 2010: 1107-1126.
xxxCalo, Ryan. 2011. "The Boundaries of Privacy Harm" in *Indiana Law Journal* 86, no. 3, 2011: 1131-1162.
XxxSolove, Daniel J. and Richard, Neil M.. 2010. "Prosser's Privacy Law: A Mixed Legacy" in *California Law Review* 98, p. 1887, 2010.

[26] Cf. Solove 2002 and also Solove and Schwartz xxx *Info Priv Law* textbook.

[27] Solove 2008, 13. Given that most of the contributors to the privacy literature are lawyers and philosophers (both of whom are as a group nearly obsessed with argumentative justification), it is not surprising that most of the literature concerning privacy is written from the point of view of *justifications* of privacy. Now, whether or not Solove himself does equivocate amongst various interpretations of privacy's *meaning*, or focus solely on *justification* as the uni-dimensional core of privacy's *meaning*, or focus primarily on something else, the shortcoming in his approach that we wish to redress concerns the fact that this approach possesses no clear way of ruling out such equivocal understandings of privacy *conceptualizations*. Whatever Solove himself may have in mind when he talks of conceptualizations of privacy, there is nothing in the theory as developed that prevents a consistent 'Solovean' from equivocating here. Such equivocation engenders confusion and accordingly renders our uncertainty about privacy a liability rather than an asset. A multi-dimensional taxonomy is designed precisely with aims of clarification in mind.

[28] Cf. Solove 2002, 1099ff. and 2008, xxx

[29] Cf. Solove 2002, 1099ff. (xxxcorrect page #s) and 2008, 14-37

[30] See Solove 2008, 38-77 for a detailed explication of his background pragmatist method. On legal pragmatism more generally see Sullivan (2007). For a more exact specification of their shared legal pragmatism as against another version of legal pragmatism, namely Richard Posner's, see Michael Sullivan and Daniel Solove (2003).(
xxxMichael Sullivan, 2007. *Legal Pragmatism: Community, Rights, and Democracy*. Bloomington: Indiana University Press, 2007.
xxxSullivan, Michael and Solove, Daniel. 2003. "Can Pragmatism Be Radical? Richard Posner and Legal Pragmatism" in *Yale Law Journal*, Vol. 113, pp. 687-741, December 2003.

[31] On "family resemblance" see Wittgenstein (1953, §§65-88). According to Wittgenstein (cf. 1953, §§65-88), it is often pointless to try to develop formal singular definitions of certain terms (e.g., that of "game") since in actual linguistic use these terms overlap and criss-cross (e.g., there are board games, sports games, video games, and even war games) in a variety of ways. Every game has features that overlap with other games but there is no essential feature which all games possess. In this respect, words like "game" are akin to family resemblances (e.g., "the family eyebrows" or "the family temper) , since everyone in a family resembles everyone else even if there is no essential feature that all members of any family possess (e.g., not everyone in the family must have those eyebrows or that temper).
xxxWitgenstein, Ludwig. 1953. *Philosophical Investigations*. G.E.M. Anscombe (trans.). Malden: Blackwell, 2000.

feature that all concepts of privacy must share, but rather a set of features that link them all together as a network. Solove's innovation is thus to target the *meaning* of privacy in order to unpack privacy's plurality of meanings.

In a subsequent article, situated in this pluralistic approach, Solove shifts his focus from unpacking privacy's meaning to exploring privacy violations in part to address the problems posed by the essential contestability of privacy.[32] By focusing on harms Solove hopes to steer courts clear of the irresolvable debates about privacy and focus them instead on the myriad of harms various forms of privacy protect against.[33] He specifies sixteen different kinds of harms mapped across four meta-categories.[34] He argues, "We should understand privacy as a set of protections against a plurality of distinct but related problems. These problems are not related by a common denominator or core element. Instead, each problem has elements in common with others, yet not necessarily the same element—they share family resemblances with each other."[35]

His key insights for our purposes are both that, "Privacy is not one thing, but a cluster of many distinct yet related things,"[36] and that privacies can—and should—be prodcutively contrasted and related along dimensions beyond the semantic. Solove's work, along with the contextualist approaches discussed below, moves the debate away from a fixation on what privacy *really is* toward the many things that privacy *actually does* (and does not do) in the practice.

Solove's approach to privacy through its plurality of *meanings* and later shift to explore a dimension other than meaning—harm—hints at the need for an analytical approach that is sensitive to the pragmatics of *context.*[37] To be sure, however, *contexts* of practice are easily bewildering. To interrogate the relationship between meanings of privacy and the practices in

---

[32] Solove Taxonomy

[33] Id. "Courts and policymakers frequently have a singular view of privacy in mind when they assess whether or not an activity violates privacy. As a result, they either conflate distinct privacy problems despite significant differences or fail to recognize a problem entirely. Privacy problems are frequently misconstrued or inconsistently recognized in the law. The concept of "privacy" is far too vague to guide adjudication and lawmaking. How can privacy be addressed in a manner that is non-reductive and contextual, yet simultaneously useful in deciding cases and making sense of the multitude of privacy problems we face?"

[34] Solovexxx/Articleand2008,101-170

[35] Solove2008,171-2

[36] Solove2008,40

[37] SeeSolove2008,41-46.

which they are rooted we need to press beyond semantics, and the single dimension of harm, deeply into pragmatics.

Unpacking Privacy's Many Uses: Pragmatic Contextualism

The pragmatics involved in our approach requires a full-scale *contextualism* about privacy. We noted above that such contextualism is explicitly endorsed, but only implicitly developed, in Solove's work. Thankfully, there are many other sources for this sort of contextualist analysis.[38]

In the privacy area, this pragmatism is best exemplified by the work of Helen Nissenbaum in which she advances a theory of "privacy as contextual integrity".[39] Nissenbaum's central claim is that privacy depends on contextual features and as such that it cannot be preordained nor universally applied. As she puts it, "finely calibrated systems of social norms, or rules, govern the flow of personal information in distinct social contexts."[40] Privacy is one such norm. It must therefore be interrogated within the social contexts within which it functions. This is because the norms governing activity in one context or sphere are often inapplicable to those operative in another sphere (e.g., think of the stark difference between concerns about privacy in the boardroom and the bedroom).

A key point for Nissenbaum is thus that, "distributing social goods [such as the protection of personal information] of one sphere according to criteria of another constitutes injustice."[41] That, in a nutshell is the injustice of essentialism—essentialism about privacy too often falls prey to the temptation to apply some norm that is appropriate in one context to every other possible context. While the work of semantic pluralists advances a similar claim, none provides the tools

---

[38] See for an instructive historical approach the work of Samantha Barbas (2012). Also in a similar vein, Debbie Kasper offers a typology of privacy invasions consisting of *extraction*, *observation*, and *intrusion* (2005). Kasper further unpacks each form of invasion to consider the *motive* behind it, the *method* used, and the *awareness* of and *consequences* for the individual subject to the invasion. The value of this approach is, according to Kasper, that: "Categorizing invasions … provides a more meaningful context for each incident, as the type indicates how a party's privacy has been violated and hints at the extent to which one is aware of and has assented to the invasion" (2005, 75).
xxx Kasper. Debbie. 2005.
Xxx Barbas, Samantha S.. 2012. "Saving Privacy from History" in *DepaulLawReview* 61, 2012, 973-1048.

[39] Cf. Nissenbaum 2010, 2004
xxx Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford UP, 2010.
xxx Nissenbaum, Helen. 2004. LR Article get cite.

[40] Nissenbaum 2010, 3

[41] Nissenbaum 2004, 127

to effectively support explorations of privacy across realms to uphold their claim. Nissenbaum's theory pushes back against such essentialization by foregrounding the practice of privacy in contexts. Her approach foregrounds a contextualist sensitivity to the way in which concepts are embedded—and achieve meaning—only in specific contexts.

Nissenbaum's approach is useful precedent for our work because her path toward pluralism is through detailed contextual analysis function and practice. At the heart of the contextual integrity model is a heuristic or analytic for interrogating the functioning of privacy in context parsed by Nissenbaum into a multiplicity of elements: activities, roles, norms, power structures, and values.[42] Nissenbaum's notion of context builds on the work of a range of contemporary social theorists, including Michael Walzer and Pierre Bourdieu, who have argued that modern societies are characterized by a plurality of distinct spheres of practical activity each of which is governed by its own internally-negotiated norms.[43] Through a careful parsing of the idea of context, Nissenbaum opens up contexts of privacy for careful interrogation, thereby exposing privacy itself to more fine-grained analytical inquiries. Our effort builds upon this pragmatic, deeply contextual, approach.

Unpacking Privacy's Generativity: Pluralism, Contextualism, and Contestability

The approach we adopt here leverages the best of semantic pluralism and pragmatic contextualism to explicate the generativity of privacy's contestability. Our analytic enables more precise disentangling and mapping of the differences and similarities among concepts and practices of privacy and by doing so supports dynamic and flexible deployment midst desirable contestability. In the spirit of Solove's semantic pluralism and Nissenbaum's pragmatic contextualism, our analytic of privacy reveals a *plurality of meaningful conceptions* of privacy and the *plurality of practical dimensions* along which they relate and vary within and across contexts.

---

[42] Nissenbaum 2010, 132

[43] Cf. Nissenbaum 2010, 130ff., 166ff.; see further Walzer 1983 and Bourdieu and Wacquant 1992. See also Van Den Hoven 2008, 313-5 for a similar use of Walzer for the purposes of a contextualist theory of privacy.
xxx Vanden Hoven, Jeroen. 2008. "Information Technology, Privacy, and the Protection of Personal Data" in Vanden Hoven and Weckert (eds.), *Information Technology and Moral Philosophy*. Oxford: Oxford University Press, 2008.
xxx Walzer, Michael. 1983. *Spheres of Justice: A Defense of Pluralism and Equality*. Press xxx.
xxx Bourdieu, Pierre and Wacquant, Loic. 1992. *An Invitation to Reflexive Sociology*. Press xxx.

Pluralism and contextualism are useful corollary starting points for exploring the benefits of contestability. Pluralism gives us an account of the many meanings of privacy that feature in conflicting accounts of privacy, and a contextualist approach to values analysis gives us tools for more detailed inquiries into privacy's many meanings so that debates about privacy can be meaningful even in the shadows of deep disagreement. We thus stitch together pluralist theory and contextualist analysis to facilitate the work of tracking contests over, debates about, and disagreements concerning privacy. These contests are of increasing important in our contemporary moment as we are witness to new technologies, new social practices, and a welter of new business and governmental strategies emerging in response to socio-technical transformations.[44]

Our emphasis on contestability, which is perhaps a species of an even more general notion of 'contestabilism', both accounts for its essential contestability and builds off recent scholarship documenting the value of the conceptual ambiguity of privacy, making more particular a general point about the usefulness of ambiguity for regulation writ large.[45] Jonathan Zittrain's work on non-formalized regimes of socially-coordinated activity is a useful exemplar.[46] His argument is that non-formalized regimes make use of ambiguities and flexibilities to achieve socially desirable outcomes where more classical approaches involving "system[s] of perfect enforcement" tend to produce only compliance with rules rather than achievement of the desired social outcome. Less formalized approaches may "foster innovation and disruption."[47] We would add, that they may also enable us to better track novel and unsettling developments upon their emergence. Further in this vein, one of the current authors claims that privacy's conceptual ambiguity appears to produce greater institutional fidelity to evolving societal privacy goals because it demands ongoing dialogue with external stakeholders

---

[44] Seeabovenote(onDwork,mosaictheory,etc.).xxx

[45] OnstandardsversusrulesseegenerallyFuller(1978),Rose(1988),Sullivan(1992),andRaban(2010).SeealsoLessig(xxx) onlatentambiguitiesinlaw.
xxxSullivan,KathleenM..1992."TheSupremeCourt,1991Term– Foreword:TheJusticesofRulesandStandards"in*HarvardLawReview*106,22(1992).
xxxRose,CarolM..1988."CrystalsandMudinPropertyLaw"in*StanfordLawReview*,40,577(1988).
xxxFuller,LonL..1978."TheFormsandLimitsofAdjudication"in*HarvardlawReview*92,xxx?(1978).
xxxRaban,Ofer.2010."TheFallacyofLegalCertainty:WhyVagueLegalStandardsmaybeBetterforCapitalismandLiberalism"in*TheBostonUniversityPublicInterestLawJournal*19,no.2,Spr.,2010:175-191.
xxxZittrain,Jonathan.2008.xxx

[46] Zittrain2008,228;seealsoShirky(xxx).

[47] Zittrai2008,8

to define, redefine, and implement. This contrasts with command and control regulation, which orients institutions around compliance rather than privacy. Privacy's conceptual ambiguity, she finds, combine with professionalization and stakeholder engagement, to produce deeper engagement with privacy and more meaningful embedding in institutional structures.[48]

Looking also toward more theoretical and philosophical sources, our view is that privacy is like other essentially-contested concepts at the core of our modern (or post-modern, if you must) culture(s): justice, right, morality, democracy, liberty, equality, and publicness.[49] Like these concepts, privacy cuts so much to the heart of our moral, political, legal, and cultural self-understandings that we cannot but disagree over its meaning, application, implementation, and justification. The attendant debates surrounding privacy, while often frustrating, are also evidence of our culture productively negotiating rapidly-changing social contexts.

Accordingly, we view the current combination of centrality and contestability of privacy as a source of hope. We believe it signals society's ongoing engagement and concern with privacy and the vibrancy of privacy to the conditions of modernity. Privacy is decidedly not dead nor at its end—it is alive and in constant use, even if its' many uses betray an essential contestability. As a core value of our liberal culture privacy's ability to perform a number of distinct and important functions reveals its vibrancy. There is, however, a stringent challenge implicit in this hope.

Some would argue that affirming privacy's contestability via an analytics of its complexity opens the door to insurmountable obstacles for those seeking to employ theories of privacy or adjudicate amongst competing theories. But this need not be the case. Through categorization, mapping, and critical analysis we can increase our understanding of privacy's multiplicitous functions. Rigorous critical scrutiny of privacy can reveal complexities in privacy's workings that allow privacy practitioners to more deftly deploy relevant concepts and to remedy the gaps in existing theoretical and legal approaches from the perspective of today's

---

[48] SeeBambergerandMulligan(2010)andBambergerandMulligan(2008). XxxMulliganandBamberger.2010."PrivacyontheBooksandontheGround"in*StanfordLawReview*,v63,Fall,2010. xxxMulliganandBamberger.2008."PrivacyDecisionMakinginAdministrativeAgencies'in*UniversityofChicagoLawReview*,v75,no.1,January,2008:pp.75-107.

[49] On'essentially-contestedconcepts'seeGallie1956.xxxForasimilarnotiondevelopedmidstaratherdifferenttheoreticaltraditionseetheideaof'emptysignifiers'inLaclauandMouffe(1985)xxx.xxx

privacy wrongs. There is, however, no doubt that this places a burden of challenging work on those who would continue to make use of privacy.

The express aim of our multi-dimensional mapping is to ease and facilitate the challenging work through an analytic for examinations of privacy in operation in specific contexts and in relation to the formation, delineation and expression of identities, relationships and communities. A multi-dimensional approach enables us to document the variance in privacy theories and practices along a broad range of dimensions. Thus we could come to regard the contestability of privacy as a testament to the importance of privacy across a range of contexts, interactions and relations. Contestability affords privacy a resilience and flexibility necessary for its continued utility and relevance in rapidly-changing socio-technical milieus, such as those we find ourselves in today as a result of new networked, digitized, and databased socio-technologies, but only if it can be easily and profitably used.

§3:A Multi-Dimensional Analytic for Privacy

Working with a fuller understanding of the many contextually-dependent features that we (privacy professionals in both the public and private sectors, privacy lawyers, privacy scholars, and privacy theorists) operate with when we work with privacy facilitates a more effective engagement with the ways in which privacy functions in practice. The multi-dimensional taxonomy we present in this section is meant to push the conversation around privacy toward more rigorous modes of analysis. Recognizing the "open texture"[50] of privacy, our multi-variable taxonomy is not meant to provide an exhaustive specification of all the possible dimensions conceptions and uses of privacy should or could have a grip on, but rather a specific starting point for expanding the range of our inquiries into the plurality of privacies.

In that spirit, we present here a specification of a range of dimensions that we consider crucial for a contextualist account of privacy. We propose to map privacy along the following

[50] Friedrich Waismann, Verifiability, 19 Proc. Aristotelian Soc'y 119, 121 (1945) (supp. volume). By open texture, we mean the recognition that the dimensions we identify and consider crucial are a product of our experience with specific instances of privacy at work as a concept in the world, and therefore reflects the limitations of current experience. We believe it both possible and likely that new experiences of privacy may identify additional dimensions of importance, thus leading to the open texture of the term and our dimensions. Accord, Jeremy Waldron, Vagueness in Law and Language: Some Philosophical Issues, 82 Cal. L. Rev. 509, 510 (1994) (explaining that Waismann's point is that attempts to pin down a precise meaning for a term are based "our best response to experience" and when presented with new experiences we construct "a different classificatory theory") Id. at 523.

fourteen dimensions (all of which are described in detail in the following sub-sections): Object, Justification, Contrast Concept, Exemplary Problem, Target, Subject, Action, Offender, From-Whom, Mechanism, Provider, Expert, Social Context, and Contextual Scope. We cluster these fourteen dimensions around a set of five meta-dimensions of *Theory*, *Protection*, *Harm*, *Provision*, and *Context*.[51] Our claim is that analytically separating these threads helps clarify privacy's function and value in practice. The central focus is on the range and variability of privacy across the first-order dimensions, the meta-dimensional clusters illustrate but one among many sets of connections to be drawn.[52] What would otherwise remain a knot is thereby opened up to analytical discrimination such that we can recognize how different privacy conceptions are operating differently in different practical contexts.[53]

Privacy Dimension	Description	Interrogation	Example
Dimensions of Theory			
Object	That which privacy provides to those protected, i.e. *privacy provides protected agents with X*.	'What's privacy for?'	Dignity Control over Personal Info
Justification	The motivation and basis for providing privacy, i.e. *privacy is justified because of X*.	'Why should this be private?'	Individual Liberty Social Welfare
Contrast Concept	That which contrasts to privacy, i.e. *that which is private is mutually exclusive with that which is X*.	'What's not private?'	Public Open Transparent
Exemplar Problem	The archetypal threat to this concept of privacy, i.e. *privacy is violated by X*.	'What's an example?'	Personal Identity Theft Intrusive Surveillance Gossiping Neighbors
Dimensions of Protection			
Target	That which privacy protects, i.e.	'What's privacy	Personal Information

[51] These unifying meta-dimensions should not be taken as definitive, as other equally viable clusters present themeslves.

[52] Our aim here is again similar to Samuelson's effort to identify and classify the existence of multiple public domains to facilitate discourse about them and more productive use of them. It allows "context-sensitive meanings of privacy to evolve, contributing to "a richer understanding" of their contents, the "social values" and communities they serve, the "legal and institutional structures available to preserve them", and finally the threats they face and strategies to abate them. At 833. Cite? See above note 6.xxx.

[53] Two qualifications are in order. First, it is not to be expected that a detailed examination of every dimension will be *necessary* in order to gain an understanding of any and every privacy violation we may meet with. Our claim, rather, is that this full list of dimensions specifies as *sufficient* range of material that one may need to assess a privacy violation. Second, it is not our view that the dimensions here specified pertain *only* to an analytical inquiry into concepts of privacy and their many functions. Clearly they pertain to *much else* besides. Our claim is that some subset of these dimensions are sufficient to elucidate privacy, not that privacy is of necessity the only field of analysis in which these dimensions might come into play.

	privacy protects things of type X.	about? Privacy of what?'	Body or Likeness Private space
Subject	Actor(s) or Entity(ies) protected by privacy, i.e. *privacy protects agent X*.	'Whose privacy is at stake?'	Myself, My Child Social Groups (e.g., teens) Roles (e.g., students)
Dimensions of Harm			
Action	The act or behavior that initiates or constitutes a privacy harm, i.e. *staring at him while he was dressing in the locker room violated his privacy*.	'What act violated privacy?'	Solove's 4 meta-harms (Collection, Processing, Dissemination, Invasion)
Offender	Actor(s) violating privacy, i.e. *privacy violated by agent X*.	'Who violated privacy?'	Government Business Entity Peeping Tom
From-Whom	Actor(s) against-whom privacy is a protection, i.e. *privacy provides protection against agent X.*	'Who is privacy protecting against?'	Everyone Government 'Friends of Friends'
Dimensions of Provision			
Mechanism	That which instrumentally secures privacy, i.e. *the lock on her door protected her privacy*.	'How is privacy provided?'	Legal Regulations Technical Design Social Norms
Provider	Actor(s) charged with securing privacy, i.e. *the telecommunciations provider was responsible for technically securing the privacy of her communications*.	'Who is supposed to provide privacy?'	Government Business Entity Technology
Expert	Actor(s) charged with determining privacy, i.e. *the determination that privacy should be provided should be made by X*.	'Who knows what privacy is and how privacy works?'	Policymakers Chief Privacy Officers Any Concerned Citizen
Dimensions of Context			
Social Context	That wherein privacy applies, i.e. *privacy applies in domain, situation, field, or site X*.	'Where is privacy found?'	Hospital or University Nation-State or Globally
Scope of Context	Extent of application of privacy, i.e. *privacy should be applied with a scope of X*.	'How widely does privacy apply?'	Universally as strict rule Casuistically as per-case

This preliminary specification of dimensions invites the question of how they relate. We propose two requirements that capture basic intuitions about the relations that hold between dimensions. It is crucial for our analytic to be clear that a key point in distinguishing the dimensions we do is to show that many of the dimensions in question are *non-covariant* at the same time that a viable practical implementation of privacy requires *coherence* amongst these

many dimensions. The *coherence* requirement just suggests that privacy in practice needs to employ objects, justifications, targets, and mechanisms (and so on), which are not in direct odds with one another. The *non-covariance* requirement allows dimensions to shift independently; for example, such that any given object-justification-target cluster might be suitably paired with any number of mechanisms for achieving privacy in that sense, given of course that the coherence condition is also met.

We now turn to more detailed discussions of each dimension with the idea of more finely specifying the ways in which privacy is woven out of this multiplicity of threads.

Dimensions of Theory

Objects of Privacy

By *object of privacy* we mean that which a conception of privacy seeks to provide, protect, secure, establish, or create. The idea of *object* refers to what might usefully be thought of as the *telic* or *functional* dimension of privacy (from the Greek *telos* for 'end' or 'aim'). The object of privacy is the goal of privacy protections. We thus conceive of the object of privacy in functionalist terms—the object of privacy has to do with the function that privacy performs. Does the concept of privacy aim to secure a zone of individual freedom of action, provide control over individualized information, insulate individuals against social scrutiny, or enable the efficient allocation of economic resources by way of socially-distributed market mechanisms? These are some of the possible objects operative in different concepts of privacy.

Delineating object as a dimension draws attention to the specific and varied ends which privacy is deployed to secure. It also allows us to appreciate the range of mechanisms that can procure this end state. The object of privacy can remain agnostic with respect to the means employed to procure it.

Discriminating amongst the possible objects toward which privacy might aim clarifies a set of confusions and equivocations that pervade contemporary debates over privacy. One example of this can be found in the tendency of existing work on privacy to trade between attempts to provide a zone of private *information* and attempts to provide a zone of private *decision* or *action*. A conception of privacy that attempts to safeguard individual dignity by guaranteeing the individual full decisional autonomy with respect to his or her self (including the body) is quite different from a conception that attempts to safeguard individual dignity by

guaranteeing the individual full control over information about his or her self (including facts about the body). These two concepts of privacy vary with respect to two different *objects* of privacy, namely 'decisions about one's body' or 'control over personal information.' Some of the most widely-discussed objects of privacy featured in the literature include: privacy as limited accessibility,[54] privacy as enabling freedom,[55] privacy as self-development,[56] privacy as intimacy,[57] privacy as tied to property,[58] and of course the objects of decisional autonomy and personal informational control just mentioned.[59] These competing concepts of privacy differ with respect to the object—the aim—and as such would require different rules to operationalize. Our ability to pose questions to these operations requires an analytic that assists in distinguishing among objects operative in the theory and practice of privacy.[60]

Justifications of Privacy

Discriminating amongst *justifications* draws attention to the analytically distinct reasons put forward in defense of a given object of privacy. Justification is the underlying beliefs or assumptions that ground and supports a conception of privacy. If the *object* is that which privacy

---

[54] See canonically Charles Warren and Louis Brandeis (1890) and more recently Ruth Gavison (1980).
xxx Warren and Brandeis cite.xxx
xxx Gavison, Ruth. 1980. "Privacy and the Limits of the Law" in *The Yale Law Journal* 89, no. 3, Jan. 1980: 421-471.

[55] See Jed Rubenfeld (1989).
xxx Rubenfeld, Jed. 1989, "The Right of Privacy" in *Harvard Law Review*, Vol. 102, No. 4 (Feb., 1989): 737-807.

[56] See Julie Cohen (2000, 2008).
xxx Cohen, Julie E.. 2000. "Examined Lives: Informational Privacy and the Subject as Object" in *Stanford Law Review* 52, 2000: 1373-1437.
xxx Cohen, Julie E.. 2008. "Privacy, Visibility, Transparency, and Exposure" in *University of Chicago Law Review* 75, 2008: 181-201.

[57] See Jean Cohen (2002).
xxx Cohen, Jean. 2002, *Regulating Intimacy: A New Legal Paradigm*. Princeton: Princeton UP, 2002.

[58] See Richard Posner (1978).
xxx Posner, Richard. 1978. "The Right of Privacy" in *Georgia Law Review* 12, no. 3, Spr., 1978: 393-422.

[59] On privacy as autonomous control see Rossler (2001) and DeCew (1997).
xxx Rossler, Beate. 2001. *The Value of Privacy*. Rupert D.V. Glasgow (trans.). Cambridge: Polity, 2005.
xxx DeCew, J., 1997, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca: Cornell University Press, 1997.

[60] This can be illustrated in the area of privacy law articulated by the well-known U.S. Supreme Court articulations of a substantive due process "right to privacy" in *Griswold v. Connecticut*, *Eisenstadt v. Baird*, *Roe v. Wade*, and *Whalen v. Roe* (see 381 U.S. 479 (1965), 405 U.S. 438, 453 (1972), 410 U.S. 113 (1973), and 429 U.S. 589 (1977)). There may appear to be some irony (orlesscharitably, no small incoherence) in the fact that this right to privacy was articulated in terms of a Constitutionally-defined right to restrict access to and use of *information* about the self, yet has been understood and used to restrict access to and dominion over the *active* (most importantly, *bodily*) self. Our approach helps elucidate the point that information is often the *target* of privacy rather than the *object* of privacy such that we can how protections of information can be part and parcel of bodily privacy.

aims to secure or defend, then the *justification* furnishes the moral basis for securing and providing it. *Justification* initiates privacy that then eventuates in its *object*.

There is much to be said about what justification properly is and what, therefore, does and does not count as an appropriate justification.[61] We here remain agnostic about these debates so far as is possible and draw on an ordinary understanding of justification which refers to that which is put forward 'in defense of' or 'as a ground for' a given object of privacy. This agnosticism supports our aim to develop a methodological analytic that enables researchers to (whether descriptively or prescriptively) assess the various kinds of justifications offered for privacy. While we do not here interrogate the merits offered to justify specific conceptions of privacy, it does reflect our belief that every theory of privacy must offer some kind of justification of the privacy object it defends or secures. A concept of privacy without a justification would find itself, obviously, indefensible.

Justifications prove exceptionally helpful for unpacking and identifying the family resemblances of privacy concepts. Different theories of privacy offer distinct justifications for the very same privacy object. A group of privacy proponents might argue that the appropriate object of privacy is a zone of individual freedom, yet disagree as to *why* this zone of freedom *ought* to be secured. A justification provides the rational answer ('why') to the normative question ('ought'). One proponent might argue that privacy as a zone of freedom is justified because it is intrinsic to human dignity, while another might argue that it is justified because it is instrumental in realizing the human capacity for self-development.[62] A wide-range of justifications are consistent with any given object of privacy, and a given justification may

---

[61] For the elaboration of a social-practical conception of justification consistent with our pragmatist approach here see work in Brandom (1994). xxx Brandom, Robert. 2004. *Making It Explicit*. Cambridge: Harvard University Press, 2004.

[62] James Q. Whitman (2004) identifies competing justifications for privacy norms in Europe and the U.S.. He claims that privacy in Europe is generally justified by personal dignity, while in the U.S. it is generally justified by personal liberty. We find Whitman's work compelling, however, as he notes, such a broad brush occludes important variance in justifications at work in U.S. privacy concepts—both legal and practical. Further, as William Fisher (2001) discusses, the importance of interrogating justifications is highlighted by the ongoing disagreement over the appropriate justification for the protection of intellectual property—utilitarianism (protecting the incentive to create, invent, or produce to maximize net social welfare), which dominates in the U.S., or natural rights (individuals have a moral right to their own creations and inventions), which dominates in Europe. xxx William Fisher, *Theories of Intellectual Property*, *in* NEW ESSAYS IN THE LEGAL AND POLITICAL THEORY OF PROPERTY 168 (Stephen R. Munzer ed., 2001).
xxx Whitman, James Q., The Two Western Cultures of Privacy: Dignity versus Liberty," Yale Law Journal, Vol. 113, April 2004.

support various objects. Distinguishing privacy's justificatory dimension therefore helps us understand how privacy is often (and certainly ideally) conceptualized from a rational-normative point of view. Crisply delineating justifications reveals an important shared trait among concepts of privacy that might be easily overlooked given the relatively high visibility of objects of theories, or *targets*—as discussed below—at issue in a given tussle over privacy grab our attention.

Contrast Concept to Privacy

Contrast concept is a casual philosophical term referring to that which properly contrasts with a concept under scrutiny. The contrast concept for black is white, hot for cold, and so on. Contrast concepts negatively define the contours of the concept in question. Defining in the negative is particularly useful when grappling with abstract concepts that often can be sensibly contrasted with a range of different contrast concepts, giving rise to a multiplicity of valences. For example, consider the concept or idea of freedom. In the classical liberal tradition, as represented by John Stuart Mill and more recently renewed by Friedrich Hayek, the proper contrastive idea for freedom is intereference.[63] In the classical civic republican tradition, as represented by Machiavelli and more recently resuscitated by Phillip Pettit amongst others, the proper contrastive idea for freedom is domination.[64] These two divergent traditions of modern political theory are both fundamentally focused on freedom as a value, yet they yield two analytically distinct concepts of freedom as non-interference and as non-domination. The general point, then, is that in the case of essentially-contested concepts like freedom and privacy, contrast concepts often advance understanding.

The contest over the meaning and function of privacy is no less fierce than our longstanding culture wars over freedom. Different conceptualizations of privacy yield a range of different contrast concepts. That which is private may be properly contrasted to that which is

---

[63] Cf. Mill (1859 and 1848, Bk. V, Ch. XI) and Hayek (1960).
xxx Hayek, F. A. von. 1960. *The Constitution of Liberty*. London: Routledge and Kegan Paul, 1960.
xxx Mill, John Stuart. 1848. *The Principles of Political Economy* in Mill, *The Collected Works of John Stuart Mill, Volume III - The Principles of Political Economy with Some of Their Applications to Social Philosophy (Books III - V and Appendices)*, ed. John M. Robson. Toronto: University of Toronto Press, 1965.
xxx Mill, John Stuart. 1859. *On Liberty*. Oxford: Oxford World's Classics, 1994.

[64] Cf. Machiavelli (xxx) and Pettit (1997)
xxx Pettit, Phillip. 1997. *Republicanism: A Theory of Freedom and Government*. Oxford: Clarendon Press, 1997.

public, as is typical of liberal political theories of governance and regulation, thus yielding a non-interference or non-intrusion image of privacy.[65] The private may be properly contrasted to the transparent or the exposed, thus yielding an image of privacy in terms of secrecy or intimacy.[66] The idea of private information may also be contrasted to a kind of information over which one has no control over access or over which there is unrestricted access, thus yielding an image of privacy as control over access.[67] There are, as well, many other contrast concepts for ideas of privacy that travel in on the ground privacy practices today. A firm grip on this dimension of privacy advances a refined understanding of what privacy requires by clarifying its absence.

Exemplary Privacy Problems

A final crucial theoretical element of privacy is the *exemplar* (or *paradigm* or *prototype*) that crystallizes the problems, harms, or violations to which a given concept of privacy responds. Our point in drawing attention to *exemplary privacy problems* is to emphasize the ways in which the theory and practice of privacy are mutually constitutive.[68] Our view is that every viable conception of privacy must present itself, at least in part, through an exemplar that crystallizes the specific upshot of that conception. A conception of privacy without an exemplary privacy problem would remain purely formal and abstract just as examples of privacy problems dissociated from a broader conceptual architecture would remain un-specified and unjustified. As such, we understand exemplars as central parts of the theories for which they are exemplary. Exemplars are not mere afterthoughts that illustrate conceptions. They are constituent parts of the conceptions. They elucidate conceptual architecture such that without a working exemplar a theory would remain very difficult to understand.

---

[65] The canonical classical liberal text thereagainis Mill (1859), yielding a picture that is best represented in the modern privacy literature by the canonical article by Warren and Brandeis (1890).
xxx Warren/Brandeis 1890. Cite. xxx

[66] See for example Thomas Nagel (2002) and again Jean Cohen (2002).
xxx Nagel, Thomas. Concealment and Exposure. Cite. xxx

[67] See Judith DeCew (1997) and Beate Rössler (2001).
xxx DeCew, J., 1997, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca: Cornell University Press, 1997.
xxx Rössler, Beate. 2001. *The Value of Privacy*. Rupert D.V. Glasgow (trans.). Cambridge: Polity, 2005.

[68] Our work here is rooted in perspectives in the philosophy of science associated with Thomas Kuhn's (1962) concept of paradigms and related work in the different context of cognitive psychology as developed by Eleanor Rosch (1973) under the heading of prototype theory.
xxx Kuhn, Thomas, 1962. xxx *Structure*.
xxx Rosch, Eleanor H. 1973. "Natural Categories" in *Cognitive Psychology* 4, 1973: 328-350.

We take it that a concern for exemplars is part of what Ann Bartow was expressing a demand for in her criticisms of Solove's pluralist account of privacy as "too much doctrine, and not enough dead bodies."[69] Bartow was not calling for sensationalism; or, rather, if she was, then surely Solove was right to reply that privacy is the sort of thing that is rarely sensational.[70] The insight we recognize in Bartow's claim is that concerns over privacy are likely to fall on deaf ears (and blind eyes) if they are not articulated in terms of compelling examples that make those concerns crystal and crisp. As such, exemplars ought to be central to the analysis of how privacy functions in practice, what privacy means in theory.[71]

A compelling vindication of exemplars comes from Justice Stewart Potter's infamous concurrence in *Jacobellis v. Ohio*, where he wrote, "perhaps I could never succeed in intelligibly" defining hard-core pornography, but "I know it when I see it."[72] The idea of an exemplary problem has much to offer to jurisprudential conceptions of legal reasoning as well as to the understanding of how theories more generally function without relying upon rules that pre-determine every instance of their application. If a scientific theory or legal principle could be deployed only by using a rule which pre-determines application in every instance, then the theory or principle in question would hardly be applicable to situations that were not anticipated at the time of the origination of the theory or principle. Law with its case-by-case development embodies the need for both clarity and forward-looking flexibility. Unfortunately, in many instances courts are constrained by miserly legal interpretations that stymie efforts to protect privacy against emerging threats. We face new privacy problems that many of the extant concepts of privacy—some now more than a hundred years old—simply could not anticipate in rule-like fashion. To the extent that concepts of privacy prove resilient is not due only to the

---

[69] Bartow 2006, 52 ("…the Solove taxonomy of privacy suffers from too much doctrine, and not enough dead bodies. It frames privacy harms in dry, analytical terms that fail to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease.") xxx Bartow, Ann. "A Feeling of Unease About Privacy Law" University of Pennsylvania Law Review 154 (2006).

[70] Cf. Solove 2011, 29ff..
xxx Solove, Daniel J.. 2011. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven: Yale University Press, 2011.

[71] Bartow illustrates the need for *exemplars* to provide visceral proof of the legitimacy of the claimed *justification* for privacy where she writes of the limitations of Solove's taxonomy: "Persuading observers to take privacy concerns seriously requires convincing them that people who are not engaging in illegal conduct are harmed in a significant, cognizable way when their personal information is collected and distributed against their will or without their knowledge. Toward this end, a more effective taxonomy would dramatically and thoroughly document the consequences of privacy violations in very visceral, dramatic ways." 2006 at p. 61.

[72] 378 US 184 (1964).

objects and justifications at the core of their architecture, but also to the exemplars that specify the workings of that architecture in the first place.

Dimensions of Protection

Target of Privacy

By *target of privacy* we refer to the specific type of thing that privacy aims to protect or safeguard. As such, the idea of a privacy target might be easily confused with the idea of a privacy *object*, but we find the analytical distinction between the two a firm one. Whereas object refers to that which privacy seeks to provide to those protected as the very aim of privacy protection, target refers more empirically to the specific types of things to which these protections apply. Thus, privacy in some instances might apply to the target of 'personal information' although the broader object of privacy in some of these instances might be 'personal dignity' or even 'personal freedom' such that privacy protections of personal information (as target) affords in a broader sense a protection of personal freedom (as object). That privacy targets and privacy objects might be easily confused for one another is likely a function of the fact that in many instances the target and object of privacy will coincide. For example, in some instances the target and object of privacy may be personal freedom or autonomy; in these instances privacy applies directly to personal freedom as that which is both directly protected (as target) and sought as the aim of privacy protection (as object). But in most instances, the target and objects of privacy prove to be distinct. If the object is the end which privacy protections are intended to bring about and the target is that which is expressly guarded by privacy protections, then we can easily recognize that privacy does not actually produce targets like personal information in the way that it might produce its more conceptual ends such as autonomy or dignity or opportunities for self-development. Some of the most familiar targets of privacy include personal information, bodily integrity, inviolate personality, decisional capacities, and individual freedom.

Subject of Privacy

By *subject of privacy* we refer to the agent or agents whom privacy protects. The dimension of *subject* simply picks out those on whose behalf privacy is provided. This is worth specifying in many instances insofar as privacy often does not apply universally to everyone in

identical fashion, say in the manner of a basic human right, but often applies to persons with respect to some particular feature of those persons or the situations in which they find themselves. Depending on context, the subject of privacy might be a single individual (e.g., 'myself' or 'my teenage daughter' or 'my elderly father'), or it might be a distinctive social class (e.g., 'teenagers' or 'citizens of California'), or it might be a distinctive social role (e.g., 'students' or 'teachers').

Dimensions of Harm

Action against Privacy

By *action against privacy* we refer to the actions that constitute or initiate privacy harms. At the level of our analytical taxonomy, our aim is merely to propose that privacy-related actions can vary in context, and independently of the other dimensions brought into focus by our analysis. Solove's specification of sixteen different violations of privacy grouped across the four categories of collection (surveillance, interrogation), processing (aggregation, identification, insecurity, secondary use, exclusion), dissemination (breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion) and invasion (intrusion, decisional interference)[73] provide a useful list of actions for consideration. We endorse Solove's list as illustrative but not exclusive, for the actions considered capable of violating privacy differ based on context and will no doubt change due to shifts in technology and norms. Future research might specify a further (or otherwise different) list of privacy-related actions that constitute privacy harms. This, however, is not our goal here. Our point is only that the specification of the harmful action involved is just one of privacy's dimensions.

Offender against Privacy

The dimension of *privacy offender* refers to those who are responsible for initiating or producing (whether intentionally or not) a violation of privacy. It is crucial to recognize that the *offender* in a given instance need not always be the same agent as that against whom privacy protections are meant to provide a shield. The offender just is that agent which brought about the

---

[73] Cf. Solove 2008, 101ff. and Solove 2006. Cf. also ??? Kasper ??? xxx Solove, Daniel. 2006. "A Taxonomy of Privacy" in *University of Pennsylvania Law Review* 154, no. 3, Jan., 2006: 477-560.

privacy invasion in question. Privacy offenders sometimes work in their own interest (as when in the case of the anxious ex-boyfriend who self-interestedly snoops around a diary or a cell phone dialed-calls list) but very often the offender against privacy creates the offense accidentally or unwittingly (as in the case of the corporation who accidentally is negligent about protecting the privacy of their clients in leaving a database of personal information unnecessarily exposed and vulnerable). These latter cases are, of course, the more unsettling because they are legally and morally much more ambiguous than cases of straightforward violations by clear-cut single-party offenders.

Privacy From-Whom

Privacy from-whom denotes those against whom privacy protections work on behalf of a given subject. For example, I may store in my email account records of personal communications to colleagues, friends, or family. I may not want certain parties referred to in those communications to have access to the things I have said about them. Thus I seek privacy from the prying eyes of other colleagues, friends, or family members.

It is often valuable to distinguish the *offender* against privacy from the *from-whom* against which privacy protects the *subject*. In many cases a single actor may occupy these two dimensions. For example, an ex-boyfriend hacks into his ex-girlfriend's email account (he is the *offender*) and reads only certain emails with his name in the subject line or body of the email (he is the intended *from-whom*). But in many cases these two dimensions do not coincide. For example, an ex-boyfriend (the *offender*) posts to their social network site a compromising picture of his ex-girlfriend (the *subject*) that she would rather her mother and her employer (the *from-whom*) not see. While she may or may not care about her ex-boyfriend viewing the picture again, a distinct loss of privacy involves the new audience. Another example reveals the importance of this subtle distinction. Consider familiar cases of computer hackers gaining access to your personal information. In this case, the hacker qua hacker is the offender, whereas the from-whom is not the hacker qua hacker so much as the hacker insofar as they are another person who should not have access to your personal information.

Dimensions of Provision

Mechanism for Privacy

The idea of *mechanism for privacy* helps delineate the technologies, techniques and tools through which privacy is or should be implemented. We presume that privacy is a normative notion, which means that it connotes should-ness and ought-ness. As such, privacy where it is not self-implementing must be, and is, implemented by means or mechanisms that vary widely. While it is sometimes assumed that the proper mechanism for implementing privacy is the law, it is crucial to recognize that a surfeit of mechanisms are in use for the provision of privacy—these include norms, transaction costs, and technology. Formalizing the category of mechanism focuses attention on the many ways privacy may be advanced. This is of particular importance due to strengths and limitations of various mechanisms. Legal rules and standards may not always be the optimal choice to protect privacy in a given context. For instance, many regulators and scholars are now focused on the potential beneficial effect technical design can have for privacy.[74] Scholars have drawn attention to a variety of other privacy mechanisms.[75]

This variety of mechanisms also speaks to the way in which an analysis of how privacy is provided benefits by taking a broad view of the social and technical affordances at play wherever privacy is produced.[76] The provision of privacy through a particular mechanism always takes place against the background of a broad network of affordances in virtue of which those mechanisms can be operative. For example, laws protecting domicile privacy are operationalizable only in the context of a built environment where dwellings are constructed to have opaque walls and closing doors, or online privacy controls implemented by social networking sites may make privacy technically possible and yet still fail because prevailing and entrenched user habits do not afford the conversion of this technical possibility into actual social reality. These examples help show that we can and should construe the class of affordances as broadly as possible.

---

[74] See Deirdre K. Mulligan and Jennifer King, "Bridging the Gap between Privacy and Design," U. Penn. Con. L. J. for an overview of current privacy by design efforts and their limitations.

[75] For example, Harry Surden (2007) highlights the important role that structural barriers play in protecting privacy by raising the transaction costs of its violation, while Helen Nissenbaum brings into focus norms that govern, establish, and afford privacy expectations in transactions involving personal information (2010).
xxx Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policity and the Integrity of Social Life*. Stanford: Stanford University Press, 2010.
xxx Surden, Harry. 2007. "Structural Rights in Privacy" 60 SMULR 1605 (2007).

[76] See Gibson (1977) for a background on affordances.
xxx James J. Gibson (1977), The Theory of Affordances. In *Perceiving, Acting, and Knowing*, Eds. Robert Shaw and John Bransford, ISBN 0-470-99014-7.

The relationship between mechanisms and affordances also helps us understand how there may be mismatch between a given mechanism and its object of protection due to a wide variety of factors that the idea of affordances can help us specify. There may be political inability—for example it would be very difficult to craft a law protecting diary entries from prying parents. There may be a mismatch between the scope of a necessary protection (global) and the field of a mechanism's operation (local or national).[77] Or we may lack the resources or knowledge necessary to benefit from the mechanism to access redress if it is breached. In some cases social norms, moral rules, and cultural customs may be more effective safeguards for privacy than legal protections due to these various attributes. In other instances architecture—physical or that of software—may provide surer protection.

Provider of Privacy

The *provider of privacy* refers to those agents who ought to provide privacy protections under a given theory. On whom does the onus fall in cases where privacy is needed but not provided? In some cases, indeed perhaps the most canonical ones, it will be apparent that the onus falls on regulatory bodies such as governmental agencies, or sovereign nation-states, or international treaty negotiations. Yet there are other cases in which it may be equally plausible to demand privacy protections from another party. For instance a corporation providing users with online email or social networking tools might be expected to provide sufficient protection to users' personal data. The increasing importance of privacy policies for online services providers is a testament to the recent trend toward thinking of privacy as something that rightly ought to be delivered as part of the services being used rather than thinking of privacy as a regulatory mandate imposed on these services by legal restriction. Users dissatisfied with the provisions offered by the service provider can in some instances bring a successful legal action to protect their privacy—in such cases we can witness a shift along this dimension of provision from 'service provider' to 'legal regime'. There are, of course, other cases in which the presumptive provider of privacy will be different: sometimes the privacy offender is the responsible party

[77] For instance, protections of databased personal information at an international level could be operationalized through criminal laws focused on deterrence, and yet these laws might fail to achieve their purpose when confronted by clever teenage hackers abroad who are difficult to identify and prosecute—see Mulligan and Schneider (2011). xxx Deirdre K. Mulligan and Fred B. Schneider, "Doctrine for Cybersecurity," *Dædalus, the Journal of the American Academy of Arts & Sciences* 140(4), Fall 2011.

whom should have observed extant privacy norms (the snoop) or sometimes the privacy subject will be held responsible for not sufficiently looking after their own privacy (the exhibitionist).[78]

Expert about Privacy

The notion of *expert about privacy* refers to the entities and agents who make the many determinations about privacy here under considerations.[79] The idea of a privacy expert closely overlaps with the idea of a privacy provider, yet in many cases it will be useful to analytically separate the two. For instance, it may be the case that a corporation reasonably ought to provide their consumers with a certain level of privacy protection, but that this determination is made by governmental agencies, concerned citizens, or privacy advocacy organizations such as Electronic Frontier Foundation rather than by the corporation themselves. To consider another instance, it is sometimes the case in 4th Amendment Jurisprudence that the provider (e.g., the U.S. government, a governmental agency, or a state-level agency) does not always live up to the privacy determinations made by the experts (e.g., the U.S. Supreme Court).

It remains, of course, an open and fertile question as to who should count as a privacy expert with respect to a given privacy problem. There is, in any heated moral or political contest, an ambiguity in the very idea of expertise itself insofar as epistemic and political authority itself is always fraught and contested. There is always ample room for debate on these matters, and we think this a good thing, though some debates do require resolution, even if only temporarily, so that determinations (e.g., laws) can be made. Other possible privacy experts beyond those named above including policymakers, corporate privacy officers, educated citizens, or more simply any person issuing a reasonable claim about a privacy violation. Consider as an example the current push by U.S. regulators for corporate agents to protect privacy by way of technical design through embedding affordances for privacy in their technical systems.[80] In combination with the prevailing U.S. approach to privacy as defined via (reasonable) user expectations, this amounts to not only placing the burden of *provision* on corporations but also to placing the burden of the *expert* work of specifying privacy's functioning on corporations. This suggests a

---

[78] Thelattercasesofexhibitionismareamongsomeofthemostinterestingaddressedinrecentscholarshiponprivacy,forinstanceasdiscussedbyAnitaAllen(2011)inherargumentformandatingprivacyevenwhenitisnotwanted. xxxAllen,Anita.2011.*UnpopularPrivacy:WhatMustWeHide?*Oxford:OxfordUniversityPress,2011.

[79] Seeforanexemplaryinstanceofanapproachtothisdimensionworkby ColinBennett(2008).

[80] Isthereanarticlewecancitehere?xxx

possible need for a change of approach: these corporations need to figure out how to put the burdens of privacy provision not on their legal team, but on their technical design teams.[81]

Dimensions of Context

Social Context

The idea of *social context for privacy* is meant to capture the inherent practicality of privacy. Privacy is practical only in a context of actual social practice. The range of contexts in which privacy functions, therefore, is vast. The way in which privacy functions in medical practices will be different from the way in which we expect it to function in educational practices, or in industrial practices, or in aesthetic practices. Contexts, of course, are not always carved at the joints of professions. In some cases, the appropriate context for privacy will be with respect to economic interactions, where privacy might function differently than it would in the contexts of religious practices or military engagements. Another often important feature of context is geography, for example a privacy norm may apply within the limits of a building or property line, it may apply more widely within the territory of a nation-state, or it may apply globally.

We do not here seek to limit the range of contexts in which privacy might function. Context is a famously slippery notion. Rather than forcing ourselves to gain a grip on it, then, it may be best to leave context open for contestation in just the way that privacy is. By doing so, we may be able to give ourselves the freedom to make determinations about appropriate context in those situations where it is most needful.

Scope of Context

The idea of *contextual scope of privacy* refers to the range or extent of application of privacy functions in question. It may be the case that a given privacy norm should apply universally in every possible instance or perhaps that it should apply universally within a specified social practice. In other cases, however, it may be more prudent to think of privacy norms as applying in a more granular fashion, such that casuistic case-by-case determinations need to be made. Scope thus specifies the boundedness of the application of privacy in a social

[81] CitehereDKM/KBandDKM/JKpapers

context where those bounds do not exactly match the bounds of the social context itself. For example, privacy protections for voluntarily-offered personal information in public forums might be designed specifically for online contexts or even more precisely for social media contexts—and yet we might also think that these protections do not apply universally within the use of social media because of certain important exceptions such as political figures or celebrities in whom there is a public interest. Or, to take another example, there has famously been much disagreement about whether or not privacy protections for intimacy always apply within the social context of the family—certainly everyone agrees that these protections should apply as a default, but historically there was much debate about whether or not privacy can be trumped by other more pressing problems, such as domestic battery. Specifying the scope of privacy may be useful toward honing in on other dimensions of privacy and how they ought to be adjusted in a given situation—for example, if we can gain a satisfactory determination about privacy's scope this may take us some way toward a satisfactory determination of mechanisms for privacy.

§4: Applying the Analytic: An Anatomy of Privacies

We turn now to an application of the multi-dimensional analytic for a variety of analyses that help us cast light on its flexibility for use. Our aim in this section, accordingly, is to show how an analytic approach such as that we offer here can be used to engage privacy's complexity from both prescriptive and descriptive angles. Through such an analytic approach we aim to make visible how privacy is always in contest, whether these contests be explicit or only implicit in actual practice. We illustrate with three cases, exploring a limited set of dimensions in each.

First, we applyour analytic to a statute designed to protect privacy, examining what the statute's structure says about its drafters' concept of privacy and how changes in technology and its use have shifted threats in ways unanticipated ways. , Our aim in this case is to clarify the prescriptive force of our approach, showing how a failure to analytically engage privacy's complexity leads to unnecessary missed opportunities or even sometimes downright errors. Second, we show its utility in illuminating on-the-ground privacy complaints over a contestable technological decision in the context of contemporary social media software. This case clarifies the descriptive value of our analytic approach by using it to illuminate otherwise difficult to see aspects of a privacy contest. Third, we use it to examine the competing concepts of privacy at

work in a famous U.S. Supreme Court case starkly revealing privacy's contestability. These cases reveal the utility of the thick approach to privacy facilitated by our analytic.[82]

The Electronic Communications Privacy Act (1986)

The *Electronic Communications Privacy Act* (ECPA) was adopted in 1986, driven by the conviction that strong privacy protections resembling those afforded to first-class mail and telephone conversations were necessary vis-à-vis the increasingly widespread adoption of electronic communications technologies and practices. The statute was initially praised as visionary and credited for its role legally stabilizing a wide range of communication and storage technologies due to the protection certainty it initially delivered. And yet twenty-five years later the statute is now viewed as woefully inadequate to provide the privacy protections that animated its adoption. Although the protections afforded by the statute remain, the risks to privacy have taken myriad new forms due to transformations in technology. In an effort to explain the mix of statutory provisions that slice and dice privacy protections in a seemingly bizarre fashion, scholars and practitioners have drawn attention to the objectives and justifications of ECPA and its tight tie to the specific systems and business models of the time.[83]

The logic of the seemingly incomprehensible statutory distinctions is revealed when they are considered against the historical backdrop of the system attributes, business practices, and privacy risks to which ECPA was an initial remedy. The provisions of ECPA were designed for a time when email communications and offsite processing were the state of the art. The statutory protections thus reflect, for instance, the privacy framework governing postal mail to which electronic communications were analogized. The resulting protections for electronic communications therefore focus on limiting access to the content of the communication based on an assumption that the addressing information already exposed as the 'envelope' of the message will be disclosed.

---

[82]Twocompanionempiricalprojectswillhelpmakethispointfurther.Thefirstinvolvesananalysisofconsumerprivacycomplaints.Thesecondinvolvesahistoricalgenealogyofaspectsofcontemporaryinformationprivacy.Inbothprojects,ourintentionthusfarhasbeentousethetaxonomyelaboratedheretoanalyticallydiscriminatenewqualitiesofprivacyconcernsastheseariseontheground.Inyetathirdcompanionprojectmappingcontemporarytheoreticalarticulationsofprivacyourintentionistousethetaxonomy(specificallytheaforementionedtheoreticaldimensions)todiscriminatearangeofdifferenttheoriesofprivacysoastoilluminatehowdifferenttheorieswieldexplanatorypower(ornot)withcertainformsofnewprivacycomplaints.Togethertheseapplicationsdemonstratesomeofthewaysinwhichourmulti-dimensionalanalyticalapproachtoprivacyhaspayoffforboththeoryandpractice.

[83]Insertcite?xxxCritic/discussionofECPA?

While email remains a core use of electronic and networked communications, the subsequent widespread use and development of the internet and the web platform have facilitated new uses that invert the assumptions upon which the postal mail analogy for electronic communications relied. For example, user-generated content sites are used to share and disseminate the content of communications, yet often do so pseudonymously or anonymously. Further, regardless of whether specific efforts are made to withhold identifying information, these communications do not depend upon the disclosure of user-specific addressing information on a message "envelope." The statutory framework of ECPA provides weak privacy protections for the identifying information held by providers such as Google, YouTube or Facebook, allowing the police as well as private parties to access them with relative ease. In contrast, the content of the communication held by service providers is afforded relatively strong protection against government access and off-limits to private litigants. But of course, the relatively strong privacy protections for content provide little comfort to anonymous or pseudonymous users posting publicly accessible content on such sites.

Lacking analytic tools to guide statutory drafting processes aimed at protecting privacy, the drafters of ECPA resorted to analogies that over-simplified the problems at hand. As technology changes, staying true to the *objectives* and *justifications* at the heart of the legislative effort requires protection for a new set of *targets*. In the case of ECPA, the assumption about how emergent technologies would be used (namely, as a replacement for mail and telephone communications) drove a statutory framework oriented around the protection of a specific set of privacy *targets*. Precisely because ECPA was focused around specific targets, it lacks the flexibility to suitably expand these targets of protection to achieve broader objective and justificatory functions when those functions shift in the context of newly-emergent technical-social targets. Although analogies are useful in motivating action (often providing otherwise unconcerned actors with vivid *exemplars*), they nonetheless risk embedding invisible assumptions about the dimensions of *protection* (that is, *target* and *subject* of privacy) and the dimensions of *harm* (that is, the *action* against privacy, the *offender* against privacy, and *from-whom* privacy is meant to protect us) that can limit a statute's ability to evolve protections midst changing contexts. In this way, then, it can be seen how the complexity of privacy revealed by our analytic can be a useful and sometimes even needed tool in the difficult work of drafting privacy-relevant statutes and privacy policies that build in flexibility around definitions of

protection and harm creating more dynamic and malleable provisions while also strengthening their clarity and rigor. To the extent that a failure to analytically engage complexity leads to protections that entrench rather than evolve existing habits of practice, there is a strong sense in which actors involved in creating protections should (rather than merely could) make use of tools that help tease apart the many dimensions of privacy.

Facebook News Feed (2006)

In September of 2006 Facebook introduced a new feature that transformed users' status updates, from posted information available to user approved visitors to a profile page, to a "News Feed" pushed out to those approved individuals, namely all those on the Facebook user's "friends list."[84] The feature provided no additional ability to distinguish among "friends" for the purpose of sharing status updates, nor could News Feed be disabled. From the recipient perspective the feature produced a "glitzy laundry list" containing status updates from all the recipient's "friends."[85] The initial response of Facebook's users was negative, with one anti-News Feed group gaining 10,000 followers on the release day. Notably neither the information being provided nor those authorized to access it had changed, nonetheless disgruntled users claimed a privacy violation. In response to user pressure, Facebook improved aspects of its privacy controls, providing users with some tools to manage some of the types of information posted to the Feed.[86]

---

[84]SeeSanchez(2009)andSimmons(2011).
AndrésSanchez,*FacebookFeedingFrenzy:Resistance-through-DistanceandResistance-through-PersistenceintheSocietiedNetwork*,6SURVEILLANCE&SOC'Y275(2009),*availableat*
http://www.surveillance-andsociety.org/ojs/index.php/journal/article/viewFile/frenzy/
frenzy;ToddSimmons,TheEthicsofPrivacyonFacebook(Apr.4,2011)(unpublished
MBApaper,St.Edward'sUniversity),http://todd-simmons.com/docs/
MBA10_GlobalDigital_PrivacyEthics.pdf.

[85]SeeSchmidt(2006).
xxxSchmidt,Tracy."InsidetheBacklashAgainstFacebook."*Time*,Sept.6,2006.Availableat:http://www.time.com/time/nation/article/0,8599,1532225,00.html

[86]"FacebookRespondstoUserFeedbackandReaffirmsPrivacyasTopPriority"Facebook.com,September8,2006.Availableat:http://newsroom.fb.com/News/220/Facebook-Launches-Additional-Privacy-Controls-for-News-Feed-and-Mini-Feed.(xxx"Thenewprivacypageincludesindividualsettingstoblockinformationon NewsFeedandMini-Feed,includingwhenauser:removesprofileinformation,postsonaWall,commentsonaNoteorphoto,postsonadiscussionboard,addsafriend,removesrelationshipstatus,orleavesagrouporanetwork.Asettingtoremovethetimestampofpostingson Mini-Feedhasalsobeenadded.InNewsFeedandMini-Feed,Facebookdoesnotpublishinformationabout Pokes,Messages,whoseprofileauserviews,whosephotosauserviews,whoseNotesauserreads,groupsandeventsauserdeclinestojoin,peopleauserrejectsasfriendsorpeoplewhoauserremovesfromtheirFriendList.").

The user response to News Feed's introduction highlights the need to appreciate the various and distinct dimensions involved in the protection of privacy. In the vocabulary of our taxonomy, the significant shift at play has to do with the subtleties of privacy *mechanisms* at play here, especially as these are related to the different *subject* positions through which privacy was sought *from* an invariant group of 'friends'. On our analysis, The switch in technology at issue in the News Feed case worked in an almost invisible way to reduce the mechanics of privacy protection that transaction costs and background norms afforded to various affected actors . Accordingly, there is a real and meaningful contest over privacy in this case, but we are led away from noticing this contest if we do not pay attention to the privacy mechanisms involved as they related to various other dimensions of privacy.

The introduction of News Feed raised several distinct kinds of objections from Facebook users. The objections can be understood as concerned with the shift from a pull to a push distribution model, that is from a billboard presentation of an individual's recent activity at her profile page available to "friends" industrious and curious enough to 'pull' this activity by visiting the page to a broadcast 'push' of recent activity indiscriminately to all "friends". This shift substantively altered the experience of sharing. By contrast to this shift in experience, defenders of News Feed sought to point out that all the user information involved had always been and still remained 'public' under terms of service. This defensive reaction is, we think, based on a misperception of the complex workings of privacy involved. Focusing on the background issue about whether or not the user information in question was always public serves to mask the foreground dynamics of privacy at stake. This shows why we need tools that facilitate more accurate descriptive analyses of privacy's complexity. We turn now to showing how an inquiry into user criticisms of this shift using our analytic is one way to get a fuller picture of what went on.

In response to the introduction of News Feed, Facebook users raised two sorts of privacy complaints. First, users complained of the increased exposure created by the push. As one Facebook user commented, "Stalking is supposed to be hard."[87] Now News Feed had made it easy. Another Facebook user drew a comparison to the availability of public records online, writing, "While it might seem a little hypocritical because you're [the one] making the

[87] Reuters, "Angry Students Lash Out at Facebook.com Privacy Changes," September 8, 2006.

information public, no one wants someone watching their every move… You can learn a lot about someone from those records even though as separate entities they don't mean anything."[88] A second privacy complaint was framed from the perspective of recipients of the news feeds. Users as recipients complained that they being "spammed" by their friends. As summed up by one user: "Personally, I don't have a problem with the information being there. I just have a problem with that HUGE amount of information in my face all the time."[89]

Much of the contemporaneous reporting as well as the legal disputes and academic literature framed Facebook News Feed's privacy problem as a failure to provide users with the opportunity to choose to participate in the service as a sender. Yet, we think that the privacy claims asserted above are more complex. Different concepts of privacy, different claims to protection, and perhaps most importantly different mechanisms are in play—the contest over privacy in question here is thus not simply about opt-in and opt-out choices. To demonstrate this, we shift gears now from a description of the background of the case to an analysis of the many dimensions of privacy that were there at play.

One of the most interesting features of the News Feed case is the variance with respect to the *subject* of privacy, that is, in our language, the agents whom privacy is designed to protect. News Feed generated concerns over privacy from two distinct subject positions, namely the positions of what we will call 'data subject' and 'information recipient'. Users in the position of data subjects noted that the shift from pull to push made information more readily accessible to their friends. Users as information recipients objected to the shift in mechanism because of the deluge of status updates it released. This distinction, though seemingly obvious, is important for analyzing the concepts of privacy at play in the News Feed case. For, as our analysis below shows, much hinges in these complaints on the explicit or implicit subject of privacy at issue.

In the complaints about News Feed, privacy was also variably invoked in the service of a range of differing *objects*. The first set of complaints, offered from the perspective of the Facebook user as data subject, would deploy privacy to limit access to the self. While the self in this case is a digital representation, and one that is in many instances surely crafted to portray a

---

[88]Commentbyadf2006(998737)onTuesdaySeptember052006,@10:46PM(#16049553)FacebookChangesProvokeUproarAmongUsers,Slashdot,September5,2006.

[89]Enoxice(993945)onTuesdaySeptember052006,@10:47PM(#16049561)FacebookChangesProvokeUproarAmongUsers,Slashdot,September5,2006

specific self the individual desires to project into the world, it is nonetheless a manifestation of a real individual who has rights and interests concerning access to that self. One could argue that the object that privacy is deployed to protect in this first set of complaints is "control over personal information," however the terms used to voice the objections "stalking", "watching," and "monitoring" speak to concerns with surveillance of the individual enabled by the News Feed feature rather than to concerns about access to the information itself: "You can learn a lot about someone from those records even though as separate entities they don't mean anything."[90] This user comment illustrates both the link to information, in its use of the term records, and its focus on the self, as reflected in its concern that the composite comprised by the bits of information divulged have a broader implication beyond their separate parts. In the second set of complaints, voiced from the subject position of information recipients, by contrast, users objected to News Feed because it intrudes on the individual. Prior to its introduction, information was available to "friends" but "friends" retained independent control over whether and when they were received. The shift to News Feed bombarded individuals' Facebook friends. The content of the informational assault unleashed by News Feed ran from the important and profound to the trivial and mundane. With the introduction of News Feed "sharing" information with friends became more akin to incessantly calling or texting them to update on often unremarkable events and observations. The *object* of privacy protection in the claims from recipients is also best understood as an interest in limiting access to the self, though here the object takes on a different sense correlative to the different subject position involved. Recipients objected to News Feed because it taxed their time and attention span.

Moving to the dimension of privacy's *justification*, we again see a variable range of approaches. On the one hand, complaints from the perspective of the sender and recipient of News Feed appear to justify privacy in terms of its importance to the "friend" relationship as constructed on Facebook. The transaction costs that limited both access and exposure to status updates prior to News Feed was, it appears, key to the construction of the category "friend" on Facebook. The justifications for the desired privacy protection are grounded in connection and community: they facilitate friendship. While the complaints can also be understood to justify

[90]Commentbyadf2006(998737)onTuesdaySeptember052006,@10:46PM(#16049553)FacebookChangesProvokeUproarAmongUsers,Slashdot,September5,2006.

privacy based on autonomy, liberty, and dignity, reading them as such misses the deeper basis. A justification based in connection or community seems particularly important in understanding this privacy conflict given that the choice to share information had already been exercised by the data subject and to some extent by the recipient who had not defriended them. Robert Post's conception of privacy as "rest[ing] not upon a perceived opposition between persons and social life, but rather upon their interdependence" is reflected in the dynamic way this change in the form of access to status updates affected social relations.[91] The initial 'pull' distribution model protected two privacy interests perceived as central to the terms of the Facebook friend relationship. The pull paradigm facilitated rampant sharing and rather promiscuous friend-ing, based upon an expectation of limited actual revelation of information. While updates were available to a relatively broad audience they remained practically obscure. The tacit understanding, expressed in user comments, was that only a limited group of their Facebook friends—their true friends, their close friends, or their family—would exert the effort necessary to scrutinize their activities and musings. Importantly, the pull paradigm also encouraged users to post relatively indiscriminately. Because their friends retained ultimate control over their actual exposure to posts, posters had limited reason to fear being perceived as a nuisance or an intrusion.

A full understanding of the privacy objections to Facebook News Feed requires engaging the dimension of privacy we refer to as *mechanism*, interrogating also the mechanics of privacy in its relation to the dimensions discussed above. In public statements defending News Feed Facebook founder Mark Zuckerberg argued that News Feed maintained the status quo with respect to privacy because it did not alter the *policy mechanisms* Facebook put in place to facilitate user decisions about privacy.[92] Facebook was honoring its users' decisions about who should have access to what as reflected in user settings. But this defensive attitude missed the point of user concerns. Users' objections were about the dissolution of another privacy mechanism, namely the transaction costs associated with the pull paradigm that previously governed access to status updates. While information was still withheld or shared with friends

[91] Post1989,959
xxxPost,Robert.1989."TheSocialFoundationsofPrivacy".xxx
[92] Needcitesxxx

on the terms users specified, it was now broadcast. News of users' activities went from being pulled-in by friends to being pushed-out to them and as a result the sharer faced far greater actual exposure. Data that once had to be actively sought by one's friends (or the broader public if the user had so chosen) was now swimming before the eyes of the audience as a routine matter. The transaction costs associated with accessing the user (represented by their newsfeed) were diminished, leading subjects to feel exposed, scrutinized and stalked, and recipients to feel deluged and intruded upon. In considering a case such as this, we need to give careful consideration to the full range of mechanisms at play—in this case, beyond formal policy or law, the reduction in transaction costs associated with accessing information about friends is significant for individual privacy. Individuals managed their privacy not only through engagement with Facebook's policy mechanism that allowed them to choose who could access certain information, but also through the additional transaction costs the pull mechanism placed on those with authorized access. The time and energy required to discover accessible information mediated the relationship between the individual and the audience. The technical mechanism provided a tacit privacy protection, what we might think of as a kind of social expectation mechanism, that users apparently relied upon to further control audience.

The dimension of *privacy-from-whom* yields further insight into the mechanism at work in the News Feed privacy problem. Facebook users were seeking to maintain privacy from some subset of their Facebook "friends." While profiles were hypothetically available to all friends, effort was required to follow a friends' daily life through their Facebook profile. It was widely understood that the category of "Facebook friends" bore little resemblance to the category of friend operating in the rest of an individual's life.[93] Surely a Venn diagram of Facebook friends would include a subset of friends, however it would also include random acquaintances, colleagues, parents of children's friends, etc. By stripping out the transaction costs News Feed removed a mechanism that users thought afforded privacy by further segmenting the audience of friends whom regularly viewed their profile. Facebook's *policy and privacy controls*—the *mechanisms* Facebook focused on—had not changed. Users' maintained control over the audience privy to their status updates. However, the change in the technology—from pull to

[93]On shifting conceptions of 'friendship' see danahboyd, "*Facebook's "Privacy Trainwreck": Exposure, Invasion, and Drama*," APOPHENIABLOG (Sept.8,2006), http://www.danah.org/papers/FacebookAndPrivacy.htm

push—removed a technical mechanism that users relied upon to protect their privacy. The removal of this implicit boundary mechanism collapsed the line between the theoretical and actual audience leaving users with the uncomfortable feeling of being both exposed and assaulted.

Kyllo v. U.S. ***(2001)***

During an investigation of a marijuana cultivation and distribution operation in coastal Oregon a federal agent used a thermal imaging device to scan the outside of Kyllo's home. The resulting thermal image reading was used in conjunction with other information to obtain a warrant to search the house. Kyllo moved to suppress the evidenced recovered pursuant to the search of his home arguing that the use of the thermal imaging device to scan it was an invasion of the reasonable expectation of privacy protected by the Fourth Amendment. The Supreme Court ultimately held that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use."[94]

In the language of our taxonomy, one key feature of the case is that the parties involved disagreed over the *object* of privacy under contention. The government argued that Kyllo had no expectation of privacy in "the heat emitted from his house" while Kyllo argued that what privacy protected was the "private activities" occurring within the home. The case was ultimately determined to be about the "use of technology to pry into our homes"[95] and the related matter of the sanctity of "private lives."[96] During oral argument the Justices drew attention to evidence provided to the appellate court revealing that a thermal image reading could "show[ed] individuals moving… inside the building"[97] although it had not in this case.[98] Justice Souter forcefully stated that what was at issue was *not* the data, but "what's going on in the house." The tension over what object should be the focus of the privacy inquiry reveals the slipperiness of the term and its capacity to create illusions of agreement where significant disagreement remains.

[94]Kyllov.UnitedStates,533U.S.27,34(2001).
[95]KYLLOv.U.S.,2001U.S.Trans.LEXIS11(U.S.Trans.2001)at18.
[96]Id.at21
[97]KYLLOv.U.S.,2001U.S.Trans.LEXIS11(U.S.Trans.2001)at6.
[98]Id.at8.

The Court *justified* its decision to prohibit the use of thermal imagers absent a warrant in order to protect the privacy of in home activities on the basis that "at the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[99] The privacy the ruling affords in home activities is justified by the need to limit the government's access to individuals' private lives. This is a classic justification for privacy in American law, reflected in the influential 1890 article by Samuel D. Warren and Louis Brandeis, in which they set forth a conception of privacy in terms of what they call "the right to be let alone" which is grounded in the idea of freedom from intrusion upon seclusion,[100] as that freedom had found expression in seminal Fourth Amendment cases.[101]

§5: Benefits of the Contestability of Privacy

Privacy is a severely contested concept. Our analytic provides a richer language for understanding privacy disputes. Our hope is that, in turn, this might facilitate more productive and reflective debates over privacy. We believe that the rigor of close analysis helps elucidate the critical importance of privacy's contestability as a basis for the innovation of privacy rather than as a debt in privacy itself that must be paid out.

We are well aware that contestability in its many forms always poses problems insofar as it can easily be used as cover for equivocation, sloppy inference, and invalid argumentation. Privacy, when left as a black box, facilitates political posturing rather than deliberative dialogue—it is often wielded not to engage, but to silence. Leaving privacy in disarray allows us to avoid the complicated and nuanced conversations that are required to maintain privacy midst its contestability. Thus, taking up privacy's contestability through analytical frameworks can help pinpoint key areas of dispute and agreement can keep privacy in play. More nuanced analytical models may thus help us to retain the heat and fervor in privacy debates whilst also increasing the capacity to illuminate the sites of struggle and therefore facilitate more productive engagement, more agile innovation, and even at times more satisfying resolutions. This is a

[99] Kyllo at 31 (internal quotations omitted)
[100] xxx Warren, Samuel and Brandeis, Louis. 1890. "The Right to Privacy" in *Harvard Law Review* 4, 1890: 193-220.
[101] Boyd v. United States, 116 U.S. 616 (1886)

much-needed alternative to the doomsday-ing and nay-saying too often kindled in today's fiery debates over privacy.

In a 1997 article titled "The End of Privacy" Richard Spinello sought to draw attention to "the stark reality that our personal privacy may gradually be coming to an end."[102] This sentiment has been more recently echoed by a host of Silicon Valley minor celebrities, including Facebook co-founder Mark Zuckerburg and Sun Microsystems co-founder Scott McNealy.[103] The force of these provocations cannot be denied by anyone able to grasp the long and slow drift of privacy's subtle erosion over the course of the last few decades.

What is not, however, clear is what it would mean for something as central to our culture as privacy to come to an end. We would argue that anything like a fully transparent society is well beyond the powers of our imagination let alone our powers of rational anticipation. Privacy is too much a part of us—it defines us. As moral philosopher Thomas Nagel astutely observes, "There is much more going on inside us all the time than we are willing to express, and civilization would be impossible if we could all read each other's minds."[104] To put Nagel's point a little more modestly: if we did not have privacy in some of the forms it takes for us today, then we would not be able to inhabit the modern forms of life that are central to nearly all of our self-understandings. Our view is that privacy is not disappearing, but is rather undergoing radical, in the full sense of that word, transformations. Perhaps these transformations are even so radical that what we will have to work with on the other side may no longer be recognizable as the privacy we all once knew, or at least thought we all knew. This is the worry that Nagel poses in noting "the culmination of a disastrous erosion of the precious but fragile conventions of personal privacy in the United States over the past ten or twenty years."[105]

---

[102] xxxSpinello
Spinello,RichardA.1997."TheEndofPrivacy"in*America*176,Jan.4,1997:9–13.
[103] GetCites….Xxxjuicyquoteswouldbegood.
xxxTheoft-
citedphrase,"Youhavezeroprivacyanyway,getoverit,"hasbeenattributedtoScottMcNealy,formerCEOofSunMicrosyste
ms.PrivateLives?NotOurs!,PCWORLD(Apr.18,2000,12:00AM),http://www.pcworld.com.article/16331/privatelives
notours.html
[104] Nagel1998a,4
XxxNagel,Thomas.1998a."ConcealmentandExposure"inNagel,xxx.
[105] Nagel1998b,27
xxxNagel,Thomas.1998b."TheShreddingofPublicPrivacy"inNagelxxx.

So are we losing a grip on the value of privacy? Privacy is doing more work than ever, and precisely for that reason has spread itself thin in going wide. Hence privacy is ineradicably contestable for us today. But privacy's contestability is one of its strengths, at least in theory, and armed with tools such as our analytic, it can be so in practice too.

A richer understanding of the plurality of objects, justifications, paradigms, mechanisms, agents, targets, and sites (and so on) of privacy that are operative in our culture provided by our multi-dimensional analytic for privacy is a key tool for understanding and advancing privacy. Our analytic provides a framework for exploring and explicating the richness of privacy in all its ambiguity, vagueness, and uncertainty, and in the varied contexts of its contestation. Such explorations and explications require a sustained practice of what pragmatist philosopher John Dewey called inquiry—demanding practical experimentation and learning just insofar as we cannot always know outcomes in advance of actual practical effort.[106] This is the only way that we can come to test, in practice, the plurality of privacy values endorsed in one instance or another. It is also the only way that we can leverage the existing riches of our privacy tradition into that uncertain future where the threats to privacy are perhaps greater than ever and at the very least different.

Without respect for the values of privacy we shall lose something that we all value in one way or another, and if we lose that we may indeed lose everything. The question we face today is no longer that old one set in false dilemmas between privacy and publicity, or privacy and surveillance, or privacy and security—the question today, in other words, is not: "Privacy, yes or no?" The question we face today concerns the plurality of privacies available to us: "Which privacy? For what purpose? With what reason? As exemplified by what?" A multi-dimensional analytic is just one useful tool in the ongoing project of answering these questions. This project is valuable just insofar as these questions are critical for understanding privacy, valuing privacy, and implementing privacy. These questions, in other words, are critical just to the extent that our culture is predicated not only on the maintenance of privacy itself but also on the very contestability of whatever forms of privacy we would work to maintain.

---

[106] On the notion of inquiry as learning in a problem-resolving manner see Dewey 1938, Chapter 6.
xxx Dewey, John. 1938. *Logic: The Theory of Inquiry*. Carbondale: Southern Illinois University Press.

xxxAcknowledgments Note.[107]

[107]xxxReaders/discussants.
Readers
ChrisHoofnagle
RyanCalo
JenKing
ShariP???
Others
PLSCaudience(specificnames?Solove?AnitaAllen?HarrySurden?)/s
XxxAnyrelevantgrantsetc..I3P?
XxxCollaborators?NickandJen(others?)