PHILOSOPHICAL TRANSACTIONS A

rsta.royalsocietypublishing.org

Research

Cite this article: Mulligan DK, Koopman C, Doty N. 2016 Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Phil. Trans. R. Soc. A* **374**: 20160118.
http://dx.doi.org/10.1098/rsta.2016.0118

Accepted: 3 October 2016

One contribution of 15 to a theme issue 'The ethical impact of data science'.

Subject Areas:
privacy design, privacy ethics, privacy law, technology ethics

Keywords:
privacy, data science, design, privacy analytic, privacy by design, values in design

Author for correspondence:
Deirdre K. Mulligan
e-mail: dmulligan@berkeley.edu

Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy

Deirdre K. Mulligan[1], Colin Koopman[2] and Nick Doty[3]

[1] University of California, Berkeley, School of Information, and Berkeley Center for Law & Technology, Berkeley, CA 94720, USA
[2]University of Oregon, Center for Cyber Security and Privacy, and Department of Philosophy, Eugene, OR 97403, USA
[3]University of California, Berkeley, School of Information, and Center for Technology, Society & Policy, Berkeley, CA 94720, USA

DKM, 0000-0003-2693-8454

The meaning of privacy has been much disputed throughout its history in response to wave after wave of new technological capabilities and social configurations. The current round of disputes over privacy fuelled by data science has been a cause of despair for many commentators and a death knell for privacy itself for others. We argue that privacy's disputes are neither an accidental feature of the concept nor a lamentable condition of its applicability. Privacy is essentially contested. Because it is, privacy is transformable according to changing technological and social conditions. To make productive use of privacy's essential contestability, we argue for a new approach to privacy research and practical design, focused on the development of conceptual analytics that facilitate dissecting privacy's multiple uses across multiple contexts.

This article is part of the themed issue 'The ethical impact of data science'.

1. Introduction

The 1970s were a watershed period for privacy. The growing use of mainframe computers by States and large corporations, coupled with controversies around State use of personal data to take often covert, illicit actions against citizens, drove policy-makers to grapple with the implications of this heady mix

THE ROYAL SOCIETY PUBLISHING

of data and computation. Experts and policy-makers convened to explore the risks and develop protections for privacy. A shared set of fair information practice principles—reflecting a commitment to protecting informational self-determination—emerged on both sides of the Atlantic [1,2].

After years of consultation and debate, fuelled by the entrepreneurial activity of a growing community of privacy professionals, these principles now form the basis of numerous countries' personal data or information privacy laws, as well as the organizing framework for much institutional and professional work across the public and private sectors. The principles have proved admirably suited to advance specific conceptions of privacy through tumultuous technical advances. They have been leveraged to protect the individual's right to informational self-determination in multiple spheres of economic life, and to address risks emerging from the introduction of technologies ranging from electronic health records to radio-frequency identification tags.

However, these principles have proved less useful with the rise of data analytics and machine learning. Informational self-determination can hardly be considered a sufficient objective, nor individual control a sufficient mechanism, for protecting privacy in the face of this new class of technologies and attendant threats. Privacy harms may arise for which individual control offers no protection or remedy, for example, when actions are taken based on group classifications [3], or new and unexpected insights are inferred from data that individuals have intentionally disclosed [4,5], or an individual's sensitive personal information is derived through analysing data revealed by others in their social network [6], their behaviour on social media [7] or by cross-referencing sets of 'de-identified' data in which they are included [8]. Such privacy harms stem from information, yet they are not addressed by strategies centred on individual control over information. These are among the most pressing challenges to privacy in a world riddled with large sets of data representing individuals' actions, transactions, interactions, physiology, beliefs, states and expressions, all algorithmically processed as grounds for making decisions about persons.

Despite their inability to speak to or remedy these emerging privacy problems, the legal regimes and professional practices that embed fair information practice principles have proved amazingly resilient. While there are vast differences in implementation, the European Union's General Data Protection regulation, as well as the mix of constitutional, legislative and agency activity that comprises the bulk of information privacy law in the USA, continue to focus on preserving individual control over information through a range of limitations on the collection, use, disclosure and processing of personal information. In the shadows of these large legal regimes, scholars and practitioners have advanced alternative conceptions of privacy that address the new risks of data science, machine learning and other technological innovations. Scholars have argued for privacy concepts and approaches that unburden the individual by attending to the contextual norms of spheres of social life [9,10], address risks posed by ancillary data [11] and attend to the emerging semantics of machine learning [4]. Professionals have developed new concepts, such as 'trust' and 'meeting expectations', and contrast concepts such as 'creepiness', in an effort to address the shifting privacy concerns of customers and citizens [12]. Privacy regulators have expanded their work as well, branching out into information ethics in response to the challenges posed by big data [13].

The limited guidance offered by informational self-determination as a core conceptual component of privacy presents a challenge and an opportunity to expand the way we conceive of privacy, its risks and our strategies for protection. As we bump up against the limits of informational self-determination, we must reflect on what gets lost when we reify privacy as just one thing—one principle, one formalization, one method of protection. We must engage with the whole tangled, ambiguous and essentially contested terrain of privacy. And yet, at the same time, the need to build privacy values into data science demands that we clarify the purposes that privacy serves, the justifications that animate it and the actions that put it at risk. Meeting these goals simultaneously is not easy, but it should be the central agenda of privacy research today.

We could avoid this agenda in numerous ways. We could seek a new definition to replace, or augment, informational self-determination and develop corresponding tools to protect privacy as redefined. We could decide that the suite of problems arising due to data analytics and machine learning are not privacy problems at all, and find them a separate conceptual home. Or, recognizing that privacy has reached this juncture before and will do so again, we could adopt the aforementioned agenda and take a more radical approach.

We advocate a more radical approach: *embracing privacy as an essentially contested concept* in order to shift the focus of research towards developing tools that facilitate our ability to work with privacy's multi-faceted and open-textured meaning. Such an approach is viable, however, only if contests over privacy can be seen as generative and productive, rather than as an excuse to dismiss privacy as a muddle or a myth, or even worse as an excuse to exert power. To further this approach, we here offer an analytic tool for mapping the many kinds of arguments, disputes and disagreements in which privacy is suffused. Mapping these contestations is crucial to realizing their generative value to privacy. We begin by surveying a notion of essentially contested concepts; we then show that this notion characterizes privacy today; on this basis, we describe the implications for designers and data scientists; and finally, we present an analytic approach to grasping privacy's value amidst its contestedness.

2. Essentially contested concepts

In 1956, W. B. Gallie argued that 'there are concepts which are essentially contested, concepts the proper use of which inevitably involves endless disputes about their proper uses on the part of their users' [14, p. 169]. Gallie sought to counter the false dilemma according to which concepts are either clearly delineated or badly confused. He argued instead that a concept is essentially contested where disputes about its 'essence or central meaning' are both paramount and central to the concept itself. Such concepts—for example, democracy, art, freedom—'evoke[s] disagreement not only about marginal cases … but also about paradigm or core cases' [15, p. 149]. Essentially contested concepts 'are present to us only in the form of contestation about what the ideal really is' [15, p. 151]. Part of their work in the world is to provide the venue for 'a particular sort of adversarial discourse' [16].

In claiming privacy as an essentially contested concept, we argue that contests about privacy and the ambiguity of meaning that they simultaneously beget are battles for its core and essential to its functioning. Concepts of privacy compete against one another at the level of both theory and practice. This suggests the usefulness of Gallie's theory in this domain insofar as, as Garver notes, '[c]oncepts are essentially contested only derivatively, because they are employed in essentially contested arguments' [17, p. 258] implying that '[p]artisans, not theorists, determine whether a conflict involves an essentially contested concept' [17, p. 258].

Scholars of privacy know well that it is a concept widely regarded as contested in practice. Sociologist Alan Westin, in his landmark 1967 book *Privacy and freedom*, penned this 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' [18, p. 5]. Philosopher of law Judith Jarvis Thomson, in a 1975 article expressing scepticism about the coherence of the very concept of privacy, wrote that: 'the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is' [19, p. 295]. More recently, legal theorist Robert Post notes that '[p]rivacy 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' [20, p. 2087]; and privacy theorist Daniel Solove simply pronounces it 'a concept in disarray' [21, p. 9].

However, not all contested concepts are essentially contested. Some are simply what Gallie referred to as 'radically confused'. In these cases, confusion can be abated by either a new meaning that engenders widespread agreement among prior disputants, or decomposition of the polysemous concept into a number of different but related concepts. Viewed in this light, we can say that legal theorists, philosophers and practitioners have generally sought to overcome

privacy's contestability in ways that involve treating privacy as simply confused. Some attempt to reduce ambiguity by narrowing the range of ideas that fly under privacy's banner, while others attempt to legitimize ambiguity through heuristics that bound multiple concepts of privacy.

Meanwhile, some have recently developed a different approach to privacy that focuses on situated practice. These bottom-up approaches promise to sidestep the idea that barriers to privacy protection are erected by privacy's ambiguity and vagueness.

For example, Helen Nissenbaum has developed a theory of informational privacy as contextual integrity [9]. This theory aims to provide a justification for personal information privacy grounded in two norms—'appropriateness' and 'distribution' (or 'flow')—that Nissenbaum argues are individually necessary and jointly sufficient for privacy. The norm of appropriateness picks out what personal information can be appropriately revealed in a given context. The norm of flow is informed by work in social theory, including by Michael Walzer and Pierre Bourdieu, claiming that modern societies are characterized by a plurality of distinct spheres of practical activity, each of which is governed by its own internally negotiated values such that what is acceptable in one sphere may be radically inapplicable to other spheres. Nissenbaum's norm of flow helps pick out 'whether [information's] distribution, or flow, respects contextual norms of information flow' [22, p. 141]. Both norms of appropriateness and flow are contextually variable yet omnipresent. In every context, some norms of appropriateness and flow are applicable, though (presumably) no norm of appropriateness or flow is applicable in every context, thus 'distributing social goods of one sphere according to criteria of another constitutes injustice' [22, p. 145] and where the social good so distributed is personal information, the form of injustice constitutes a privacy violation.

For another example of this approach, consider the work of legal theorist Daniel Solove. Rather than attempting to displace extant privacy concepts with a single unitary concept, even if a flexible one, Solove deploys Ludwig Wittgenstein's famous metaphor for language to develop a pluralistic 'family resemblance' method of conceptualizing privacy [21]. Following Wittgenstein's argument that it is often pointless to try to develop formal singular definitions of certain terms (e.g. that of 'game'), since in actual linguistic use such terms overlap and criss-cross in a variety of ways [23], Solove argues that 'privacy is not one thing, but a cluster of many distinct yet related things' [21, p. 37]. Solove develops a taxonomy of 16 distinct privacy harms arranged across four categories of information collection, information processing, information dissemination and invasion. His pluralist approach decomposes privacy into a set of discrete but related concepts while maintaining a contextual, open-ended and flexible approach to deployment.

The directions taken by Nissenbaum, Solove and others [24–28] are appealing in that they facilitate privacy research in the face of the contestability that some have used as an excuse for dismissing privacy's contemporary relevance altogether—perhaps best exemplified in former CEO of Sun Microsystems Scott McNealy's famous claim, 'You have zero privacy anyway, get over it'. Both Nissenbaum and Solove work past privacy's disarray while retaining its multiplicity. Yet neither engages head-on with privacy's essential contestability. Thus, their efforts advance privacy work, but in ways that risk diminishing the generative power of contestability.

Recognizing privacy's essential contestedness is key to securing its generativity for generations to come. Privacy's ability to respond to problems created by technology and societal change is essential to its ongoing relevance. Essential contests are, notes Gallie [14, p. 184], an 'actual inchoate condition of growth'. By recognizing privacy as essentially contested, we acknowledge that rival uses are 'not only logically possible', and 'humanly' probable, but also of 'permanent potential critical value' [14, p. 193]. It is ongoing debates about privacy's meaning and application that ensure its relevance to tomorrow's challenges. Privacy's open texture, and the existence of multiple conceptions of the concept contesting at the level of theory and application, enable this concept to do its most meaningful work. These, then, would be the advantages of working with privacy's essential contestedness.

But is privacy actually an essentially contested concept? In the following section, we argue that it is. On that basis, we will then turn in §4 to delineating important implications of this view for the direction of privacy research and the practice of data science today.

3. Evaluating privacy's essential contestedness

Gallie sets out an analytic framework consisting of seven criteria for essentially contested concepts. The criteria are as follows:

- *Appraisiveness*. The concept must signify or accredit a valued achievement.
- *Internal complexity*. While the concept's 'worth is attributed to it as a whole' [14, p. 172], it must be a 'normative concept[s] with a certain internal complexity' [15, p. 150]; it must be multi-dimensional, allowing for different principles of operation, different values to be served, and different objectives and justifications.
- *Diverse describability*. Owing to the internal complexity, disputants can describe the concept in different ways, using different features and according them different weight.
- *Openness*. The concept must allow for unpredictable and unprescribed changes over time to address evolving circumstances.
- *Reciprocal recognition*. Conceptions of the concept must be used and maintained against other uses both aggressively and defensively. Gallie's claim requires that disputants must recognize the contestation and have some sense of the underlying criteria at the source of the disagreement with others; however, many have questioned whether mutual recognition is required.
- *Exemplars*. The competing conceptions of the concept must derive from an original authoritative exemplar (generally thought to allow for multiple, rather than a singular, paradigmatic example) acknowledged by all disputants.
- *Progressive competition*. The continuous contestation must contribute to sustaining and/or developing the concept in an optimum manner.

(a) Appraisiveness

Gallie's first condition requires essentially contested concepts to be appraisive. In Gallie's examples—art, democracy and being a champion athlete—the concepts are certainly typically considered achievements. While Gallie's initial formulation focused on the appraisive nature of the concept—the 'sense that it signifies or accredits some kind of valued achievement' [14, p. 171]—others have refined the understanding of appraisiveness, explaining that essentially contested concepts are evaluative (positive or negative) and descriptive. Privacy is appraisive—the best, most true conception of privacy is both hotly contested and normatively desirable. While the results of its use are not always positive, and those who can demand it do not always choose to avail themselves of it, it is always valued, and those who can successfully claim privacy have power over those who cannot. Being able to secure one's privacy against the State or other individuals is a valued achievement.

We see privacy as appraisive in that typical debates over privacy share the common assumption that privacy is a good thing to have, that it is good for society or at least for the individual. Even in controversies where privacy is argued by some to be on the whole negative (the alleged ability of terrorists to keep their communications private from law enforcement agencies, say), this is typically not because support for privacy is not something to praise, but because some other value (security, say) outweighs it in a given instance.

Waldron explains that essentially contested concepts can be 'solution-concept(s)' as well as 'achievement-concept(s)' [15, p. 158]. Privacy 'is the concept of a solution to a problem we're not sure how to solve; and rival conceptions are rival proposals for solving it or rival proposals for doing the best we can in this regard given that the problem is insoluble' [15, p. 158]. Like rule of law, privacy concepts are put forth to solve problems, to 'captur[e] an elusive sense, that we all share … that … there is an important ideal that social and political systems should aspire to. What that ideal is exactly none of us can say … without offering a conception of it that is bound to be controversial' [15, p. 151].

Other scholars have explained that, in addition to the normative valence associated with essentially contested concepts, they can be descriptive—describing the necessary attributes or component parts of a valued state. Privacy can function in this way too: as discussed below, its various internal attributes can be used both to describe states that satisfy the conditions for a particular conception of privacy, and to posit its normative value. The ability to traverse descriptive and normative explains part of the complexity and dynamism of contests over privacy. It allows for multiple levels of disagreement operating on the empirical and theoretical levels [29,30]. Such disagreements will often take the form of rational argumentation, but they can also be rooted in more emotional, affective and embodied differences [31].

(b) Internal complexity

Scholarship, practice and contemporary debates evince privacy's internal complexity. The contest over privacy is fuelled by complexity at multiple levels. Despite a long pedigree, there are ongoing contestations over privacy's objectives, justifications, applications and ongoing relevance for contemporary life. The harms it can be leveraged to protect against range from physical intrusions on the person, to trespasses on certain physical spaces, to meddling in relationships, to observations and informational uses.

The multiple adjectives that moderate privacy today—decisional privacy, associational privacy, informational privacy, bodily privacy—attest to a different aspect of its internal complexity [30]. Importantly, the ability to separate privacy into distinct strains does not preclude it from being an essentially contested concept. In some instances, disaggregation may solve privacy contests. But despite efforts to distinguish privacy strains that apply to different situations or objects—informational privacy protecting personal data; decisional privacy protecting the mental space necessary for individual judgement; bodily privacy protecting against physical incursions; limited access to the self-protecting against unwanted visual and auditory access; etc.—contests over privacy's core continue because often the abstract lines connecting privacy strains to contexts or conditions or objects are less neat and tidy in practice or not appreciated by those faced with the need to deploy privacy protection. Different concepts may be more or less fit for certain situations, yet they routinely compete, and agreement is only partial at both the theoretical and applied levels. Even in the face of disaggregation, all strains of privacy operate under the concept of privacy [30].

An example from a watershed US Supreme Court privacy case illustrates the complexity operating at multiple levels. *Kyllo v. US* involved an investigation of a marijuana cultivation and distribution operation in which a federal agent used a thermal imaging device to scan the outside of Kyllo's home [32]. The resulting thermal image was used to obtain a warrant to search the house. Kyllo moved to suppress the evidence recovered from the search of his home, arguing that the use of the thermal imaging device to scan it was an invasion of his reasonable expectation of privacy. In a five to four decision, the Supreme Court 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' [32, p. 28]. The *Kyllo* case was contested at every level. The parties disagreed over the object of privacy under contention. The government argued that Kyllo had no expectation of privacy in 'the heat emitted from the home' [33], while Kyllo argued that what privacy protected was the 'private activities' occurring within the home. The five justices who made up the majority determined that the case was about the 'use of technology to pry into our homes' [33], the related matter of the sanctity of 'private lives', and the need to draw a not only 'firm but also bright' [32, p. 40] line to protect the sanctity of the home and the activities occurring within it. 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' to emphasize that what was at risk was not data, but 'what's going on in the house' [33].

The dissenting justices drew a distinction between 'through-the-wall surveillance that gives the observer or listener direct access to information' [32, p. 41] and 'inferences from information in the public domain' [32, p. 49] explaining that inferences drawn from 'gathered data exposed on the outside of petitioner's home' [32, p. 41] did not intrude on privacy. Justice Stevens's writing for the dissent explained, 'it would be quite absurd to characterize [the police's] thought processes' [32, p. 44]—the inference they drew from the data that seeped through the walls—as 'searches'.

The majority 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' [32, p. 31]. The ruling was justified by the need to limit the Government's access to individuals' private lives.

(c) Diverse describability

Owing to its internal complexity, privacy can be described in multiple ways. *Kyllo v. US* just discussed offers one example. Another more recent case, *US v. Jones*, presents a whole parade of privacy formations. The three opinions—majority and two concurring opinions—offer different formulations of privacy. Each of the opinions find the Government actions to violate the Fourth Amendment, but each emphasizes different aspects of the Governments' actions as problematic—one focusing on the intrusion on private effects and one on the risk posed by warrantless GPS surveillance to the Fourth Amendment goal of 'curb[ing] arbitrary exercises of police power' and 'preventing "a too permeating police surveillance"' [34, p. 4], and the third on 'what is really important (the use of a GPS for the purpose of long-term tracking)' [34, p. 7]. While reaching the same result, the analysis in each opinion focuses on different aspects of the Government's behaviour, different risks and different justifications. In fact, the second concurrence, written by Justice Alito, agrees with little in the majority opinion save the holding. Each of the opinions has merit, and 'there is nothing absurd or [completely] contradictory' in the distinct efforts to protect privacy [14, p. 172].

(d) Openness

Fourth, Gallie argues that an essentially contested concept is persistently vague or open, it 'admits of considerable modification in the light of changing circumstances' [14, p. 172]. It is popular to describe privacy as 'contextual' in a narrower sense, to argue that, for example, sharing of information with your doctor in your doctor's office is different from sharing that same information at a cocktail party, because of the contextual situation. But the concept of privacy (not just its application) is itself 'open'. The history of privacy exhibits this openness. And, relevant in particular to contemporary trends in data science and information technology, privacy's ongoing contestability can be closely tied to the creation of particular technologies and the business models or use cases to which they were applied.

To illustrate, consider two small slices of privacy's history:

1. *The late-nineteenth century*. In response to the invention of 'instantaneous photographs' and the business model of 'newspaper enterprise', Warren and Brandeis's 'The right to privacy' in the *Harvard Law Review* began a trend of privacy as 'being let alone' [35, p. 193]. Codified into torts (in particular, by Prosser [36]), law in the USA recognized protection from gossip about people in the newspaper or use of one's image in advertising.
2. *The mid-twentieth century*. As computer technology developed across the twentieth century, it became increasingly possible to collect and analyse relatively large numbers of records related to a single person. 'Privacy' was applied in a new way, to describe protection not from gossip, but from decisions made in impersonal government databases or actuarial tables. The now ubiquitous fair information practice principles, enumerated in a 1973 report on *Records, computers and the rights of citizens* [1], described limiting

disclosure, as well as rights to access and correct data that might be used to make Government determinations. These principles were reflected in the US Privacy Act of 1974, in the OECD guidelines in 1980 [2] and are still apparent in FTC reports and EU data protection regulation.

The distance between privacy as it figured in public and legal discussions from the 1890s to the 1960s and privacy as it was later refigured in the 1970s is an exhibit of privacy's openness. The technological and social contexts in which privacy was invoked in each moment were radically different. And yet privacy was leveraged in both contexts, and across both contexts, in such a way as to protect that which people valued. Importantly, despite its differences, appeals in both contexts were made to privacy. Practitioners in the later context could have jettisoned the concept. Rather than discard it, they sought to transform it, and to do so by arguing over its meaning. That privacy was transformable in this way indicates its conceptual openness.

Today, we again face the prospect of an open and transformable concept of privacy. As we described in the Introduction, the 1970s-era guidelines that continue to structure our thinking about privacy are bumping up against powerful new technologies that expose their limits.

(e) Reciprocal recognition

Subsequent scholars have questioned whether recognition by other disputants is a requirement for essentially contested concepts. Regardless of whether it is a formal requirement or a looser test for evaluating contestedness, disputants frequently are aware that they are supporting different conceptions of the concept of privacy and are also aware of specific points of deviation. The *Jones* and *Kyllo* decisions present examples of the knowing competition over privacy contests. Such contests occur at the 'street level' too, where competing privacy concepts are aggressively and defensively advanced.

(f) Exemplars

After describing the preceding five definitional characteristics of essentially contested concepts, Gallie introduces two more characteristics that attempt to distinguish essentially contested concepts from radically confused ones. How can we be sure that disagreements over privacy are genuine disagreements over the concept itself and not just examples of talking past one another, where one group simply uses the word 'privacy' to refer to something different from the other?

In part to resolve this difficulty, Gallie introduces the idea of an 'exemplar', where those who disagree on the definition of a concept can agree that a particular instance embodies the concept in question. Part of the point is that 'exemplars', rather than a single 'exemplar', are most appropriate, given the openness described above. A compelling vindication of the place of exemplars comes from Justice Potter Stewart'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' [37, p. 197].

In the case of privacy, there are numerous exemplars that motivate standard expectations. A peeping tom peering through a window to watch someone's morning routine is an invasion of privacy. So too is a wiretap on a landline telephone transmitting all conversations to a Government agent in the attic of the next building over. So too is a scenario in which a stranger on the street takes a photograph of me in a slightly compromising light, perhaps just as the contents of my taco have fallen all over my shirt, and then later distributes the photograph online where my co-workers or distant friends see it. Taken as a group, these familiar exemplars do not all point to the same underlying conditions of privacy, nor to a singular essence of privacy. Yet they all do point to the concept of privacy.

(g) Progressive competition

Gallie's final criterion helps further distinguish contested from confused concepts. This criterion is of particular interest for our approach to privacy, in that Gallie suggests that contestability, unlike confusion, can be a generative or progressive feature of conceptual disagreement. Gallie's seventh criterion is that ongoing uses of, and disputes over, contested concepts help to preserve and develop the functionality of such concepts.

Importantly, the seventh criterion must always be evaluated prospectively, because it concerns downstream consequences of the ongoing contestedness of a concept. Thus, Gallie notes that the final criterion is 'conditional in the extreme' [14, p. 179]. It is conditional, at least in part, upon the future. It often cannot be easily settled in advance as an extant feature of a concept. For it is a criterion whose applicability is better assessed in terms of the consequences of taking a concept as contestable and continuing the contest over its function and meaning. For these reasons, we believe that Gallie's seventh criterion motivates a turn to the implications that would follow from a reorientation of our understanding of privacy towards seeing it as an essentially contested concept. To such implications, we now turn.

4. Implications for design

What could we conclude from an argument that privacy is an essentially contested concept? For us, the importance of the conclusion is inherently practical with respect to scholars in the area of privacy, technologists in the practice of data science and ethicists of technology in general. Drawing on a (much-debated) convention within the field of human–computer interaction [38], we present the following implications for design.

1. *Debate over the definition of privacy is productive, even though* (*indeed because*) *it is unlikely to be definitively decided.* To avoid unproductive conversation or the threat of relativism, scholars should use specific qualifiers and justifications when discussing the definition or definitions of privacy. We believe that the analytic, as described below, will be a useful map for such conversations.
2. *No single checklist will ensure that the designer or data scientist does not encounter an unexpected privacy concern. However, considering different assemblages of privacy—actors, harms, justifications, etc.—throughout the design of a system can improve support for privacy.* That privacy is an essentially contested concept confirms some best practices and common design advice, but might also suggest others. A user-centred design process that works closely with different stakeholders to understand their concerns is likely, by virtue of being more grounded, to anticipate user values. However, contestation should also encourage designers to consider concepts at a high level. If the designer understands the object or justification of privacy in play behind a particular privacy concern, she might more readily discover a way to support that value directly. The *values-in-design* literature provides examples of both the challenges in and potential techniques for identifying and implementing values in technical designs [39].

   It is important to bear in mind that the internal complexity of privacy means that privacy can be contested even within a particular context. Thus, designers must consider the possibility that privacy may be conceived of by different parties—users and subjects of a technology, for example—towards different ends. The variation between parties within a single context may generate equally varied requirements for design.
3. *When values are affected by changes in technology, concepts for those values are likely to remain open and contested, or be re-contested. We should anticipate and accept this openness.* Many of the seven characteristics discussed above might apply to other values, not just privacy. But in areas most affected by increases in collection and analysis of data (which might include privacy, security, fairness, freedom from discrimination, accessibility), we should

expect that changes in technological capability might re-open values that had seemed settled or 'decontested' [30, p. 218].

4. *To improve implementation of values in design, we must document high-level principles, low-level properties and mappings between them.* We suggest that it would be useful for privacy research to develop tools that will help those in need of privacy (practitioners, users, legislators and regulators, compliance officers) map the variety of ways in which privacy is being contested within different contexts. Recent workshops have discussed the utility of enumerating detailed privacy properties for which specific technical measures can be developed [40]. As one tool for this mapping, we propose the following provisional analytic as an example of what such a shift in research focus might yield.

   The purpose of such an analytic would be to assist in the better mapping of privacy. But this should not be taken to be designed with the express goal of mapping the one true, or the one best, definition of privacy. The purpose of such mapping tools should not be to eliminate privacy's contestability. Rather, it should be to work with it.

   The multi-dimensional analytic we propose is offered as an example of how to press the conversation around privacy towards more rigorous modes of analysis in the face of privacy's essential contestability. Recognizing the generative contestability of privacy, our multi-variable analytic is meant to provide not an exhaustive specification of all the possible dimensions, conceptions and uses of privacy, but rather a specific starting point for expanding the range of our enquiries into the plurality of privacy. In enquiring into privacy, we should aim not to pin down privacy, but instead to clarify its many different contexts of usage, so that different usages can lead to meaningful contestation rather than a breakdown of discussion.

5. An analytic for mapping the multiple dimensions of contests over privacy

We propose an analytical tool for mapping claims for, criticisms of, and contests over privacy along the following 14 dimensions (all of which are described in the following subsections): object, justification, contrast concept, exemplar, target, subject, action, offender, from-whom, mechanism, provider, social boundaries, temporal scale and quantitative scope (see table 1 for a summary presentation). We cluster these 14 dimensions around a set of five meta-dimensions of *theory*, *protection*, *harm*, *provision* and *scope*.[1] Our claim is that analytically separating these threads helps clarify privacy's function and value in practice. What would otherwise remain a knot is thereby opened up to analytical discrimination so that we can recognize how different privacy conceptions are operating differently in different practical contexts.[2]

(a) Dimensions of theory

(i) Objects of privacy

By *object of privacy*, we mean that which a conception of privacy seeks to provide, protect, secure, establish or create. 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?

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

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

[2]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 a *generally sufficient* range of material that one may need to assess a privacy violation. Second, it is not our view that any of the dimensions here specified pertain *only* to an analytical enquiry into concepts of privacy and their many functions. Clearly, they pertain to *much else* besides. Our claim is that some subset of these dimensions is sufficient to elucidate privacy, not that privacy is of necessity the only field of analysis in which these dimensions might come into play.

Table 1. Dimensions of contests over privacy.

privacy dimension	description	interrogation	examples
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 information
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	the archetypal threat to this concept of privacy, i.e. *privacy is violated by X*	'What's an example?'	identity theft; intrusive surveillance; gossiping neighbours
dimensions of protection			
target	that which privacy protects, i.e. *privacy protects things of type X*	'What's privacy about? Privacy of what?'	personal information; 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 behaviour 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 four meta-harms (collection, processing, dissemination and 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
dimensions of scope			
social boundaries	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
temporal scale	the time span at which privacy applies, *i.e. privacy applies for a span of X time*	'How long is privacy required?'	permanent; fixed expiration; variable expiration
quantitative scope	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

can procure this end state. The object of privacy can remain agnostic with respect to the means employed to procure it.

(ii) Justifications of privacy

Discriminating among *justifications* draws attention to the analytically distinct reasons put forward in defence of a given object of privacy. The dimension of justification refers to the underlying beliefs or assumptions that ground and support a conception of privacy. If the *object* is that which privacy aims to secure or defend, then the *justification* furnishes the moral basis for securing and providing it.

Different theories of privacy offer distinct justifications for the very same privacy object. 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. One proponent might argue that privacy as a zone of freedom is justified because it is intrinsic to human dignity, while another might justify it as instrumental for realizing self-development. A wide range of justifications are consistent with any given object of privacy, and a given justification may support different objects. Distinguishing privacy's justificatory dimension thus helps us understand how privacy gets conceptualized from a normative point of view. Crisply delineating justifications helps us understand how to argue about, that is, how to keep contesting, privacy.

(iii) Contrast concept to privacy

Contrast concept refers to that which properly contrasts to an effective conception of privacy. Contrast concepts negatively define the contours of the concept in question. This is useful when grappling with abstract concepts that appear to sensibly contrast with a range of different contrast concepts. In the case of privacy, its different conceptualizations yield differing contrast concepts. That which is private may be properly contrasted to that which is public, as is typical of liberal political theories of governance and regulation, thus yielding a non-interference or non-intrusion image of privacy. Or, privacy may be properly contrasted to transparency or exposure, thus yielding an image of privacy in terms of secrecy or intimacy.

(iv) Exemplary privacy problems

Another 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. As Gallie notes, every viable conception of a contested concept 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. As such, we understand exemplars as central parts of the conceptions of which they are exemplary, not as mere afterthoughts to those conceptions once they are already established.

(b) Dimensions of protection

(i) 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. Although 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 of personal information (as target) could afford a broader protection of personal freedom (as object). In many instances, the target and object of privacy can 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 there are plenty of instances where targets and objects of privacy are distinct. Some of the most familiar targets of privacy include personal information, bodily integrity, intimacy in relationships, and personal effects such as diaries or calendars.

(ii) Subject of privacy

By *subject of privacy*, we refer to the agent or agents whom privacy protects. The *subjects* are those on whose behalf privacy is provided. This is worth specifying insofar as privacy often does not apply universally to all in identical fashion, but often applies to persons with respect to some particular feature of those persons or the situations in which they find themselves. The subject of privacy might be a single individual (e.g. 'myself' or 'my teenage daughter'), might be a distinctive social class (e.g. 'teenagers' or 'citizens of California') or might be a distinctive social role (e.g. 'students' or 'teachers').

(c) Dimensions of harm

(i) Action against privacy

By *action against privacy*, we refer to the actions that constitute or initiate privacy harms. This is based on the recognition that privacy-related actions can vary in context, and independently of the other dimensions brought into focus by our analysis. Daniel Solove's taxonomical specification of 16 different violations of privacy grouped across the four categories of collection (surveillance and interrogation), processing (aggregation, identification, insecurity, secondary use and exclusion), dissemination (breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion) and invasion (intrusion and decisional interference) provide a useful list of actions for consideration [21]. We endorse Solove's list as illustrative but neither exhaustive nor exclusive.

(ii) 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 privacy invasion in question. Privacy offenders sometimes work in their own interest (as in the case of the anxious ex-boyfriend who self-interestedly snoops around a diary or a cell phone dialled-calls list) but very often the offender against privacy creates the offence 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.

(iii) Privacy from-whom

Privacy from-whom refers to those against whom privacy protections work on behalf of a given subject. 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.

(d) Dimensions of provision

(i) 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 the strengths and limitations of various mechanisms.

(ii) Provider of privacy

The *provider of privacy* refers to those agents who ought to provide privacy protections. On whom does the burden fall in cases where privacy is needed but not provided? In some cases, indeed perhaps the most canonical ones, it will be apparent that privacy is taken to 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 towards 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.

(e) Dimensions of scope

(i) Social boundaries

The idea of *social boundaries for privacy* captures the inherent social contextuality of privacy. 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. Yet another crucial aspect of context concerns the way in which privacy is differently shaped by power in different contexts.[3]

(ii) Temporal scale

The idea of the *temporal scale of privacy* provides a way of picking out the temporal expectations that attach to any attempt at privacy protection or any actual privacy harm. With respect to a given piece of personal information, it may be that privacy requires functionally unending protection. Other bits of personal information, however, may require protection for only a specified amount

[3]An enriched account of the dimension of social boundaries would refer to these multiple micro-dimensions of context. We do not here undertake these more fine-grained analyses, but we do register that we have constructed the analytic so that it would be fully consistent with such an enriched account of social context. These are developments we hope to undertake in future work, especially with respect to mapping the role of power in contests over privacy.

of time. While I may want to keep my social security number protected from the general public for the full extent of my lifetime, I may not require the same extent of protection for my bank account number (if I switch banks), my salary (if decades later I have a higher salary in a different field) or the address of the surprise party (after the party has begun). In short, different kinds of information require different temporal lengths of protection.

(iii) Quantitative scope

The idea of *quantitative scope* refers to the extent of application of privacy functions in question. This extent can be expressed as a function of traditional logical quantities such as universality, generality and particularity. It may be that a given privacy norm should apply universally in every possible instance, or it may be 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 manner, especially in contexts where case-by-case determinations need to be made. Quantitative scope thus specifies the boundedness of the application of privacy in a social context where those bounds do not exactly match the bounds of the social context itself.

6. Conclusion

Contestability in its many forms poses problems insofar as it can easily be used as cover for equivocation, sloppy inference and invalid argumentation. Privacy disputes often facilitate political posturing rather than deliberative dialogue. Privacy disputes are often wielded not to engage, but to silence. Privacy disputes often encourage us to avoid the nuanced conversations that are required to maintain privacy.

Coupling an embrace of contestability with analytical frameworks can facilitate more productive and reflective debates over privacy. It combines the generativity of contestability with rigorous close analysis that helps elucidate privacy contests and pinpoint key areas of disagreement. Analytic tools for dissecting privacy such as the one just presented can help us to retain the heat and fervour in privacy debates while also increasing the capacity to illuminate the sites of struggle. Such tools, therefore, facilitate more productive engagement, more agile innovation, and can even lead to more satisfying resolutions. This is a much-needed alternative to the doomsday-ing and nay-saying too often kindled in today's fiery debates over privacy. Recognizing privacy as an essentially contested concept may embolden those who benefit from keeping the privacy debates muddled. But, coupled with analytic tools such as ours, this recognition could also increase the ways in which enquiry and deliberation help tease out and advance privacy and reduce the role that power inherently plays in defining privacy in contemporary contests. Privacy is not disappearing, but it will—and more importantly must—undergo radical transformations. In the face of these transformations, privacy's contestability can be one of its strengths, at least in theory, and armed with tools such as our analytic, it can be so in practice too.

The question we face today is not simply: 'Privacy, yes or no?' While dilemmas between privacy and publicity, or privacy and surveillance, or privacy and security persist, the question we more often face today concerns the plurality available to us amidst contests over privacy: 'Which privacy? For what purpose? With what reason? As exemplified by what?' A multi-dimensional analytic is just one useful tool in our ongoing attempts to answer these questions. Such attempts are needful insofar as these questions are critical for understanding, valuing and implementing privacy. These questions 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.

Authors' contributions. All authors contributed to the research and drafting of all sections of the manuscript. D.K.M. and C.K. especially developed the analytic described in §5. All authors read and approved the manuscript.

Competing interests. The authors declare that they have no competing interests.

Funding. This project has been supported by the TRUST (Team for Research in Ubiquitous Secure Technology) Center, which receives support from the National Science Foundation (NSF award no. CCF-0424422); the US Department of Homeland Security under Grant Award no. 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research programme managed by Dartmouth College; the Berkeley Center for Law & Technology through a grant from the Nokia Corporation; and by a University of Oregon Incubating Interdisciplinary Initiatives (I3) grant on privacy and security.

Acknowledgements. We are grateful to Maydha Basho for research and analysis that supported this project, and the following for their reviews and feedback on drafts: Anita Allen, danah boyd, Paul Duguid, Chris Hoofnagle, Jennifer King, Rachel Rudolph, Daniel Solove, Luke Stark, Harry Surden and Peter Swire; anonymous referees of this journal; participants at the Third Annual Privacy Law Scholars Conference June 2010; participants at the REWIRED: How Law and Technology Shape Social Progress symposium at the Wayne Morse Center for Law and Politics, January 2014, Eugene, Oregon; the participants at the Computing Community Consortium's Visioning Workshops on Privacy by Design: State of Research and Practice, February 2015, UC, Berkeley; Privacy Enabling Design, May 2015, Georgia Tech; Engineering Privacy, August 2015, Carnegie Mellon University; Regulation as Catalyst, January 2016, Georgetown University; the NCO/NITRD National Privacy Research Strategy Workshop, February 2015, Arlington; the National Security Agency's Principles and Practice of Privacy Science (3PS) Workshop, December 2015, College Park, Maryland; and attendees at talks at Microsoft, Facebook and IDEO.

Disclaimer. The views and conclusion contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the US Department of Homeland Security, the I3P, Dartmouth College or the authors' affiliated institutions.

References

1. Department of Health, Education and Welfare. 1973 *Records, computers and the rights of citizens*. Washington, DC: Department of Health, Education and Welfare.
2. Organisation for Economic Co-operation and Development. 1980 *Guidelines governing the protection of privacy and transborder flows of personal data*. Paris, France: OECD.
3. Floridi L. 2014 Open data, data protection, and group privacy. *Philos. Technol.* **27**, 1–3. (doi:10.1007/s13347-014-0157-8)
4. Crawford K, Schultz J. 2014 Big data and due process: toward a framework to redress predictive privacy harms. *Boston College Law Rev.* **55**, 93. See http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4/.
5. Horvitz E, Mulligan D. 2015 Data, privacy, and the greater good. *Science* **349**, 253–255. (doi:10.1126/science.aac4520)
6. Jernigan C, Mistree BF. 2009 Gaydar: Facebook friendships expose sexual orientation. *First Monday* **14**, 10. (doi:10.5210/fm.v14i10.2611)
7. De Choudhury M, Counts S, Horvitz EJ, Hoff A. 2014 *Characterizing and predicting postpartum depression from shared Facebook data*, pp. 626–638. New York, NY: ACM.
8. Narayanan A, Shmatikov V. 2008 Robust de-anonymization of large sparse datasets. In *Proc. 2008 IEEE Symp. on Security and Privacy* (*SP 2008*), *Oakland, CA, 18–22 May*, pp. 111–125. Washington, DC: IEEE Computer Society. (doi:10.1109/SP.2008.33)
9. Nissenbaum H. 2009 *Privacy in context: technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.
10. Barocas S, Nissenbaum H. 2014 Big data's end run around anonymity and consent. In *Privacy, big data, and the public good: frameworks for engagement* (eds J Lane, V Stodden, S Bender, H Nissenbaum), pp. 44–75. Cambridge, UK: Cambridge University Press.
11. Dwork C. 2006 Differential privacy. In *Proc. 33rd Int. Colloq. on Automata, Languages and Programming, part II* (*ICALP 2006*), *1 July* (eds M Bugliesi, B Preneel, V Sassone, I Wegener), pp. 1–12. Berlin, Germany: Springer.
12. Bamberger KA, Mulligan DK. 2015 *Privacy on the ground: driving corporate behavior in the United States and Europe*. Cambridge, MA: MIT Press.
13. European Data Protection Supervisor. 2015 *Establishing an external advisory group on the ethical dimensions of data protection*. Decision. See https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/AdvisoryGroup/15-12-03_EthicsGroup_Decision_EN.pdf.
14. Gallie WB. 1956 Essentially contested concepts. *Proc. Aristotelian Soc.* **56**, 167–198. (doi:10.1093/aristotelian/56.1.167)

15. Waldron J. 2002 Is the rule of law an essentially contested concept (in Florida)? *Law Philos.* **21**, 137–164. See http://www.jstor.org/stable/3505128.
16. Garver N. 1998 Violence and social order. In *Philosophy of law, politics, and society, Proc. 12th Int. Wittgenstein Symp., Kirchberg, Austria, 8–13 August 1987* (eds O Weinberger et al.), pp. 218–233. Berlin, Germany: Springer.
17. Garver E. 1990 Essentially contested concepts: the ethics and tactics of argument. *Philos. Rhetoric* **23**, 251–270. See http://www.jstor.org/stable/40237644.
18. Westin A. 1967 *Privacy and freedom*. New York, NY: Atheneum.
19. Thomson JJ. 1975 The right to privacy. *Philos. Public Affairs* **4**, 295–314. See http://www.jstor.org/stable/2265075.
20. Post RC. 2000 Three concepts of privacy. *Georgetown Law J.* **89**, 2087. See http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1184&context=fss_papers.
21. Solove DJ. 2008 *Understanding privacy*. Cambridge, MA: Harvard University Press.
22. Nissenbaum H. 2004 Privacy as contextual integrity. *Washington Law Rev.* **79**(1), 119–158. See https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/61/volume79.pdf.
23. Wittgenstein L, Anscombe GEM. 2008 *Philosophical investigations.* (German text, with a revised English translation). Malden, MA: Blackwell.
24. Allen A. 2003 Privacy. In *The Oxford handbook of practical ethics* (ed. H LaFollette), pp. 485–513. Oxford, UK: Oxford University Press.
25. Lipton JD. 2010 Mapping online privacy. *Northwestern University Law Rev.* **104**, 477. See https://ssrn.com/abstract=1443918.
26. Vasalou A, Gill AJ, Mazanderani F, Papoutsi C, Joinson A. 2011 Privacy dictionary: a new resource for the automated content analysis of privacy. *J. Am. Soc. Inf. Sci. Technol.* **62**(11), 2095–2105. (doi:10.1002/asi.21610)
27. Finn RL, Wright D, Friedewald M. 2013 Seven types of privacy. In *European data protection: coming of age* (eds S Gutwirth, R Leenes, P de Hert, Y. Poullet), pp. 3–32. Dordrecht, The Netherlands: Springer.
28. Koops B-J, Newell BC, Timan T, Chokrevski T, Galič M. 2016 A typology of privacy. *Univ. Pennsylvania J. Int. Law* **38**(2) (in press).
29. Connolly WE. 1993 *The terms of political discourse*. Princeton, NJ: Princeton University Press.
30. Collier D, Daniel Hidalgo F, Olivia Maciuceanu A. 2006 Essentially contested concepts: debates and applications. *J. Polit. Ideol.* **11**, 211–246. (doi:10.1080/13569310600923782)
31. Stark L. 2016 The emotional context of information privacy. *Inform. Soc.* **32**, 14–27. (doi:10.1080/01972243.2015.1107167)
32. US Supreme Court. 2001 *Kyllo v. United States*, 533 U.S. 27, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001). See https://supreme.justia.com/cases/federal/us/533/27/.
33. US Supreme Court. 2001 *Kyllo v. United States*, US TRANS LEXIS 11 (February 20, 2001). Oral argument. See https://www.supremecourt.gov/oral_arguments/argument_transcripts/99-8508.pdf.
34. US Supreme Court. 2012 *United States v. Jones*, 565 U.S. 945, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012). See https://supreme.justia.com/cases/federal/us/565/10-1259/.
35. Warren SD, Brandeis LD. 1890 The right to privacy. *Harvard Law Rev.* **4**, 193–220. See http://www.jstor.org/stable/1321160.
36. Prosser W. 1960 Privacy. *California Law Rev.* **48**, 383. See http://www.jstor.org/stable/3478805.
37. US Supreme Court. 1964 *Jacobellis v. Ohio*, 378 U.S. 184, 84 S. Ct. 1676, 12 L. Ed. 2d 793 (1964). See https://supreme.justia.com/cases/federal/us/378/184/.
38. Dourish P. 2006 Implications for design. In *Proc. of the Sigchi Conf. on Human Factors in Computing Systems*, pp. 541–550. New York, NY: ACM.
39. Flanagan M, Howe DC, Nissenbaum H. 2008 Embodying values in technology: theory and practice. In *Information technology and moral philosophy* (eds J van den Hoven, J Weckert), ch. 16, pp. 322–353. Cambridge, UK: Cambridge University Press. (doi:10.1017/CBO9780511498725.017)
40. Doty N, Drobnis A, Mulligan DK, Wong R. 2015 Privacy by design—state of research and practice. Workshop 1 report. *Computing Community Consortium Workshop 1, Berkeley, CA, 5–6 February*. See http://cra.org/ccc/wp-content/uploads/sites/2/2015/02/PbD-Workshop-1-Report-.pdf.