LOSSES VERSUS VIOLATIONS: 
THE UNITY AND LIMITS OF PRIVACY

(manuscript under review)

Jeffrey M. Skopek

TABLE OF CONTENTS

INTRODUCTION ..................................................................................1

I. DIFFERENTIATING PRIVACY ............................................................5
   A. Normative Theories .................................................................5
   B. Descriptive Theories .............................................................9

II. CONFLATION ERRORS .................................................................11
   A. Mistargeted Critique .............................................................11
   B. Misguided Skepticism ............................................................14

III. PRIVACY LOSSES .......................................................................18
   A. Access ....................................................................................19
   B. Epistemic Merit .....................................................................27
   C. Truth .....................................................................................33

IV. PRIVACY VIOLATIONS .................................................................36
   A. The Path-Based Element .......................................................37
   B. Rethinking Aggregation and Use ..........................................40
   C. The Status of Inferences .......................................................49

CONCLUSION ..................................................................................56
INTRODUCTION

It is widely thought that the core problems posed by new technologies of personal data mining and analysis, as well as their solutions, can be explained in terms of privacy. Take, for example, the uses of personal data in these cases:

- an employer rejects a job applicant on the basis of a health trait inferred from non-health data in his application;
- a landlord screens out applicants on the basis of a proxy for religion;
- the police aggregate data about a person’s public movements, thereby discovering the person’s sexual and political orientations;
- an internet platform infers private facts about a person from his browsing history and uses this to tailor content;
- a government agency makes a decision about an individual entitlement on the basis of an algorithmic assessment that it cannot explain.

These and other related uses of personal data are widely seen as violating privacy rights. But this is a mistaken diagnosis, arising from the failure to differentiate between privacy losses and privacy violations. In these cases, there may be losses, but not violations. To understand and address the actual threats posed by new ways of accessing and using personal data, it is necessary to step back and clarify what privacy is and what it is not.

For as long as privacy has been the subject of academic study, privacy scholars have highlighted that it is an ill-defined concept, and for as long as they have tried to clarify it, their definitions have been rejected by others as being too broad, too narrow, or both. In light of this history, Dan Solove has championed the growing view that we should abandon our attempt “to locate the ‘essential’ or ‘core’ characteristics of privacy,” which he identifies as the cause of the deep disagreements in the literature. The way forward, he

3 In 1978, David O’Brien concluded that the unitary definitions of privacy that had been developed by others were either “imprecise, or too broad, or too narrow,” David M. O’Brien, Privacy and the Right of Access: Purposes and Paradoxes of Information Control, 30 ADMIN. L. REV. 45, 62 (1978). Nearly 25 years later, Dan Solove reached the same conclusion: “The most prevalent problem with the conceptions is that they are either too narrow or too broad…. Often, the same conceptions can suffer from being both too narrow and too broad.” Daniel J. Solove, Conceptualizing Privacy, 90 CAL. L. REV. 1087, 1092 (2002).
argues, is to understand privacy as a Wittgensteinian “family resemblance” concept that is not unified by any essential features, but rather held together by a common pool of similar features. While Solove’s analysis is illuminating, it has hidden costs, which are avoided by an alternative diagnosis of the current state of affairs.

This will article will demonstrate that the two trends in the privacy literature identified thus far—the reliance on privacy to articulate an ever-growing list of concerns about data-driven technologies, and the growing skepticism about whether privacy has a unifying core—are both misguided for the same reason. They both arise from the failure to differentiate between descriptive and normative theories of privacy and the different questions that they seek to answer (explored in Part I). As used in ordinary language, the term privacy may refer either to a right or to a value-neutral state of affairs. In having these two dimensions, privacy is similar to many other important moral and legal concepts, such as liberty and discrimination, where the two dimensions are generally recognized. With privacy, however, the distinction, which was once widely recognized as significant, is now generally overlooked. As a result, two different questions have become conflated: the first is the descriptive question of whether a person has suffered a privacy loss, and the second is the value-laden question of whether a person has suffered a privacy violation.

The conflation of these questions is problematic for several reasons, including that it has generated significant misconceptions in the privacy literature (demonstrated in Part II). First, it has generated mistargeted
critiques in which descriptive theories are rejected for failing to answer normative questions. This type of analytical error, known as a “category error,” has led many to believe that there is greater disagreement in the literature than is actually the case. Second, the conflation of privacy losses and privacy violations has generated misguided skepticism about the possibility of developing a unified theory of privacy. This skepticism assumes that a unified theory of privacy must be grounded in normative coherence (i.e., in an agreement about what constitutes a privacy violation). An alternative approach, which has been overlooked, is to ground it in descriptive coherence (i.e., in an agreement about what constitutes a privacy loss).

On the question of what constitutes a privacy loss, there is also disagreement in the literature, but common ground is easier to find. Critical reflection on how the concept is used in ordinary language reveals three criteria that together define it (developed in Part III). First, a person or information about a person must have been accessed by someone else. Mere accessibility, lack of control over access, and access by non-persons might seem to constitute privacy losses—as others have argued—but closer analysis reveals that these criteria track related but distinct matters. Second, the means of access must have some epistemic merit. While knowledge is not required to cause a privacy loss, a lucky guess is insufficient. Third, the object of the access must be a person or fact about a person. Access to false information alone cannot cause a privacy loss.

Building on this understanding of the nature of privacy losses, it is possible to identify the common core of privacy rights: they restrict the means by which privacy losses can permissibly occur. On this account (developed in Part IV), a person suffers a privacy violation when a restriction on the permissible means of generating such access is breached. Thus, a key difference between privacy losses and violations is that losses are outcome-based, whereas violations are path-based. Privacy rights do not protect a reasonable expectation that privacy will be maintained, but rather a reasonable expectation that privacy will not be lost in certain ways.

For the avoidance of confusion, it is worth highlighting that although this theory defines privacy violations in terms of privacy losses (which provides for the coherence of privacy), it does not suggest that a privacy loss is a necessary element of a privacy violation. On the contrary, in line with common intuitions, it explains how a privacy violation can occur without the occurrence of a privacy loss.\footnote{For example, it suggests that the police could violate your privacy rights by installing an unauthorized wiretap your phone (breaching a restriction on means of access), even if you do not end up speaking on the phone (so access is not obtained). Cf. Schoeman, supra note 6, at 4 (“We can also envision situations in which we would want to say that a person has not in fact suffered a loss of privacy but has suffered a violation of his right to privacy.”).}
Note also that this theory does not take a position on the question of which means of access are impermissible, but rather provides a foundation for a wide range of positions on this and other related questions (such as why privacy is valuable and what types of facts should be protected). Because it unifies privacy along its descriptive rather than its normative dimension, it is compatible with disagreement on these questions. For example, it is compatible with Helen Nissenbaum’s argument that privacy rights should be understood as rights to “contextual integrity,” as well as Lior Strahilevitz’s argument that privacy rights should be focused on protecting interests against intrusion and disclosure.

At the same time, the theory has a critical edge, challenging widespread claims about whether and how privacy rights are violated by data aggregation, the unconsented use of personal data, and the inference of private facts from disclosed data. Paying attention to the loss/violation distinction reveals that the scholarship on these issues has misinterpreted key Supreme Court cases, including the landmark technology cases of Carpenter v. United States and Kyllo v. United States. In addition, it helps clarify the normative reasons why privacy rights should not be expanded in the ways that have been suggested.

To be clear, in challenging widespread claims about how aggregation, unconsented use, and inferential analysis violate privacy rights, this article is not arguing that restrictions on these practices are unjustified. Rather, the argument is that the justification must often be found outside privacy rights. The mere fact that a harm arises from the mining or use of personal data does not make it a privacy harm.

It is likely that analytical precision will reveal that some complaints that have been characterized as privacy violations should not be legally actionable at all. In other cases, it will allow us to develop causes of action that are justified by the actual interests at stake. For example, privacy is often conflated with autonomy, fairness, and due process—all of which are distinct interests that may independently deserve protection. But here too, greater precision will reveal previously unrecognized limits: when the actual interests

10 Cf. Ronald Dworkin, Taking Rights Seriously 116–18 (1978) (explaining that the theory that best fits and justifies an area of law will often not fit all of our judgements about it; rather, to achieve coherence, it will often find some judgements to be mistaken or misconceived).
13 Privacy harms are one type of information-based harm, not vice versa. For this reason, data protection law is not the EU’s version of privacy law, as is often suggested. Because data protection law is far more expansive, it remains outside the scope of this article, and it may not fit within any single unifying theory—though that is question that must be set aside.
at stake are identified, it will become clear that they do not always justify restrictions that are as expansive as those imposed by privacy rights. For all who are concerned about the ever-expanding uses of our personal data, this may appear to be a cost of my theory. But if so, it should be accepted as the cost of coherence. Recognizing the difference between losses and violations reveals the unity and limits of privacy.

To summarize and provide a roadmap of this analysis, there are four core steps: Part I provides a taxonomic analysis of the privacy literature that differentiates between normative and descriptive theories of privacy, the different questions that they address, and the answers that have been offered. Part II demonstrates that the conflation of normative and descriptive questions has generated mistargeted critique and misguided skepticism, identifying descriptive coherence as a potential foundation for a unifying theory of privacy. Part III develops and defends the claim that privacy losses are defined by three core criteria: access, epistemic merit, and truth. Part IV argues that a privacy violation occurs when a restriction on the permissible means of access is breached, challenging widespread claims about how privacy rights are violated by the aggregation, unconsented use, and inferential analysis of personal data.

I. DIFFERENTIATING PRIVACY

A review of the vast body of privacy scholarship might lead one to conclude that it contains intractable conflict about the nature of privacy, but there is actually less disagreement than it seems. Much of the apparent conflict arises from a failure to differentiate between normative and descriptive theories of privacy, the variations within them, and the different questions to which they provide answers. A taxonomic analysis of these differences (in this Part) helps reveal the errors caused by their conflation (in the next Part). While some of the individual themes identified in this survey of the literature have been noted by others, many of the most important distinctions have not.

A. Normative Theories

Most of the privacy literature is devoted to the development of normative theories of privacy (as a matter of law or morality) that provide an account of one or more of the following: the nature of privacy interests, the rights that arise from these interests, and the scope of these rights.

---

14 See supra notes 2-3 and infra Part II.A.
15 Cf. Solove, Conceptualizing Privacy, supra note 3, at 1099–1124 (identifying some of the themes, but without the same analytical framework).
1. Interests in privacy

A significant body of privacy scholarship has defined privacy in terms of the interests that it protects. Three sets of interconnected interests—individual, relational, and societal—have received significant attention.16

The interests of the individual in being an autonomous person are at the core of many definitions of privacy. For example, privacy has been defined as protecting “inviolate personality” (Samuel Warren and Louis Brandeis),17 “the individual’s interest in becoming, being, and remaining a person” (Jeffrey Reiman),18 “the individual’s independence, dignity and integrity” (Edward Bloustein),19 and other similar values.20

It is widely agreed, however, that privacy does not just protect the individual in isolation, but also the personal relationships that are essential to human flourishing. Often, these interests are identified in terms of intimacy.21 For example, Tom Gerety defines privacy as “control over the intimacies of personal identity”22 and Julie Inness identifies intimacy as the defining feature unifying the set of intrusions that are properly called privacy invasions.23 But others characterize the relational interests more broadly. For example, Charles Fried defines privacy as protecting relationships of “respect, love, friendship and trust.”24

Finally, extending beyond personal relational interests, there are the interests of the individual in participating in social and political life. For example, Julie Cohen suggests that privacy fosters a capacity for autonomy that “is an indispensable condition for reasoned participation in the

---

16 See generally NISSENBAUM, supra note 8, at 67–89 (identifying these three categories).
21 See Solove, Conceptualizing Privacy, supra note 3, at 1121 (providing an overview).
22 Gerety, supra note 2, at 236.
23 JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992). See also JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2011); Robert S. Gerstein, Intimacy and Privacy, 89 ETHICS 76, 81 (1978) (stating that “intimacy simply could not exist unless people had the opportunity for privacy”).
24 Charles Fried, Privacy, 77 YALE L.J. 475, 482 (1968). See also James Rachels, Why Privacy Is Important, 4 PHIL. & PUB. AFF. 323, 323 (1975) (arguing that privacy is needed “to create and maintain different sorts of social relationships with different people”).
governance of the community and its constituent institutions.” Highlighting that freedom from surveillance is “foundational to the practice of informed and reflective citizenship,” Cohen argues that privacy “is an indispensable structural feature of liberal democratic political systems.” This general position has also been developed by others.

2. Rights of privacy

Along with providing an account of the interests that are protected by privacy, a normative theory of privacy must identify the moral or legal rights that we have by virtue of these interests. This is perhaps the most contentious issue in the privacy literature, with four broadly-different positions being advanced.

The first set of positions build on the foundational claim of Brandeis and Warren that the right of privacy is a right “to be let alone.” This conception of the right of privacy, which treats it as a negative right, is fairly abstract; but it has been developed to include concrete rights restricting privacy intrusions and the disclosure of private information. These rights have been recognized to varying degrees in common law, constitutional law, and statute. Recently, Lior Strahilevitz has proposed combining these two rights into a single right that could be used as the basis for reunifying privacy law across multiple areas.

---

27 E.g., Ruth Gavison, Privacy and the Limits of Law, 89 YALE L.J. 421, 423 (1980) (arguing that privacy is important because it promotes “liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society”); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 213 (1995) (“Privacy…has value not just to the individual as an individual or to all individuals in common but also to the democratic political system.”); SOLOVE, UNDERSTANDING PRIVACY, supra note 2, at 93.
28 Another underlying question here is whether and how privacy rights are distinct from other rights that seem to provide similar protections. Compare Judith Jarvis Thomson, The Right to Privacy, PHIL. & PUB. AFF. 295 (1975) (arguing that privacy rights are reducible to other rights) with Thomas Scanlon, Thomson on Privacy, 4 PHIL. & PUB. AFF. 315 (1975) (rejecting Thomson’s reductionism).
29 Warren & Brandeis, supra note 17, at 205.
30 These are the two core privacy rights identified by Prosser in his foundational work. William Prosser, Privacy, 48 CAL. L. REV. 383 (1960). I set aside his other two privacy torts (misappropriation of identify and false light), as Prosser admits that they do not cohere, and his suggestion that they are privacy rights is often rejected. See, e.g., Gerety, supra note 2, at 246–81 (arguing that only the intrusion and disclosure torts are truly concerned with privacy); RICHARD POSNER, THE ECONOMICS OF JUSTICE 272–73 (1981) (identifying seclusion and concealment as the core of privacy).
31 See generally Strahilevitz, supra note 9.
The second set of positions, which develop privacy into a positive rather than negative right, define it as a right to informational control. This conception of privacy became influential in the 1960s through the work of Alan Westin, who argued that privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others,” as well as Charles Fried, who defined privacy as “the control we have over information about ourselves.” In the following decades, this control-based definition was widely advanced, sometimes with further refinements.

The third set of positions characterize informational control as just one aspect of a broader privacy right—a right that encompasses various forms of decisional autonomy. For example, Julie Inness defines privacy as “the state of possessing control over a realm of intimate decisions, which include decisions about intimate access, intimate information, and intimate actions.” This conception of privacy rights was also adopted by the Supreme Court in its decisions establishing rights to contraception and abortion under the Constitution. It originally referred to these as privacy rights, but it no longer does so, in line with the widespread criticism that the interest at stake in these cases is liberty, not privacy. I will likewise exclude pure liberty rights from my analysis of privacy.

The fourth approach to privacy rights argues that they are context-dependent rights governing the transmission of personal information. For example, Helen Nissenbaum argues that “a right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information,” and that the content of this right is defined in terms of social

---

32 See generally Solove, Conceptualizing Privacy, supra note 3, at 1109–15 (discussing this approach).
33 ALAN WESTIN, PRIVACY AND FREEDOM 15 (1967).
34 Fried, supra note 24, at 482.
35 E.g., ARTHUR RAPHAEL MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971) (defining privacy as “the individual's ability to control the circulation of information relating to him”).
36 For example, Richard Parker specified the information pathways to which control might apply: “The definition of privacy defended in this article is that privacy is control over when and by whom the various parts of us can be sensed by others. By ‘sensed,’ is meant simply seen, heard, touched, smelled, or tasted.” Richard B. Parker, A Definition of Privacy, 27 RUTGERS L. REV. 275, 281 (1973).
37 INNESS, supra note 23, at 140.
40 Note that some decisional non-interference rights are not purely about autonomy, but rather have an information privacy component. Neil Richards, The Information Privacy Law Project, 94 Geo. L.J. 1087, 1106–16 (2006).
41 NISSENBAUM, supra note 8, at 127.
norms: “Inappropriate information flows are those that violate context specific informational norms … a subclass of general norms governing respective social contexts.”42 These norms differ depending on the type of information at issue, the actors involved, and the principles under which the information is transmitted.43 Highlighting the role of context in determining the content of privacy rights, Nissenbaum suggests that the right to privacy is a right to “contextual integrity.”44

3. The domain of privacy

In addition to providing an account of the content of privacy rights, a normative theory of privacy might specify and thereby limit the conduct or matters to which they apply—what might be called the domain of privacy rights. For example, it is often suggested that informational privacy rights only apply to certain types of information that can be properly classified as private.45 In specifying what information counts, many privacy scholars have identified “intimacy” as a key criterion.46 But this approach has been criticized for failing to protect other important aspects of privacy.47 There is also a growing view that the domain of privacy rights cannot be defined categorically, but rather must be responsive to context.48

B. Descriptive Theories

While recent debates about privacy have focused on the normative questions identified above, privacy is not only a normative concept of law or

42 Id. at 9.
45 See, e.g., Solove, Conceptualizing Privacy, supra note 3, at 1104. A related normative claim is that information can be private even if it is known to others. Id. at 1108–9.
46 See, e.g., INNESS, supra note 23, at 56 (stating that “privacy is the state of the agent having control over a realm of intimacy, which contains her decisions about intimate access to herself (including intimate information) and her decisions about her own intimate actions”).
47 See, e.g., Gerety, supra note 2, at 282 n.175 (arguing that it is a mistake to think that intimacy is “reducible to what may be its paradigm, sexual intimacy”).
48 See, e.g., Parker, supra note 36, at 279 (“It is tempting to try and limit the definition of privacy to control over certain items of information. But this approach is a mistake. Although there is some information which seems peculiarly related to privacy.… a loss of control over most items of information about ourselves is sometimes related to privacy and sometimes not.”); Marc J. Blitz, Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity, 82 TEX. L. REV. 1349, 1412 (2004) (providing examples).
morality, but also a descriptive one. It refers not only to rights and interests that can be violated, but also to a state of affairs that can be lost. In having two senses—one normative, one descriptive—privacy is similar to many other important moral and legal concepts, such as liberty. This distinction is now often overlooked, but it was once widely recognized as important.

Those who have identified and explored the descriptive side of privacy have generally defined it in terms of “limited access” to some dimension of one’s self. For example, Hyman Gross defined the condition of privacy as “the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited.” David O’Brien defined it as “an existential condition of limited access to an individual’s life experiences and engagements,” and William Parent defined it as “the condition of not having undocumented personal knowledge about one possessed by others.”

As I will ultimately advance a version of this approach, I will at this point merely highlight three issues along which limited access theories sometimes diverge. First, there is the question of whether access can be completely defined in informational terms, or whether non-informational access can cause privacy losses. Second, there is the question of whether a person—informational or otherwise—must be actually be accessed to cause a privacy loss, or whether mere accessibility is sufficient. Third, there is the

---

49 See supra note 5.

50 See, e.g., Schoeman, supra note 6, at 3 (highlighting the importance of differentiating “the question of whether or not one has undergone a loss of privacy from the questions of whether or not one’s right to privacy has been infringed or violated”); Parent, supra note 6, at 309 (“The concept of a right to privacy is quite different from and should not be confused with the concept of privacy simpliciter”); Gross, supra note 6, at 35–36 (“Privacy is a state of affairs, and before we speak of ‘rights of’ or ‘interests in’ or ‘invasions of’ it, we ought to be acquainted with its distinguishing features.”); O’Brien, supra note 3, at 75 (criticizing the privacy literature’s “failure to adequately distinguish between the concept of privacy and a right to privacy”). The distinction is now often overlooked, or if acknowledged, dismissed as unimportant. See, e.g., Moore, supra note 6, at 421 (concluding that “we should not be overly worried about defining a state or condition precisely”). But there are exceptions, such as Powers, supra note 6.

51 Gross, supra note 6, at 35–36.

52 O’Brien, supra note 3, at 75.

53 Parent, supra note 6, at 269.

54 For example, Ruth Gavison rejects the pure informational approach, arguing that the condition of privacy consists of limited access across three dimensions: secrecy, anonymity, and solitude. Gavison, supra note 27, at 428.

55 For example, Anita Allen tracks Gavison’s three-prong definition, except for the fact that she adopts a criterion of limited inaccessibility rather than limited access: “My own restricted-access definition of privacy is this: personal privacy is a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others.” ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 15 (1988). The difference between access and accessibility is highly significant for reasons discussed in Part III.A.
question of whether the limitation on access or accessibility must be desired by the person to count as privacy, or whether privacy can be imposed.\footnote{For example, Sissela Bok tracks Gavison’s three-prong definition, but with the additional requirement that the lack of access across the three dimensions be desired by the person at issue: “I shall define privacy as the condition of being protected from unwanted access by others — either physical access, personal information or attention.” SISSELLA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 10 (1982). But see ALLEN, supra note 55, at 27 (“Privacy aptly describes even some conditions of unwanted inaccessibility.”).}

It is also possible to depart entirely from the limited access framework in defining the condition of privacy. For example, drawing on normative theories of privacy, one could argue that “informational control” describes not only the right of privacy, but also the condition of privacy. On this account, privacy would not exist, as a descriptive matter, when an individual lacks informational control. However, this approach is uncommon—and for good reasons, which I will discuss in Part III, after first demonstrating the more basic problems of conflation.

II. CONFLATION ERRORS

Having identified the distinction between normative and descriptive theories of privacy—and the different questions that they might seek to answer—I will now demonstrate how their conflation has given rise to two related errors in a significant body of privacy literature: mistargeted critique, in which descriptive theories are rejected for failing to answer normative questions; and misguided skepticism, in which the failure to differentiate between them has resulted in the mistaken conclusion that a unified theory of privacy is unattainable.

A. Mistargeted Critique

A large body of critical scholarship suffers from a type of logical error known as a “category mistake,” in which something that belongs in one category is treated as though it belongs to a different category. Often, category errors occur when an object of critique is treated as though it has, or should have, a property that it cannot have. In the privacy literature, this is widespread: descriptive theories of privacy are often rejected for failing to provide answers to normative questions. This can be seen in three widespread critiques of limited access theories of privacy, which track the taxonomic analysis developed above.

In the first critique, limited access theories are rejected for failing to provide an account of interests protected by privacy. For example, Dan Solove argues that many limited accessed theories should be rejected on the
grounds that they fail to provide an account of the “value of privacy,” which he states is needed to answer important questions about the nature of privacy rights and private matters. 57 Others make similar claims. 58 It should now be clear, however, that these complaints are misguided. They fail to recognize the nature of a descriptive theory.

In the second critique, limited access theories are rejected for failing to provide a theory of privacy rights. For example, many scholars have rejected this approach on the grounds that it fails to provide criteria by which to differentiate between legitimate and illegitimate modes of acquiring information, 59 to identify clear cases of privacy violations, 60 and to explain what is important about privacy rights. 61 But again, these criticisms are based on a category error: they expect an account of the condition of privacy to be an account of the right of privacy.

In the third critique, limited access theories are rejected for failing to identify the domain of privacy rights. There are two general versions of this critique. The first suggest that limited access theories are under-inclusive because personal facts can be known to others, but private. 62 The second

57 Solove, Conceptualizing Privacy, supra note 3, at 1104. See also Solove, Understanding Privacy, supra note 2, at 20.
58 See, e.g., Inness, supra note 23, at 45 (arguing that limited access theories should be rejected on the grounds of they define privacy in a value-neutral way); Judith Wagner DeCew, The Scope of Privacy in Law and Ethics, 5 LAW & PHIL. 145, 152 (1986) (rejecting William Parent’s limited access definition because it provides “no way … to judge what should or should not be a part of the public record” and “leaves no room for a normative sense of privacy encompassing interests worthy of protection”).
59 E.g., DeCew, supra note 58, at 152 (rejecting Parent’s definition on these grounds); Solove, Understanding Privacy, supra note 2, at 20 (arguing that a problem with limited access theories is that they provide “no understanding as to the degree of access necessary to constitute a privacy violation”).
60 E.g., Inness, supra note 23, at 46–47 (arguing that limited access theories should be rejected because they suggest that a person’s privacy is not violated when they must hide to avoid being seen by a Peeping Tom). Likewise, when Inness rejects limited access theories on the grounds that privacy and access are not opposed if privacy’s function is “to provide the individual with control over certain aspects of her life,” she makes a claim is about privacy rights (and their function), not the condition of privacy. Id. at 6.
61 E.g., Steve Matthews, Privacy, Separation, and Control, 91 MONTIST 130, 141–42 (2008) (“When we say… it is important to respect a person’s privacy, we surely do not mean it is important to respect the mere condition someone is in of being secluded from us… What we are respecting is the person’s explicitly expressed choice, or a choice we must presume they would reasonably make.”).
62 E.g., DeCew, supra note 58, at 155 (“[P]rivate information about one’s debts or odd behavior may be publicized. Although it is no longer concealed, it is no less private.”); Solove, Conceptualizing Privacy, supra note 3, at 1109 (“The books we read, the products we buy, the people we associate with—these are often not viewed as secrets, but we nonetheless view them as private matters.”). Solove also attributes this position to Stanley Benn, though Benn in fact differentiates between the descriptive issue of whether something is done “in private” (which he defines in terms of informational access) and the normative question of whether something is a “privacy matter” (which he states is both norm-dependent and norm-invoking). Stanley
version of the critique suggests that they are over-inclusive because personal facts can be unknown to others, but not private.\textsuperscript{63} Setting aside the validity of the assumption that some \textit{types} of information can be categorically classified as private (and others as not), which there is good reason to reject,\textsuperscript{64} the problem that I want to highlight is that these critiques assume a normative conception of privacy. What constitutes a “private matter” is determined by reference to a conception of the value of privacy or an understanding of the types of information that people often want to keep private (i.e., in terms of interests in privacy). Thus, it is a category error to suggest that these critiques identify a problem with a limited access theory of privacy, which is descriptive and intentionally sets aside the question of when privacy should be protected.

In short, limited access theories are often rejected for failing to explain the nature of privacy interests, the content of privacy rights, and the domain of privacy—or in other words, for failing to address the three elements of normative theories identified above. In these ways, the common critiques all entail category errors. But this is not the only problem.

These claims are also unjustified, as they criticize limited access theorists for failing to answer normative questions that they do in fact answer. For example, DeCew suggests that Parent’s account provides no way to “judge what should or should not be a part of the public record,”\textsuperscript{65} but he does address the “criteria for wrongful invasion” in his discussion of the right to privacy.\textsuperscript{66} In addition, Parent and others such as Ruth Gavison and Hyman Gross devote large parts of their articles to the value of privacy, after they have first defined the condition of privacy in value-neutral terms.\textsuperscript{67} Furthermore, they all clearly explain this structure of their analyses. For example, Hyman Gross explains: “Privacy is a state of affairs, and before we

\textit{Benn, Privacy, Freedom, and Respect for Persons, PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY} 223, 223 (Ferdinand D. Schoeman, 1984).

\textsuperscript{63} For example, Solove writes: “Without a notion of what matters are private, limited-access conceptions do not tell us the substantive matters for which access would implicate privacy. Certainly not all access to the self infringes upon privacy.” \textit{SOLOVE, UNDERSTANDING PRIVACY, supra} note 2, at 20. \textit{See also} DeCew, \textit{supra} note 58, at 155; Solove, \textit{Conceptualizing Privacy, supra} note 3, at 1111–12.

\textsuperscript{64} The problem is that there is not any type of information that is categorically related, or unrelated, to privacy. While there are some types of personal information that most people want to keep private (for example, information about sexual habits), this speaks to the value of privacy. Further, this value is ultimately determined by the context of a factual disclosure—not the type of fact disclosed. \textit{See supra} note 48.

\textsuperscript{65} DeCew, \textit{supra} note 58, at 152.

\textsuperscript{66} Parent, \textit{supra} note 6, at 278–88. Likewise, DeCew argues that his “descriptive emphasis… leaves no room for a normative sense of privacy encompassing interests worthy of protection,” DeCew, \textit{supra} note 58, at 152. But again Parent does in fact address this issue when discussing the value of privacy and the right to privacy. Parent, \textit{supra} note 6, at 278–88.

\textsuperscript{67} Parent, \textit{supra} note 6, at 275–77; Gavison, \textit{supra} note 27, at 440–55.
speak of... ‘interests in’ or ‘invasions of’ it, we ought to be acquainted with its distinguishing features.\textsuperscript{68}

Thus far, I have argued that the dominant critiques of descriptive theories of privacy are mistargeted. In response, one might argue that the entire project of developing a descriptive theory of privacy does not make sense—and that this is what underlies the critiques that I have identified.\textsuperscript{69}

But there would be two problems with this response. First, the critiques that have been offered do not actually address the question of whether it makes sense to have a non-normative conception of privacy.\textsuperscript{70}

Second, there are good reasons to maintain the distinction, including that the term privacy is clearly used in both ways in ordinary language and academic writing; the failure to recognize this has produced significant confusion in the literature; and the distinction allows one to separate questions that should be capable of having different answers. At the very least, a definition of privacy should allow for different answers to the questions of whether privacy is protected in a given case and whether it should be protected. The definition should not entail the view that privacy should always be protected.\textsuperscript{71}

Another benefit of descriptive theories will become apparent in the next section: they provide the basis for a unifying theory of privacy.

\textbf{B. Misguided Skepticism}

\textit{1. Denying coherence}

The failure to distinguish between normative and descriptive theories of privacy has generated not only mistargeted critique, but also misguided skepticism about the possibility of developing a unified theory of privacy. This skepticism has taken two general forms. Both conclude that we should not seek a unified concept of privacy or privacy rights, but they reach this conclusion for different reasons.

The first form of skepticism rejects the coherence of privacy on the grounds that there is nothing distinctive about the concept of privacy—

\textsuperscript{68} Gross, \textit{supra} note 6, at 35.

\textsuperscript{69} Cf. \textit{INNESS}, \textit{supra} note 23, at 44 (arguing that value-neutrality is a reason to reject limited access theories of privacy); Moore, \textit{supra} note 6, at 414 (stating that descriptive accounts are “largely uninteresting”).

\textsuperscript{70} Moore briefly touches on this issue in discussing Parent’s non-normative definition. However, he primarily assumes a normative conception is necessary and criticizes Parent for failing to provide one. Further, he does not address any of the arguments about why it makes sense to differentiate and develop both descriptive and normative theories, as Parent does.

\textsuperscript{71} Going even further, Parker suggests that an adequate definition of privacy must allow us to differentiate between five separate questions: “(1) whether a person has lost or gained privacy, (2) whether he should lose or gain privacy, (3) whether he knows that he has lost or gained privacy, (4) whether he approves or disapproves of the loss or gain, and (5) how he experiences that loss or gain.” Parker, \textit{supra} note 36, at 278.
nothing that makes it unique from other concepts. This position, sometimes called “reductionism,” but more accurately called “eliminativism,” suggests that “our concept of privacy highlights different and unrelated interests in the various contexts in which it applies,” such that “all talk of privacy could (and perhaps should) be eliminated in favor of talk of the unrelated interests.” For example, Judith Thomson argues that “every right in the right to privacy cluster is also in some other right cluster” and that “the wrongness of every violation of the right to privacy can be explained without ever once mentioning it.” For this reason, Thomson concludes, “there is no need to find the that-which-is-in-common to all rights in the right to privacy cluster and no need to settle disputes about its boundaries.”

The second form of skepticism rejects the eliminativist position and maintains that privacy is distinctive, but nevertheless denies its coherence. This position has been best developed by Dan Solove, who argues that most privacy theorists have created confusion by adopting what he calls the “traditional method” of conceptual analysis by which they attempt “to articulate what separates privacy from other things, what makes it unique, and what identifies it in its various manifestations.” Solove argues that it is a mistake to search for “the ‘essence’ of privacy” and the “common set of necessary and sufficient elements that single out privacy as unique.” Instead, he argues, we should understand privacy in terms of Ludwig Wittgenstein’s notion of “family resemblances,” which suggests that concepts are not held together by a single common characteristic, but rather by a common pool of similar elements.

Wittgenstein illustrates this view of language by reference to the concept of a game:

Consider for example the proceedings that we call ‘games.’
I mean board-games, card-games, ball-games, Olympic games, and so on.... [I]f you look at them you will not see

---

72 The contrary view, non-eliminativism, can take two forms: (1) fundamentalism, which maintains that the interest protected by privacy is an irreducible and sui generis interest; and (2) reductionism, which maintains that interest protected by privacy can be explained in terms of other interests, but that the concept of privacy cannot be eliminated in favor of a more fundamental concept. David Matheson, A Distributive Reductionism About the Right to Privacy, 91 MONIST 108, 108–9 (2008). See also Powers, supra note 6, at 372.
73 Matheson, supra note 72, at 108.
74 Thomson, supra note 28, at 313.
75 Id. See also Anderson, supra note 4, at 82; Richard Volkman, Privacy as Life, Liberty, Property, 5 ETHICS & INFO. TECH. 199 (2003).
76 Solove, Conceptualizing Privacy, supra note 3, at 1095.
77 Id. at 1096.
78 Id. at 1095.
79 Id. at 1090–91.
something that is common to all, but similarities, relationships, and a whole series of them at that.\textsuperscript{80}

Drawing on this metaphor, Solove argues: “Wittgenstein’s notion of family resemblances frees us from engaging in the debate over necessary and sufficient conditions for privacy, from searching for rigid conceptual boundaries and common denominator.”\textsuperscript{81} Instead, Solove argues, privacy theorists should adopt a pragmatic orientation and focus on understanding the features of different types of activities that can pose privacy problems.

While Solove’s approach to privacy is illuminating, it is important to recognize that it maintains the distinctiveness of privacy by denying that it has a core, which gives rise to two related problems that he does not sufficiently address. One problem is that the Wittgensteinian approach to language strips concepts of the power to do any normative work. While it does not matter if concepts such as “games” lack coherence, as the concept is not employed as the basis of normative claims, the same is not true of the concept of privacy, as matters of importance turn on its use. For example, it matters whether the Supreme Court cases recognizing reproductive rights are said to be based in principles of privacy or liberty. This is relevant not only to a proper analysis of the interests at stake (as privacy differs in important ways from liberty), but also to the legitimacy of the decisions (for example, their grounding in the text of the Constitution). Thus, while Solove’s taxonomy of “privacy problems” provides an illuminating account of practices that seem troubling to many, it is not clear that they entail the violation of privacy rights (or of other rights).

A related problem, identified by Ryan Calo, is that a Wittgensteinian approach treats classification as a pure matter of social convention: an activity counts as a “privacy problem,” or not, based only whether it has achieved a sufficient degree of social recognition as such.\textsuperscript{82} Thus, this approach provides no grounds for challenging a societal consensus about what counts as a privacy problem—and more problematically, it rejects the possibility of doing so. For example, if enough people were to agree that there can be no privacy in public or that non-persons can have privacy, these positions would thereby be correct. As Calo highlights, there would be no way of “denying that a given harm is a privacy harm… [or] arguing that a new harm should be included as a privacy harm, before the right sorts of authorities have

\begin{itemize}
\item \textsuperscript{80} Ludwig Wittgenstein, Philosophical Investigations sections 65-66 (Third ed. 1958).
\item \textsuperscript{81} Solove, Conceptualizing Privacy, supra note 3, at 1126.
\item \textsuperscript{82} Ryan Calo, The Boundaries of Privacy Harm, 86 Indiana L.J. 1131, 1141 (2011). See also Solove, Understanding Privacy, supra note 2, at 101–2, 172 (acknowledging this aspect of his account).
\end{itemize}
recognized it as such. Instead, one would just need to wait until they had done so.

In response to this criticism, one might argue that although the Wittgensteinian approach has these limitations, they are unavoidable if one wants to adopt a theory that can capture the heterogeneity of privacy that has been recognized in the literature. But this would be incorrect. Even if were true that the interests protected by privacy fail to cohere at a fundamental level, it would not necessarily follow that privacy lacks a distinctive core (as Thomson concludes) or unified core (as Solove concludes). To identify the problem with both of these conclusions, it is necessary to first differentiate between two ways in which a theory of privacy could potentially cohere.

2. Rethinking coherence

The first possible form of coherence, which the privacy literature has generally assumed is the only possibility, is normative coherence. On this approach, coherence would be achieved by identifying the criteria that uniquely justify all the rights that we consider to be privacy rights. This is goal of what Solove calls the “traditional approach” to conceptualizing privacy. While this goal has generally been assumed rather than chosen (as the alternative of descriptive coherence has generally not been recognized), it is nevertheless widely stated as the goal of theorizing privacy. For example, Reiman states: “What we are looking for is a fundamental interest . . . which provides a basis for a right to privacy to which all human beings are entitled.”

The assumption that normative coherence is the goal of theorizing privacy is not only found in those who adopt the “traditional approach,” but also in its critics. The growing skepticism about the possibility of developing a unified account of privacy assumes that normative coherence is the only form of coherence. It is only on the basis of this assumption that the heterogeneity of interests protected by privacy—and the intractable disagreement in the privacy literature—answers the question of whether a common account of privacy can be identified. But this assumption is unjustified, as normative coherence is not the only way in which the concept of privacy might cohere.

---

83 Calo, supra note 82, at 1141.
84 Id.
85 In developing this distinction, I draw on Madison Powers’s very helpful distinction between “justificatory reductionism” and “definitional reductionism.” Powers, supra note 6, at 384–85.
86 Reiman, supra note 18, at 38. See also James Rachels, Why Privacy Is Important, 4 Philosophy & Public Affairs 323, 333 (1975) (“[T]he first element of a theory of privacy should be a characterization of the special interest we have in being able to be free from certain kinds of intrusions”).
The second possibility, which has been largely overlooked in the literature, is descriptive coherence. Under this approach, coherence would be achieved by identifying the state of affairs that is uniquely described as the condition of privacy. The benefit of this approach is that it can accommodate the heterogeneity of the value of privacy. As Alan Rubel explains in another context:

There is little reason . . . to think that privacy has a single type of value. Privacy regarding one’s voting habits with respect to state actors may be an important political value, whereas privacy regarding one’s shopping habits with respect to marketers may be instrumentally valuable. Indeed, many instances of privacy loss are likely of no moral concern.\(^{87}\)

A descriptive theory can accommodate this heterogeneity by locating the coherence of privacy in a state of affairs, rather than the moral value of this state of affairs. Although a descriptive theory needs to be supplemented by a normative theory if we are to determine when privacy violations occur, this approach “ensures that we are talking about the same subject when we use the language of privacy rights.”\(^{88}\) So before exploring questions about privacy rights and their violation, it is essential to clarify the nature of privacy losses.

### III. Privacy Losses

I have thus far argued that the failure to differentiate between descriptive and normative theories of privacy—between privacy as a value-neutral state of affairs that can be lost, and privacy as a right that can be violated—has generated misguided critique and skepticism in the literature. In what follows, I turn to the first core question raised by this analysis: the question of how we should understand privacy losses. My analysis of this issue will give special consideration to the epistemological dimensions of privacy. Although privacy has frequently been defined in terms of knowledge,\(^{89}\) few have explored whether or how the various elements of knowledge . . .

---

\(^{87}\) Alan Rubel, *The Particularized Judgment Account of Privacy*, 17 RES PUBLICA 275 (2011). Likewise, Madison Powers concludes that we should “doubt that any value could be adequate to account for all cases in which privacy matters, or to suppose that any grouping of these diverse values uniquely supports privacy rights rather than rights of some other sort.” Powers, supra note 6, at 385.

\(^{88}\) Powers, *supra* note 6, at 386.

\(^{89}\) This approach dates back at least as far as 1890 when, shortly before Brandeis and Warren published their canonical article, E.L. Godkin defined the “right to privacy” as a person’s right “to decide how much knowledge of his personal thought and feeling, and how much knowledge . . . of his own private doings and affairs . . . the public at large shall have.” E.L. Godkin, *The Rights of the Citizen, IV—To His Own Reputation*, 8 SCRIBNER’S MAGAZINE 58, 65 (1890). More recently, knowledge has been incorporated into limited-access definitions
knowledge are actually essential to privacy losses (or privacy violations). My argument, in short, will be that a privacy loss occurs when a person or fact about a person is accessed in a way that has epistemic merit. There are three essential criteria in this account: access, epistemic merit, and truth.

A. Access

It is uncontroversial to suggest that access is at the core of many paradigmatic cases of privacy losses (such as those caused by wiretapping, computer hacking, physical surveillance, and the like), but my claim that it is an essential criterion faces three sets of challenges.

1. Mere accessibility

The first set of challenges comes from theorists who argue that privacy should be understood in terms of limited accessibility, rather than limited access. Anita Allen, for example, argues that privacy is the “condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others.” On this account, a privacy loss occurs whenever information becomes accessible to others, regardless of whether the information is ultimately accessed, and cases of complete though unexploited accessibility are “not adequately described as conditions of privacy.” If this is right, various new data-mining and processing technologies could generate privacy losses merely by increasing the accessibility of personal data.

---

90 Of privacy, e.g., Gavison, supra note 27, at 423 (privacy concerns “the extent to which we are known to others”), as well as control-based definition, e.g., Fried, supra note 24, at 483 (“Privacy…is control over knowledge about oneself”).

91 The one notable exception is a small set of articles published in a special issue of the journal Episteme on “Privacy, Secrecy, Epistemology” published in Volume 10(2) 2013. In addition, many privacy scholars have indirectly made arguments that are relevant to the epistemology of privacy, which I will draw on and refine in my analysis.

92 While a definition of privacy losses might also limit the types of facts that count, attempts to identify categories of “private” information face problems that have been identified in the literature. However, there might be some limits on the type of information that counts as a “fact about a person.” For example, it seems plausible that a person cannot “lose privacy about the fact that he is self-identical,” as that fact is not specific to any person. Don Fallis, Privacy and Lack of Knowledge, 10 Episteme 153, 156 (2013).

93 Id. at 29 (arguing that privacy would be lost, though not completely).

94 A similar conclusion would also follow from defining privacy in terms of a low likelihood of access, rather than limited accessibility. While the two criteria will often result in the same conclusion—and face similar objections (noted next)—they would result in different outcomes in some cases. For example, an email left open on a public computer might be easily accessible, but unlikely to be read (e.g., if the computer is rarely used); whereas an email on a secure server might be fairly inaccessible, but likely to be read (e.g., if it contains information desired by hackers).
In support of this account of privacy as limited accessibility, Allen and others have offered a variety of hypotheticals that they think will be seen as cases of privacy losses despite the fact that access itself has not occurred. Imagine, for example, that a government sets up an extensive camera surveillance system but does not turn it on; an ocean wave pulls off one's bathing suit but no one sees; a person finds a lost diary in a park but does not read it; or a hacker has access to one’s web-browsing history but chooses not to view it.  

While the intuitive pull of some of these examples is clear, it is a mistake to identify them as cases of privacy losses. To do so is to conflate the condition of privacy with the conditions that protect privacy. These are clearly cases in which people’s privacy is not well protected, and in which they may not have reasonable expectations of privacy. But while the protection of privacy may be relevant to the question of whether one can expect to have privacy in the future, it is not relevant to the question of whether one has privacy in the present.

In response, and in defense of an accessibility of account of privacy, one might argue that there are cases in which accessibility is worse than actual access. Compare, for example, the following two scenarios: (1) in which a nude photo of you is shared with one and only one person; and (2) in which a nude photo of you is made accessible to 100 people. It seems likely that many people would agree that it is worse to be in scenario 2 than it is to be in scenario 1—and one might argue that this demonstrates that scenario 2 entails a greater privacy loss than scenario 1.

This argument would mistakenly assume, however, that the undesirability in the two scenarios can be best explained in terms of privacy losses. The problem with this assumption can be seen by reference to cases involving monetary losses. Imagine, for example, that you can choose between these scenarios: (1) in which you will lose $100; and (2) in which you will experience a 10% chance of losing $10,000. As in the privacy cases, it is likely that most people would choose scenario 1 over scenario 2. But this preference does not entail the view that scenario 2 entails a greater loss of money—or a loss of money at all. While it is possible to identify losses and risks of losses that are functionally equivalent from an economic perspective, it does not follow that the risk entails a loss of money.

Of course, the imposition of risk might itself constitute a harm; but before getting to this issue, it is worth briefly noting that the economic

---

95 See, e.g., Allen, supra note 55, at 29; Alan Rubel, The Particularized Judgment Account of Privacy, 17 RES PUBLICA 275, 278, 284 (2011).

96 If this were the case and a monetary (or privacy) loss occurred at the time the risk was imposed, it would follow that a monetary (or privacy) gain would occur when the risk did not materialize. But this account would create confusion that is avoided by the normal way of describing this situation: there was a risk of a loss, but the loss did not materialize.
perspective does explain why scenario 1 is preferable to 2 in the above cases. It is because the probability-weighted value of the loss in the first scenarios is greater than it is in the second scenarios. Furthermore, while all of the cases that I have discussed have involved ex-ante uncertainty (about whether a loss will occur), the same analysis applies to ex-post uncertainty (about whether a loss has occurred).  

Thus far, I have argued that even if there are cases in which people would prefer accessibility to access, this does not suggest that accessibility is a form of privacy loss. There are also affirmative reasons to reject this claim. The most important of these arise from the fact that it collapses the distinction between privacy losses and risks of privacy losses, which generates two problems.

The first problem is that this account is unable to explain the qualitative difference between cases of access and cases of accessibility. Compare, for example, these two cases: (1) my email has been read by hackers, and (2) my email account has been hacked but my emails have not been read. The limited accessibility account of privacy would require us to conclude that there is, at most, only a minor quantitative difference between these two cases. But it seems that most would agree that there is a significant qualitative difference between a case in which my emails are read and one in which they could have been read.

To be clear, I am not saying that there is a qualitative difference between the privacy violations in these two cases. On this matter, the two cases might be similar or the same: for example, if the hackers conduct the same type of hack in both situations, the same privacy right may have been violated. But this does not mean that both cases entail a privacy loss. Rather, as I will argue in Part IV, the best account of the nature of privacy rights defines them by reference to privacy losses, while allowing for the possibility of violations without losses.

The second problem with the accessibility account is that it collapses the distinction, which should be morally relevant, between causing an outcome and causing a risk of the outcome. For example, if A buys surveillance technology in order to learn about B (and thereby makes information about B more accessible), he would have thereby caused B a privacy loss on this account; there would be no difference between causing a loss and causing a risk of a loss. Perhaps an advocate of the limited accessibility account would respond that an increased risk of a loss can be considered a type of loss. This position is itself controversial. But even when

---

97 For example, imagine that you can choose between being person A (who knows that his nude photo was shared with 1 person) and person B (whose knows that his nude photo might have been shared with 100 people); or A (who has lost $100) and B (who may have lost $10,000). The same analysis applies.
this is accepted, there is a recognized moral difference between causing a risk of a loss and causing the loss.

For all these reasons, the condition of privacy should not be defined in terms of limited accessibility; this account does not provide a viable challenge to the claim that access is necessary for privacy losses.

2. Lack of control

The second challenge to the claim that access is necessary for privacy losses comes from privacy theorists who argue privacy consists of control over information about oneself. While this account of the nature privacy has generally been advanced in normative theories of privacy (and is best interpreted as an argument about the content of privacy rights), it has also appeared in definitions of the condition of privacy, suggesting that privacy can be lost through losses of control. But this interpretation of the control theory of privacy faces significant problems.

One problem is that control is clearly not sufficient for privacy, as others have noted. Imagine, for instance, that I intentionally share previously-secret information about myself with a group of people who have an obligation (that I know they will uphold) to seek my permission before using or sharing the information with anyone else. In this scenario, there would be no change in my control over my information. But it seems uncontroversial to say that in this case, I have experienced a privacy loss (though not a privacy violation), merely because others have learned new information about me. For this reason, privacy cannot be defined simply as “control over knowledge about oneself.”

To avoid this problem, control-based theories of privacy might be interpreted as a supplement, rather than an alternative, to access-based theories. Support for this view (according to which control and limited access are both necessary but insufficient conditions for privacy) can be found in the work of Charles Fried, one of the most influential advocates of a control-based theory. In explaining the role of control in his canonical work on privacy, Fried writes:

As a first approximation, privacy seems to be related to secrecy, to limiting the knowledge of others about oneself. This notion must be refined. It is not true, for instance, that the less that is known about us the more privacy we have.
Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves. Here, Fried can be interpreted as saying that privacy exists when others have limited access to us because we have exercised control over their access. In support of this claim that control is necessary for privacy—that mere lack of access is not sufficient—Fried offers the example of an isolated person on a desert island: “To refer ... to the privacy of a lonely man on a desert island would be to engage in irony. The person who enjoys privacy is able to grant or deny access to others.”

Before turning to the merits of this claim that control is necessary for privacy, three caveats should be noted. First, it is unclear whether Fried’s claim is meant to apply to the value-neutral condition of privacy, or merely to the right to privacy. The latter seems to be the better reading, but I will tentatively assume the former, as Fried’s work has been used in this way. Second, even if Fried is referring to the value-neutral condition of privacy, it is unclear whether the passage is saying that the man on the desert island lacks privacy, or merely that the man lacks what is valuable about privacy. Again, the latter seems to be the better reading, but I will assume the former for the same reason. Third, it is unclear whether most people would agree that a man on a desert island lacks privacy. This is not my view, but as it is shared by some, I will set aside this question, accepting the premise (that the man lacks privacy) in order to challenge the conclusion (that privacy requires control).

Even if a man on a desert island lacks privacy as a descriptive matter, it does not follow that control is necessary for privacy. To see the problem with this conclusion, it is necessary to clarify the way in which this man would lack privacy on the proposed account. An example helps illustrate this. Imagine that the man, before becoming stranded on the island, is on a ship with others, where he maintains the privacy of the information in his diary. The ship then crashes, and he becomes stranded alone on an island. Presumably, no one would claim that at the moment he becomes stranded, he experiences a privacy loss with respect to the information in his journal that was previously kept private—that he loses privacy because there is no longer

---

102 Id. at 482.
103 Id.
104 Support for this interpretation comes from the fact that Fried says that control is necessary to “enjoy” (not possess) privacy and that it would be “ironic” (not false) to say the person has privacy.
105 E.g., Graeme T. Laurie, Challenging Medical-Legal Norms: The Role of Autonomy, Confidentiality, and Privacy in Protecting Individual and Familial Group Rights in Genetic Information, 22 J. LEGAL MED. 1 (2001); SOLOVE, UNDERSTANDING PRIVACY, supra note 2, at 20; INNESS, supra note 23, at 44. See also WESTIN, supra note 33, at 7 (arguing that “privacy is the voluntary and temporary withdrawal of a person from the general society”).
anyone to steal and read his diary. But if this is right and he does not suffer a privacy loss at this moment, the man on the island will not lack privacy in an ordinary sense, as the contents of his diary will have gone from being “private” to “not private” without any privacy loss. Thus, to the extent that the man on the desert island lacks privacy, it is in the technical sense that privacy gains/losses are not possible. But if this is what it meant, the desert island example does not pose a challenge to limited access theories of privacy, as it ceases to be a case of limited access without privacy. If the person on the island is not in control (in the technical sense that control is impossible), then access to the person is not limited (in the technical sense that access is impossible).

Moreover, if control and access limitations are impossible on the desert island, the hypothetical is not useful for exploring whether control is an essential element of privacy. To answer the question of whether control is necessary for privacy, we must look at cases in which control is possible but absent. (In addition, to eliminate a potentially confounding factor, it is important to look at cases where there is no access or risk of access). Take, for example, a case in which my doctor orders a genetic test with my consent, but then decides for clinical reasons to not look at the results or share them with me or anyone else; or a case in which the government holds information about me but refuses to share it with anyone. While these are cases in which I might not have a right to privacy—as the non-disclosure of my data is being imposed rather than chosen—it hard to imagine anyone arguing that this non-disclosure does not constitute the state of privacy. The best description of these cases is that my privacy (as a state of affairs) is being protected, even though I do not choose it. If so, personal control is not necessary for privacy.

If one does not have clear intuitions about these cases, however, it might help to make a slight modification to the facts. Imagine, for example, that after keeping my results secret for a month, my doctor subsequently discloses them to the public. If personal informational control is necessary for privacy (such that I did not have privacy in the first month), then I would not suffer a privacy loss when my information was disclosed to the public. But this conclusion would clearly be at odds with widespread judgements

---

106 Scholars have offered a variety of examples to support the argument that control is not necessary, but many of these confuse the analysis with examples that involve both loss of control and an increased risk of disclosure. For example, it is widely suggested that control-based theories should be rejected on the grounds that they fail to distinguish between actual and threatened losses of privacy: e.g., the difference between a case in which a peeping Tom looks inside a house, versus a case in which he is able to do so. It is suggested that because both cases involve a lack of control, they would both be privacy losses on a control-based account—and that this conclusion is clearly wrong, so the theory must be rejected. However, this type of counter-example has the potential to confuse matters as the two cases also differ in terms of access (in one case, there is access, and in the other, there is risk of access). It is helpful to keep risk of access constant when evaluating the relevance of control.
about privacy losses, suggesting that the claim that privacy requires control should be rejected.

In sum, lack of control is neither a necessary nor a sufficient element of a privacy loss. Like accessibility discussed above, lack of control might place one’s privacy at risk, but it is not constitutive of the privacy loss. Thus, this theory of privacy does not provide a viable challenge to my core claim that privacy losses turn on access.

3. Data capture and processing

The third challenge to the claim that access is necessary for privacy losses comes from those who argue that mere data capture and processing can cause privacy losses, independently of any human access to the information. For example, it has been suggested that privacy is implicated by unmonitored surveillance systems, the collection of cell-location data, web-scraping tools, algorithms that personalize content, etc. Setting aside possible control-based accounts of the privacy loss caused by these types of technologies (which I have rejected for reasons discussed above), there are three main ways in which they might be said to cause privacy losses.

One possibility is that the interactive features of these technologies can cause privacy losses. Take, for example, the Google algorithm that “reads” email messages in Gmail accounts and draws inferences about the users’ interests in order to provide personalized content. This type of targeting has been said to diminish privacy. While the argument here is not well-developed, one possible claim is that the display of the personalized content causes a privacy loss. In support of this claim, one might draw a comparison to the tort of intrusion upon seclusion, as the receipt of personalized content might be as unsettling as an intrusion (especially if it reveals interests that one thought were secret; or interests that one had not recognized in oneself). But this would vastly expand the concept of privacy losses, capturing cases of non-human intrusions clearly unrelated to privacy, such as disturbing noises.

In order to avoid this problem, one might argue that the privacy loss in fact arises from the underlying data processing: for example, the algorithmic discovery of a person’s interests, characteristics, etc. But like the intrusion-based argument, this argument would entail an implausible expansion of the concept of privacy loss. It would mean, for example, that a privacy loss occurs when an electronic scale displays a person’s weight, or a motion detector turns on a light when a person enters a room.\footnote{Cf. Matthew Tokson, Automation and the Fourth Amendment, 96 IOWA L. REV. 581, 617 (2011) (“[W]ithout some modicum of human observation, disclosure of our information to automated systems alone is ultimately no different from ‘disclosure’ to any other inanimate

\footnote{\textsuperscript{107} Cf. Fallis, supra note 91, at 165 (arguing that privacy is diminished by automated targeted advertising).}
these cases, the technologies gather and process data in order to generate new information about the people interacting with them.

Furthermore, there is a strong argument that automated data processing can actually protect against privacy losses. As Richard Posner has argued in the surveillance context, “computer sifting prevents most private data from being read by an intelligence officer or other human being by filtering them out.”

This leaves one final possibility: locating the privacy loss in the underlying capture of the data. In support of this theory of privacy loss, one might cite Jeremy Bentham’s Panopticon, which demonstrates how a surveillance system can incentivize prisoners to behave as if they are being watched, even if they are not. Applied outside the prison context, what this example illustrates is how data-capturing and data-scraping technologies can—even if no person is involved—produce the same type of chilling effects on behavior and speech as actual surveillance. On this basis, one might argue that mere data capture can cause a privacy loss. But the fact that mere data capture can have the same deterrent effect as human access does not mean that they both cause privacy losses.

Further, the intuition that privacy is implicated by mere data capture seems to be driven by the risk of human access—by the possibility that someone will decide to look at the data that has been collected. An example helps illustrate. Imagine, for instance, that a video camera surveillance system records the activities of someone living on a desert island. In this situation, the recording might put the person’s privacy at risk, as it would take inaccessible facts and make them potentially accessible (if it is possible that someone might access the recording in the future). But it is hard to see how the mere existence of the recording could be said to constitute a privacy loss.

If this does not seem clear, imagine this further modification of the hypothetical: the video cameras on the desert island are turned on and capturing data, but they are not recording anything. This is a case of pure momentary data capture, without any confounding factors. To claim that a privacy loss occurs in this scenario would seem to commit one to the further view that a privacy loss occurs whenever a picture of a person is momentarily created, including by less technologically-sophisticated means. But if this were correct, it would mean that even a mirror would cause a privacy loss—which presumably is not the view of those who suggest that mere data capture causes privacy losses.

object that stores our personal data. Automated computers alone do not ‘observe’ us any more than a digital bathroom scale observes our weight . . . or our word-processing document observes what we type.”).

109 Richard A. Posner, Not A Suicide Pact: The Constitution in a Time of National Emergency 97 (2006); see also Tokson, supra note 108, at 617 (“[A]utomated systems are increasingly the means by which we maintain privacy in a world where virtually every transaction involves the collection of personal information”).
In sum, while there is intuitive appeal to the claim that data capture and processing technologies can cause privacy losses, independently of any human access, this intuition does not withstand scrutiny. The strongest argument in support of it relies on the problematic conception of privacy as inaccessibility. What these intuitions capture is a concern about the risk of privacy loss. In addition, there is another problem with the view that non-cognitive access can cause a privacy loss, for as is discussed next, there are epistemic criteria for privacy losses that non-cognitive access will fail to satisfy.

B. Epistemic Merit

My argument thus far—that access is a requirement of privacy losses—raises the question of whether any type of access is sufficient, or whether it must meet additional epistemic criteria, such as those of knowledge. Although knowledge is included in many limited-access theories of privacy (defining privacy in terms of limits on knowledge) and control-based theories (defining privacy as control over knowledge), this element of their definitions has received little attention and there is almost no literature on it.110

The intuition that knowledge might be required to cause a privacy loss is not difficult to generate. Imagine, for example, that I have a dream in which I learn a secret piece of information about a person; that I later forget that I learned this in a dream and so believe that it is true; and that the information happens to be true as a matter of mere chance. It seems uncontroversial to suggest that this person does not suffer a loss of privacy via my dream, and that the reason for this is that the belief is not connected in any way to the fact that makes it true. The belief is true merely as a matter of luck.

The idea that mere true beliefs (i.e., beliefs that are true by luck) do not count as knowledge dates back at least as far as Plato, but the task of identifying the additional epistemic criteria that must be satisfied has challenged philosophers for generations. Increasingly intricate theories have been proposed in a vast literature, and there is still no consensus. Luckily, it is possible to answer the question of whether knowledge is required for privacy losses without reaching a definitive answer on what counts as knowledge. An understanding of some of the foundational approaches is sufficient to clarify whether knowledge—or as I will propose, a set of epistemic desiderata related to knowledge—is an essential element of a privacy loss.

110 See supra notes 89-90.
1. Theories of knowledge

A canonical way of explaining why merely true beliefs do not count as knowledge is to impose a justification requirement for knowledge.\textsuperscript{111} This is known as the “justified true belief” (JTB) theory of knowledge and requires that a true belief be adequately grounded in evidence and reasons to count as knowledge.\textsuperscript{112} This definition has clear intuitive force and was for a long time widely accepted. But it is now generally rejected for failing to exclude cases of epistemic luck. This is illustrated by the following non-privacy example (which I have created in order to make the following problems and responses easier to follow):

\textit{False Premise:} I believe that the lottery number will be 1215 because I believe that the machine has been rigged, and I have good reasons for this belief. But I am incorrect, and it has not been rigged; yet it nevertheless generates the number 1215 randomly.\textsuperscript{113}

In this case, I have a belief that is both true and justified; but because the justification relies in part on a false premise, my belief is only true by coincidence and so is insufficient for knowledge. This type of problem spurred an attempt to find additional criteria to add onto the JTB theory, such as a defeasibility criterion, which would require that the justification not be

\textsuperscript{111} The term “justification” is sometimes used in two different ways, which can cause some confusion. The term is traditionally used to refer to when a person has good reasons/evidence for a belief and is able to identify those reasons and evidence. However, the term is also occasionally used to refer to other ways in which a belief might be epistemically warranted (e.g., the types of warrant identified by the “causal” and “reliabilist” theories discussed below). In the interest of clarity, I will use the term in its narrower traditional sense.

\textsuperscript{112} There are different views on the question of how this line of reason-giving must ultimately be grounded for a true belief to count as knowledge, but such details are not crucial here. One view is that the process must end in some “foundational reasons” that are not supported by other reasons (a position known as “foundationalism”); another view is that the process can be grounded in a system of mutually supporting beliefs that cohere (a position known as “coherentism”).

\textsuperscript{113} This type of counter-example to the JTB theory of knowledge is based on Edmund L. Gettier, \textit{Is Justified True Belief Knowledge?}, 23 \textit{Analysis} 121 (1963), and is often referred to as a “Gettier problem.”
undermined by missing evidence. But this and other additional criteria proved unable to remedy all of the problems with the JTB theory.

This led some to reject the entire approach of defining knowledge internally (in terms of reasons/evidence), and to instead ground knowledge externally. An early example of this approach is the “causal theory” of knowledge, which suggests that a true belief is knowledge only when it is caused by the fact that makes it true: for example, I believe that it is hot outside, it is hot, and my belief is caused by the fact that it is hot. By imposing a causation requirement, the theory seems to exclude beliefs that are true merely by luck. But it soon became clear that this theory was also too permissive in some cases, such as:

Unjustified Trust: I believe the lottery number will be 1215 because my friend tells me that the machine is rigged, and the

114 The basic idea here is that knowledge does not turn solely on the evidence that one possesses (and the reasons for the belief that they provide), but also on the evidence that one does not possess. There cannot be any evidence that would, if one possessed it, undermine the justification of one’s belief. This explains why the case of False Premise is not knowledge. This criterion is often attributed to Keith Lehrer & Thomas Paxson, Knowledge: Undefeated Justified True Belief, 66 J. Phil. 225 (1969). A related earlier proposal was to add a “no false lemmas” criterion, which could deal with the problem posed by False Premise, but it soon became apparent that it was insufficient for reasons identified in Alvin I. Goldman, Discrimination and Perceptual Knowledge, 73 J. Phil. 771 (1976) (proposing the “barn facsimiles” hypothetical).

115 The reason for this is that even when true beliefs are based on good reasons and true premises, they might not rise to the level of knowledge. The problem can be illustrated with a slightly-modified case:

Missing Evidence: I believe that the lottery number will be 1215, and the reason for my belief is that I know it was rigged by my friend yesterday. What I do not know, however, is that another person subsequently fixed the machine, and that it was then rigged again in the same way by someone else.

In this case, all of the above identified criteria are met: my true belief is based on good reasons and no false premises (as the machine is in fact rigged), and having access to all the evidence (e.g., the fact that it was fixed and rigged again) would not defeat my justified true belief. Yet nevertheless, it would seem that my belief is not epistemically warranted, as it is again only true by chance. It is a matter of pure luck that the machine was rigged again in the same way. This is a slightly modified version of the well-known “barn facsimiles” counterexample to the “no false lemmas” criterion. See Goldman, supra note 114 (developing the “barn facsimiles” problem). Unlike in the “barn facsimiles” case (where a justified true belief becomes unjustified when new evidence is added), the justified true belief in this case continues to be justified after the new evidence is added (though it becomes justified on the basis of different evidence). It is possible that a defeasibility theory could account for the problem in Missing Evidence by maintaining that the relevant question is whether the new evidence would alter the justification for the belief (rather than rendering the belief unjustified). However, defeasibility theories also face other problems—most notably, the problem of dealing with “misleading defeaters.”

116 This also makes sense of the problem in Missing Evidence, supra note 115: the problem is that my belief is based in the fact that my friend rigged the machine, but that fact is not what causes my belief to be true. Rather, my belief is true because of a different fact (i.e., the fact that it was subsequently rigged, after being fixed, by someone else).
reason he believes it is rigged is that it is rigged. I also believe that my friend is a compulsive liar and should not be trusted, and I have good reasons for this belief; but when he tells me the machine is rigged, I believe him anyway (for no particular reason).

According to the causal theory, my belief would be warranted, because the causal criterion is satisfied: there is a causal connection between the fact that the lottery is rigged, the fact that my friend tells me that it is rigged, and the fact that I believe it is rigged. Yet it seems that I do not have knowledge, given that I have compelling reasons to believe that the machine is not broken, which I am ignoring for no reason. Further, while the causal theory is too permissive in this type of case, it is too restrictive in others. In order to address some of the limits of the causal theory, philosophers developed the third and final theory of knowledge that I will discuss: reliabilism. Instead of requiring an appropriate causal connection between the fact and the belief, reliabilist theories require that the process resulting in the belief produces true beliefs sufficiently often. Like the causal theory, reliabilist theories provide a fairly straightforward account of what makes knowledge non-accidental. But unlike the causal theory, they can explain why I lack knowledge when I rely on the unreliable testimony of my friend in Unjustified Trust. Like the other theories, however, reliabilism also has limits that render it an insufficient theory of knowledge. One core problem is illustrated by the following modification to the facts:

*Brain Implant:* I believe that the lottery number is going to be 1215 because I have a chip implanted in my brain that is connected to the lottery machine, which transmits the number to me before displaying it on the screen. I do not know, however, that I am connected to the machine in this way. I just experience a strong belief about what the number will be.

---

117 Notably, the causal theory is also too permissive in other cases, such as this modification to *Missing Evidence*, supra note 115: Imagine that I believe that the lottery number will be 1215 because I know my friend rigged the machine. What I do not know, however, is that there are many different machines that might be used. By chance, the rigged machine is used; so it turns out that I had a justified true belief, and that the truth and justification of my belief were caused by the fact that the machine was rigged. But this was a matter of luck; if I had known about the other machines, I would not have been justified in believing that the number would be 1215. Here, the defeasibility criterion explains the nature of the problem.

118 For example, the causal theory would seem to exclude that we can have knowledge of *a priori* propositions (e.g., “7 is a larger number than 6”) and counterfactuals (e.g., “if it had not been broken, it would have probably not generated the number 7”), as it is not clear how these beliefs can be causally connected to the facts that make them true.

119 This is based on a frequently discussed counter-example proposed by Keith Lehrer, *Theory of Knowledge* 163–64 (1990).
In this case, my true belief satisfies the basic requirement of the reliability theory, but it would be odd to say that I know what the outcome will be, as I do not have any reason to think that my belief is true. In this way, the reliabilist theory is insufficiently restrictive, which is just one of several grounds on which it has been rejected.\textsuperscript{120}

2. Epistemic warrant and privacy

In light of the challenges facing these and other theories of the nature of knowledge (I have only summarized the foundational attempts), some philosophers have argued that we should adopt a pluralistic approach to knowledge that recognizes a variety of epistemic desiderata.\textsuperscript{121} Setting aside the question of whether pluralism is ultimately satisfying as an approach to defining the nature of knowledge (a question that is outside the scope of this paper), I will suggest that this approach can be adopted to define the epistemic criteria that must be satisfied for privacy losses. To explain how, it is necessary to first take a step back and make two preliminary observations regarding the scope of the epistemic criteria that must be satisfied for a privacy loss to occur.

First, at one end of the spectrum, it seems clear that a completely unwarranted belief about a person is not sufficient to diminish that person’s privacy, for reasons I discussed at the start of this section. The hypothetical of the dream illustrated that in order to cause a privacy loss, personal information must be accessed in a way that has some epistemic merit. The belief cannot be true as the result of mere luck.

Second, at the other end of the spectrum, it seems clear that a privacy loss can occur in the absence of knowledge. Justified true beliefs, for example, are not needed, as Anita Allen illustrates with the example of a person who reads a celebrity’s diary that is known to contain a mix of “saucy facts and fantasy.”\textsuperscript{122} In this case, the person’s access to facts about the celebrity seems to cause a privacy loss, even though the person is not justified in believing any particular statement in the diary (given that the person knows that any statement could be fantasy). This suggests that justified true beliefs

\textsuperscript{120} There are four other dominant critiques. The first problem is that reliability does not appear to be necessary for a true belief to be warranted. Stewart Cohen, \textit{Justification and Truth}, 46 PHIL. STUD. 279 (1984). The second is the problem of defining the level of generality at which the relevant process is defined. Richard Feldman & Earl Conee, \textit{Internalism Defended}, 38 AM. PHIL. Q. 1 (2001). The third is the problem of “easy knowledge.” Jonathan Vogel, \textit{Reliabilism Leveled}, 97 J. PHIL. 602 (2000). The fourth is the problem of explaining why, on a reliabilist theory, knowledge is more valuable than mere true belief. Linda Zagzebski, \textit{The Search for the Source of Epistemic Good}, 34 METAPHILOSOPHY 12 (2003).

\textsuperscript{121} See generally \textsc{William Alston, Beyond Justification: Dimensions of Epistemic Evaluation} (2005).

\textsuperscript{122} \textsc{Allen, supra} note 55, at 21. Allen acknowledges that the “justified true belief” is just one way of defining knowledge.
LOSSES VERSUS VIOLATIONS

are not necessary to cause privacy losses—nor by definition are more restrictive versions of this general approach, such as those that add defeasibility criteria.123

Likewise, it seems clear that privacy can be lost through access that does not take the form of a causal connection. Imagine, for example, that I know—because I have access to data that is not widely known—that all the members of a given group (e.g., the group of people who voted for a particular political candidate) share a particular trait (e.g., they have an income of over a million dollars). If I then meet someone who tells me that he is a member of that group, I will know that he has that trait. This is a matter of basic logic (specifically, the principle of modus ponens). This suggests that a privacy loss can occur in the absence of a causal connection.

The same is true of reliabilist theories of knowledge: a privacy loss can occur even if information is accessed in a way that is not reliable. Don Fallis illustrates this with the example of a compulsive liar who knows a secret about someone and discloses it to others who know he is a compulsive liar and thus have good reason to doubt him (even though in this case he happens to be telling the truth).124 Fallis argues that in this case, the disclosure causes privacy loss even though the source is unreliable (and thus cannot support knowledge under a reliabilist account) and is known to be unreliable (and thus cannot support knowledge under a justification-based account).125

If the same is true for every other theory of knowledge when considered in isolation (which seems plausible, though not necessary to verify for reasons that will soon become clear), one might conclude that something more than true belief, but less than knowledge, is necessary to cause privacy losses. This is the conclusion reached by Dan Fallis, who is one of the few philosophers who has devoted significant attention to this question.126 On the basis of this conclusion, he attempts to identify the type of connection between belief and fact that is sufficient to cause a privacy loss. Drawing on causal theories of knowledge, he argues that certain types of causal connections will be sufficient, though not necessary.127 While this analysis by Fallis offers valuable insights, it is limited by the fact that he treats each theory of knowledge individually. In order to identify the necessary conditions for privacy losses, it is helpful to look past theories of knowledge in isolation.

---

123 For example: imagine that I correctly believe that my friend attended a secret club because I saw him entering it; but that unbeknownst to me, he has an identical twin brother who also attended the club. As knowledge of this additional fact would defeat the justification for my belief, I would not “know” that my friend attended the club, under this theory of knowledge. But clearly, he would have lost privacy in this fact.

124 Fallis, supra note 91, at 157.

125 Id.

126 Id. at 160.

127 Id. at 160–61.
If instead the competing theories of knowledge are seen collectively—i.e., as each identifying one criterion in a broader set of epistemic desiderata—a more significant insight emerges: in order to cause a privacy loss, the access must satisfy at least one desideratum in this set. This can be seen in all of the examples discussed above (each of which seemed to indicate that knowledge was not necessary). Take, for example, Anita Allen’s example of the celebrity diary. In this case, the justification criterion for knowledge is not satisfied, but the causal criterion is: there is a causal connection between the saucy facts about the author, the author’s inclusion of these facts in his diary, and the reader’s access to these facts. In Fallis’s example, by contrast, the justification and reliabilist criteria are not satisfied, but the causal criterion is: there is a causal connection between the truth of the information, the fact that the liar knows it, and the fact that the listener thereby gain access to it. Conversely, in my example of inferred traits, the causal criterion is not satisfied, but the justification criterion is (given that the belief is based in valid reasons), as is the reliabilist criterion (given that a deductive inference from true premises is a reliable means of producing true beliefs).

Furthermore, this pluralist account of the necessary conditions can explain cases in which privacy is not lost, such as in the case of true beliefs form via dreams. These true beliefs are not justified, caused by the facts that make them true, generated through a reliable process, etc., and so are properly excluded from causing privacy losses.

For ease of reference, I will refer to this requirement of satisfying at least one epistemic desideratum in the set—but failing to satisfy all the criteria necessary for knowledge—as the requirement of “epistemic merit”.

C. Truth

Thus far in my argument that privacy losses turn on access, I have assumed that the object of the access is a physical person or a fact about a person. But this is an assumption that must be explored and justified, as there are several privacy scholars who have argued that privacy losses can occur through the acquisition and disclosure of false information. In support of the argument that privacy losses can occur through access to false information, Pierre Le Morvan cites Anita Allen’s example

128 In addition, the reliabilist criterion is satisfied, assuming that reading people’s diaries is generally a reliable way of learning information about them.
129 E.g., Johnson, supra note 2, at 162; Rubel, supra note 95, at 277; Pierre Le Morvan, Privacy, Secrecy, Fact and Falsehood, 40 J. PHIL. RES. 313, 316–21 (2015).
(discussed above) of a celebrity diary containing “saucy facts and fantasy” being covertly obtained and read by a stranger.  

While Allen offers the example to support the claim that privacy losses do not depend on knowledge, Le Morvan uses it to argue that privacy losses do not even depend on true beliefs.  

He argues that if the stranger “believes several fantastical entries to be true,” the celebrity has “incurred a loss of privacy relative to these fantastical entries even though they are false.”  

While it might be the case that privacy is implicated in some way in this example, it does not necessarily demonstrate that access to false information can cause a privacy loss, as there are confounding factors. Most significantly, it seems that this conclusion is driven by the fact that the case arguably entails a privacy violation: the stranger’s covert method of obtaining the diary may have constituted a privacy violation, even if it did not cause a privacy loss. In addition, the stranger in the case will have gained some true knowledge about the celebrity’s diary, even though it leads to false beliefs.  

Without these elements, it is hard to imagine that anyone would think that the celebrity’s privacy is implicated. For example, imagine that the facts of the scenario generally stay the same, except for these two changes. First, the stranger finds the diary in a park, so there is no privacy violation. Second, the stranger is mistaken in thinking he has the celebrity’s diary; instead, he has the diary of the celebrity’s friend, on the basis of which he develops the same false beliefs about the celebrity. If access to false information about a person could cause a privacy loss, we would be forced to conclude that the privacy of the celebrity (and not her friend) would be diminished here. This is implausible. If anyone suffers a privacy loss in this case, it is surely the person whose diary has been read.  

The notion that privacy losses can turn on access false information also has other untenable implications, including about the privacy implications of correcting false beliefs. While those who advance this position have not weighed in on the question of what happens when false beliefs are corrected, it seems that they would need to adopt one of two possible positions, neither of which is plausible. One possibility is that access to false information creates a privacy loss, and that this privacy loss is not modified by the subsequent realization that the information is false. This cannot be right. If the thief realizes he has the wrong diary, this must alter the celebrity’s privacy loss. The other possibility is that access to false information creates a privacy loss, and that this privacy loss ceases to exist when the mistake is realized. But this would mean that privacy losses turn entirely on what people think they know, which is incompatible with the project of identifying the criteria of privacy as an objective state of affairs.

130 Allen, supra note 55, at 21.  
131 Le Morvan, supra note 129, at 318.  
132 Id.
2. Data disclosure

The claim that access to false information can constitute a privacy loss is also often supported with examples involving the disclosure of false information. For example, Alan Rubel offers this hypothetical: “Suppose that a healthcare provider confuses medical records such that P’s name is attached to the medical history of another. If the provider releases that record, it would seem that P’s privacy has diminished. P has a legitimate complaint against the medical provider and that complaint is grounded in a diminution of her privacy.”

While I imagine that most would agree that P has a legitimate complaint in this situation, Rubel’s further claim that this complaint is grounded in a loss of privacy is more controversial and must be further analyzed. The reason is that P’s complaint may instead be grounded in a related type of harm. According to Parent, for example: “The spreading of falsehoods or purely subjective opinions about a person does not constitute an invasion of his privacy. It is condemnable in the language of libel or slander.” Building on this claim, one might further argue that the intuition that privacy is implicated in Rubel’s scenario is motivated by the fact that the publication of true and false information can be equally harmful—but that it is a mistake to classify all information-related harms as privacy harms.

This line of objection strikes me as compelling, but it is unclear how far it applies. The open question is whether information-related harms (such as those captured by libel and slander) are at the core of all legitimate complaints about access to false information. Rubel argues that they are not. In support of this view, he asks that we imagine that in the hypothetical he has offered, patient P is benefitted by the release of the false medical records. According to Rubel, P would still have a valid complaint: “P’s complaint is that the record was released, period—and that release diminishes her privacy.” Again, I imagine that many will share the view that P has a legitimate complaint in this case, even if the information is beneficial. But it would be a mistake to conclude, on the basis of this view, that access to false information can itself cause a privacy loss. There are two reasons for this.

The first reason is that Rubel (like others who argue that informational conceptions of privacy are insufficient) is making a claim about whether P has a privacy-based complaint. But even if this claim is correct, it does not tell us whether P has suffered a privacy loss. Rather, it tells us whether he has suffered a privacy violation, and P can suffer a privacy violation without suffering a privacy loss.

\[^{133}\text{Rubel, supra note 95, at 277. See also Johnson, supra note 2, at 162.}\]
\[^{134}\text{Parent, supra note 6, at 269 n.1.}\]
\[^{135}\text{Rubel, supra note 95, at 277.}\]
\[^{136}\text{E.g., Johnson, supra note 2, at 160–61; Gavison, supra note 27, at 433.}\]
The second problem with Rubel’s conclusion is that the publication of information in his hypothetical does provide genuine access to P. The publication puts P into the public gaze, thereby causing a privacy loss (and also, possibly, a privacy violation). In this way, the situation is similar to that of a Peeping Tom who looks at a naked person through a hole in the person’s fence and develops a false belief that he has a tattoo. The person in such a case suffers a privacy loss, but not by virtue of the false belief; rather, it is because the Peeping Tom is in fact looking at him.

Finally, if privacy losses could occur through disclosure of false information, people would not be able to protect their privacy by disclosing false information about themselves to others. Imagine, for example, that a woman who is pregnant tells other people that she is not pregnant in order to protect her privacy. If access to false information can cause privacy losses, then the woman would diminish her own privacy (without a privacy violation) by spreading this false piece of information about herself. Perhaps some would describe this as a case of a trade-off between privacy losses, in which the woman loses privacy with respect to the false information but maintains privacy with respect to the true information. But it seems to me that the more natural description of this situation is that the woman lies to protect her privacy. This is yet another reason to reject the claim that access to false information can itself cause a privacy loss.

IV. Privacy Violations

The preceding analysis has sought to establish that the concept of privacy loss as used in ordinary language is defined and unified in the following way: a privacy loss occurs when a person or fact about a person is accessed in a way that has epistemic merit. Building on this, I will now argue that the core of privacy rights is that they restrict the means by which privacy losses can occur. On this account, a person suffers a privacy violation when a restriction on the permissible means of obtaining such access is breached. Unlike privacy losses, which are outcome-based, privacy violations are path-based.

To be clear, this is a primarily an argument about the form of privacy violations, and not their substance. Thus, this theory of privacy does not take a position on the question of which means of access are impermissible or what types of facts should be protected. Because it unifies privacy along its descriptive rather than its normative dimension, it is compatible with disagreement on these and other related normative questions. For example, it is compatible with and provides a foundation for Helen Nissenbaum’s argument that privacy rights should be understood as rights to “contextual
At the same time, the theory has a critical edge, challenging widespread claims about whether and how privacy rights are violated by data aggregation, the unconsented use of personal data, and the inference of private facts from disclosed data. Paying attention to the loss/violation distinction reveals that the scholarship on these issues has misinterpreted key Supreme Court cases, including the landmark technology cases of Carpenter v. United States and Kyllo v. United States. In addition, it helps clarify the normative reasons why privacy rights should not be expanded in the ways that have been suggested.

Note that in exploring the lessons to be learned from my theory of privacy violations, I will primarily focus on those that follow from its grounding in an access-based account of privacy losses, as these are likely to be the most controversial. But the other two criteria identified above—epistemic merit and truth—also highlight important questions that require further attention, which I will briefly explore in my analysis of the status of inferences.

Finally, it is worth clarifying in advance a crucial feature of the relationship between privacy losses and violations on this account. While privacy violations are defined terms of privacy losses (which provides for the coherence of privacy rights), this does not mean that a privacy violation can only occur if privacy is in fact lost. Rather, a restriction on a means of access that is meant to protect against privacy losses can be violated even if access to the person is not ultimately achieved.

A. The Path-Based Element

The role of the means of access in privacy violations has received little explicit attention in the literature, but upon analysis, it is clear that privacy rights do not restrict access per se. Rather, they restrict specific means

---

137 On Nissenbaum’s theory of privacy as contextual integrity, the right to privacy is “the right to appropriate flow of personal information,” and “inappropriate information flows are those that violate context specific informational norms,” which differ depending on the type of information at issue, the actors involved, and the principles under which the information is transmitted. Nissenbaum, supra note 8, at 9, 127.

138 See generally Strahilevitz, supra note 9.

139 Cf. Dworkin, supra note 10, at 116–18 (explaining that the theory that best fits and justifies an area of law will often not fit all of our judgements about it; rather, to achieve coherence, it will often find some judgements to be mistaken or misconceived).


of access (which I will refer to as “path-based” restrictions for short). This can be seen across our core constitutional, statutory, and common law privacy rights.

For example, the Fourth Amendment’s protection of “reasonable expectations of privacy” does not protect a reasonable expectation that a given piece of information will not be accessed (i.e., that the person will not suffer a privacy loss), but rather that the information will not be accessed in certain unexpected ways. This feature of the Supreme Court’s Katz jurisprudence has often been overlooked in the literature (giving rise to some confusion discussed in the next section), but it is hard to imagine anyone rejecting my claim. For example, as United States v. Jones highlights, it is impermissible to track a person’s movements with GPS for an extended period, but permissible to do so by following them in a car, even if both methods reveal the same location data. Even information in the home is protected by path-based restrictions, as the Court explains in Kyllo.

The core privacy statutes of state and federal law also do not restrict access, but rather specific means of access: for example, wiretapping telephones, intercepting electronic communications, using two-way mirrors in specified areas, and looking through the windows of a home. Likewise, the common law tort of intrusion on seclusion only provides a cause of action if the means of access is highly offensive to a reasonable person.

The same is true of rights restricting the generation of access via disclosure. Take, for example, the constitutional right to information privacy, which has been assumed (though not formally recognized) by the Supreme Court. In Whalen v. Roe, the Court held that the Constitution might protect an “individual interest in avoiding disclosure of personal matters,” but that this would only require the state to avoid unreasonable disclosure. As the state had taken adequate security measures (i.e., it had restricted the pathways

144 The Court frames the point from the other direction, but its substance is the same: “The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful.” Kyllo, 553 U.S. at 35 n.2.
145 See generally Solove, A Taxonomy of Privacy, supra note 1, at 491–93.
147 In two cases, Supreme Court has stated that it would assume there is such a right for the sake of its analysis, but it found that even if there is such a right, it would not have been violated. NASA v. Nelson, 131 S.Ct. 746, 749-51 (2011); Whalen v. Roe, 429 U.S. 589, 599 (1977)). In NASA v. Nelson, Justice Scalia strongly objected to the Court's working assumption, declaring: “A federal constitutional right to 'informational privacy' does not exist.” Nelson, 131 S.Ct. at 764 (Scalia, J., concurring).
by which disclosure might occur), there was no violation of the right.\textsuperscript{149} Path-based restrictions—regarding how and to whom information is disclosed—can also be found in a wide range of federal privacy laws.\textsuperscript{150} These laws also generally impose related duties, such as data security requirements, which likewise restrict means of access.

Thus, across the various areas of privacy law that restrict acquisition and disclosure, privacy violations are path-based: they depend not on whether a person or a personal fact has been accessed, but rather on how this has been achieved. (Under most of these rights, a violation also depends on what information has been accessed, but that is not relevant here).

Of course, as a normative matter, one might argue that there is no reason why privacy rights should be limited to path-based restrictions. For example, George Brenkert has argued that certain types of information acquisition can constitute a privacy violation regardless of the way in which they are generated:

[T]here are certain things which people (in their various roles as employers, government officials, physicians, etc.) and institutions (governments and businesses, etc.) ought not to know about individuals, however they might come to know these facts . . . For example, it would be wrong, however they went about it, for government officials to make it their business to know the details of the sexual practices of each particular citizen.\textsuperscript{151}

Brenkert further argues that “since they ought not to know such facts, those individuals who are the ultimate object of this knowledge may legitimately object to a violation of their rights.”\textsuperscript{152}

While many might agree with Brenkert that it would be wrong for government officials to seek to discover the sexual practices of their citizens via any means, it does not necessarily follow that that privacy losses can (in and of themselves) constitute violations of privacy rights. Two aspects of this conclusion require unpacking. First, even if one agrees with Brenkert that the government official who sees the person engaged in sexual activity “ought not to know such facts” about the person, it does not follow that he has a duty to not know them (and violates the person’s rights merely by knowing them).

\textsuperscript{149} Some lower courts have gone further and required the government adopt the least intrusive means of disclosure. \textit{E.g.}, Donohue \textit{v.} Hoey, 109 F. App’x 340, 361 (10th Cir. 2004).
\textsuperscript{152} Id.
Second, the government officials in the hypothetical have intent, which seems to drive the intuition that they are behaving wrongfully. To see this, imagine that there is no intent: for example, that a government official walks into a public bathroom where a person is engaged in sexual activity. In this case, it is hard to imagine a plausible normative argument that official violated the person’s rights.

Thus, it seems that most would agree with Judith Thomson when she writes: “[N]one of us has a right over any fact to the effect that that fact shall not be known by others. You may violate a man’s right to privacy by looking at him or listening to him; there is no such thing as violating a man’s right to privacy by simply knowing something about him.” Privacy rights that impose access restrictions should—as a positive and normative matter—be interpreted as restricting the means of access, not access itself.

B. Rethinking Aggregation and Use

While my argument thus far has focused on privacy rights that restrict access, there are practices that are widely said to violate privacy rights without violating access restrictions: namely, the aggregation and unconsented use of personal data. If it is true that these practices violate privacy rights, this would pose a problem for my account of privacy violations, along with the account of privacy losses that underlies it. As I will argue, however, they do not. Differentiating between privacy losses and violations reveals the nature of the mistake and sheds light on how we should actually understand the privacy implications of aggregation and unconsented use.

1. Aggregation

Both advocates and critics of a privacy right against aggregation often agree on one point: that courts have rarely recognized such a right, but that the Supreme Court did so in the recent landmark case of Carpenter v. United States, as well as in United States Department of Justice v. Reporters Committee for Freedom of the Press. This point of agreement is, however, based on a mistaken reading of the two cases. Attention to the loss/violation distinction reveals the mistake and clarifies what the Court actually held.

In Carpenter, the Court addressed the question of whether the government had violated the defendant’s reasonable expectations of privacy

---

153 Thomson, supra note 28, at 307. See also Scanlon, supra note 28, at 315 (describing privacy rights as enforcing “norms specifying when, where, and in what ways we may and may not be observed, listened to, questioned, and in other ways kept track of”).
154 For an overview of these positions in the literature, see Solove, A Taxonomy of Privacy, supra note 1, at 505–10.
under the Fourth Amendment when it obtained historical “cell-site location information” (CSLI) data from his wireless carriers. This included 12,898 location points over a period 127 days. Under the Court’s well-established “public exposure” doctrine, it seemed that this data would be excluded from Fourth Amendment protection. But in a significant shift, the Court found this doctrine inapplicable, in part because of the aggregated nature of the data. The Court held that although Carpenter had exposed each of his physical movements to different people at different places and times, he had not exposed the whole of his physical movements to any single person.  

In other words, by reframing the doctrinal question to focus on aggregated data and a single observer (rather than disaggregated data and multiple observers), if found that the public exposure doctrine did not apply. From here, it went on to conclude that “individuals have a reasonable expectation of privacy in the whole of their physical movements,” and that this expectation was violated when the government acquired Carpenter’s CSLI data.

In holding that individuals have a reasonable expectation of privacy in the whole of their physical movements, Carpenter has been widely described as a radical change in the Court’s Fourth Amendment jurisprudence. For example, Orin Kerr states that Carpenter creates an entirely new type of search:

_Carpenter_ holds, for the first time, that a search occurred without it being a taking of information from any particular place, thing, or person…. [T]he government simply ended up with too much information about someone. How it ended up with too much information isn’t particularly relevant in the Court’s view. The point is the result, not the process.

A similar point is made by others who suggest that Carpenter adopts the “mosaic theory” of privacy violations. The mosaic theory has been articulated in different ways, but the core idea is that the aggregation of information about a person can violate a reasonable expectation of privacy because it provides a picture that is greater than the sum of its parts. For example, in Justice Sotomayor’s Jones concurrence, she concludes that the aggregation of publicly-exposed location information could violate a reasonable expectation of privacy because it could reveal a person’s “familial,

---

157 Carpenter, 139 S.Ct. at 2217.
159 Carpenter, 139 S.Ct. at 2217, 2219.
161 See, e.g., Caminker, _supra_ note 158, at 21–25.
political, professional, religious, and sexual associations.”¹⁶² This language is, notably, quoted by the majority in Carpenter.¹⁶³

If it were true that Carpenter recognized a new type of privacy violation based entirely on “the result, not the process,” the case would pose a challenge to my claim that a core difference between privacy violations and losses is that violations are path-based whereas losses are outcome-based. But this interpretation of the case is based on a conflation of two different issues. While the Court in Carpenter quotes Sotomayor’s language from Jones, it does not follow her in concluding that a reasonable expectation of privacy can be violated by the aggregation of publicly-exposed location data. To see the error underlying this widespread reading of the case, it is necessary to differentiate between two different questions that arise in the case—questions that track the privacy loss/violation distinction.

The first question is whether Carpenter’s CSLI data is excluded from the Fourth Amendment’s privacy protections by virtue of the public exposure doctrine. Note that this is a privacy loss question, asking whether Carpenter has already lost privacy in his physical movements. It is in the Court’s answer to this question—not the substantive violation question—that it could be said to adopt a version of the mosaic theory.¹⁶⁴ As explained above, the Court holds that public exposure doctrine does not apply because “the whole” of Carpenter’s physical movements (i.e., the mosaic) was never exposed. For this reason, it is eligible for Fourth Amendment protection, giving rise to the second question.

The second question is whether the government’s acquisition of CSLI data violated a reasonable expectation of privacy protected by the Fourth Amendment. On this question, the Court does not adopt the mosaic theory, but rather recognizes a violation based on the means by which the government accessed this information. The Court’s decision is based on the fact that tracking via CSLI data allows “tireless and absolute surveillance” that is “retrospective,” “nearly infallible,” and “practically no expense.”¹⁶⁵ The Court holds that “when the Government accessed CSLI from the wireless carriers, it invaded Carpenter’s reasonable expectation of privacy.”¹⁶⁶ The fact that the means of access was central to the holding is confirmed by the Court’s subsequent clarification of its scope: “Our decision today is a narrow

¹⁶³ Carpenter, 139 S.Ct. at 2217
¹⁶⁴ At times, Caminker suggests that the Court adopted the mosaic theory in this way; but at others, he suggests that it adopted it as a theory of privacy violations. Compare Caminker, supra note 158, at 21 (discussing the public exposure question) with id. at 22 (discussing the “Court’s first-ever embrace of a mosaic-defined search”).
¹⁶⁶ Carpenter, 139 S.Ct. at 2219.
one. We do not … call into question conventional surveillance techniques and tools, such as security cameras.”

If the government had accessed the same information via a different permissible means, there would have been no violation.

Thus, Carpenter does not recognize a right against aggregation, as has been widely suggested. It is not the case that the government merely ended up with too much information. Rather, the process was central to the violation. The Court recognized a privacy right that imposes a path-based restriction on access to aggregated data. Carpenter thus supports my theory of the difference between privacy losses and violations, which in turn clarifies what is revolutionary about Carpenter—and what is not. Attention to the loss/violation distinction clarifies that the Court did not establish an entirely new type of search through aggregation, but rather recognized the possibility of privacy in public.

The same lessons can be drawn from Reporters Committee, which has surprising parallels to Carpenter, but in the context of the government’s disclosure of aggregated data under the Freedom of Information Act (rather than government’s acquisition of data under the Fourth Amendment). The question in this case was whether FOIA’s privacy exemption, which restricts disclosures that “could reasonably be expected to constitute an unwarranted invasion of personal privacy,” applied to FBI “rap sheets” that aggregated criminal information about individuals from various public sources. The Court held that disclosure of this information would constitute an unwarranted invasion of personal privacy, and on this basis, Reporters Committee has been cited as the first Supreme Court case recognizing that privacy can be violated by aggregation. As with the literature on Carpenter, however, this conclusion is mistaken because it fails to differentiate between two questions that track the loss/violation distinction.

The first question (the privacy loss question) is whether the aggregated data can be considered private if the underlying data is in the public domain. The plaintiffs in Reporters Committee advanced an argument similar to the government’s “public exposure” argument in Carpenter, and the Court rejected it on similar grounds, concluding that the aggregated data provided a picture of the individuals that was not in fact public. This conclusion has, moreover, been read as recognizing a privacy violation via data aggregation. But as with Carpenter, this reading is mistaken.

---

167 Carpenter, 139 S.Ct. at 2220.
168 See, e.g., Solove, A Taxonomy of Privacy, supra note 1, at 509.
169 US Dept. of Justice v. Reporters Committee, 489 U.S. 749, 761 (1989) (“[T]here is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information”).
170 See, e.g., Solove, A Taxonomy of Privacy, supra note 1, at 509.
When the Court in *Reporters Committee* addressed the second question (the privacy violation question), it explicitly rejected the claim that aggregation violated a privacy right, stating that the Constitution “does not prohibit such a compilation.” Instead, it held that that disclosure of the aggregated data by the government could cause a privacy violation. Thus, *Reporters Committee* recognized a path-based privacy right—a right to prevent the flow of information between two specific parties. Further, its rationale for recognizing this right was also path-based: it was because the government was able to require access to the data (i.e., a means of access not available to the public) that it had a duty of non-disclosure. So again, the case supports—and is clarified by—my theory.

Further, as a normative matter, the fact that the Court did not recognize a privacy right against aggregation in either of these cases should be seen as a good thing. There are two core sets of reasons for this.

One set of reasons arise from the fact that a right against aggregation itself would impose an outcome-based restriction, rather than a path-based restriction. This feature of the right is problematic in various ways that have been explored in depth in the critical literature on the mosaic theory. Some of the problems identified in this literature are specific to the Fourth Amendment context, but the core problems apply more generally. Orin Kerr, for example, has identified a dizzying set of questions that judges would need to answer in order to enforce such a right, leading many to conclude that the theory is unworkable. Imagine, for example, a case in which data is collected through various different forms of human and technological observation: should all the different types of data grouped together in the mosaic analysis, or are there multiple groups?—and does this change if the data was collected by different people for different purposes? There are also hard quantification questions: for example, if a technology records the location of person at 12 pm every day for five days, does this count five seconds or five days of location data? To answer these and related questions, it seems that courts would need to draw unprincipled lines.

In addition, and perhaps even more troubling, there are the problems facing those who want to conform their conduct to the law ex ante. For

---

171 *Reporters Committee*, 489 U.S. at 770. While the Court recognized that the accumulation of personal information posed a “threat to privacy,” *Reporters Committee*, 489 U.S. at 770, it is important to differentiate between risks and their materialization for reasons discussed above. See Part III.A.1.

172 *Reporters Committee*, 489 U.S. at 770.


example, a person who collects data using different tools at different times might often have no way of knowing whether he is going to end up with a privacy-violating mosaic. Further, data-gathering that is legal at the time that it is conducted could, at any point in the future, retroactively become unlawful if the data subsequently becomes part of a privacy-violating mosaic. For these reasons, amongst others identified in the literature, the mosaic theory is problematic as a theory of privacy violations (though not as a theory of privacy losses). This is one set of reasons why privacy rights should—as a normative matter—be defined as imposing path-based restrictions, not outcome-based restrictions.\textsuperscript{176}

Another problem with a right against aggregation that is highlighted by the loss/violation distinction arises in a standard account of the way in which aggregation violates privacy. This account suggests that aggregation violates privacy by revealing sensitive information that was not visible in the disaggregated data. For example, Solove writes: “People expect certain limits on what is known about them and on what others will find out. Aggregation upsets these expectations, because it involves the combination of data in new, potentially unanticipated ways to reveal facts about a person that are not readily known.”\textsuperscript{177} Likewise, as noted above, Justice Sotomayor’s concurring opinion in \textit{Jones} states that reasonable expectations of privacy are violated when personal location information about individuals is “recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.”\textsuperscript{178}

Paying attention to the path-based element of privacy violations reveals a potential problem with this account. For example, in Sotomayor’s example, it highlights that the government is not “acquiring” political/religious/sexual information about a person—at least not in the ordinary sense of the word. Rather, the government is inferring it. And the fact that information is being inferred, rather than discovered, is relevant in ways that have gone unexplored. On one hand, it could be argued, this account of the privacy violation avoids some of the problems identified above, as it locates the violation in the decision to analyze and draw inferences from aggregated data (rather than the mere fact that aggregation has occurred). On the other hand, the claim that aggregation can violate privacy on these grounds entails the premise that an inference is a means of access that can violate privacy rights. This premise, which has not been recognized or defended in the literature, is problematic for reasons that I explore in Section

\textsuperscript{176} This point has been recognized and developed by Gray and Citron, who argue that “quantitative privacy” should not be defined in terms of “how much information is gathered in a particular case” but rather on “how information is gathered.” David Gray & Danielle Citron, \textit{The Right to Quantitative Privacy}, 98 MINN. L. REV. 62, 126–30 (2013).

\textsuperscript{177} Solove, \textit{A Taxonomy of Privacy}, supra note 1, at 507.

C below. Before doing so, however, it will be helpful to first clarify the issue of unconsented use.

2. Unconsented use

The second challenge to my claim that privacy rights impose path-based restrictions on access comes from the claim that unconsented use of personal data can itself violate privacy rights. If the best theory of privacy rights includes rights that restrict unconsented use per se—thereby protecting pure informational autonomy—these rights would pose a challenge to my account. But as with aggregation, this expansive interpretation of use restrictions should be rejected.

To start with matters of existing law, this position is at best only plausible with respect to a limited set of privacy rights, and even in the case of this limited set, the claim should ultimately be rejected. There are four core points here: two about limits, and two about deeper problems.

First, a right to restrict or control the use of one’s information is not protected by any of the foundational areas of privacy law, including the Fourth Amendment, the common law privacy torts, and the constitutional right to informational privacy. Insofar as there is such a right, it is to be found in sector-specific privacy laws that have their origin in set of “principles of fair information practice” set out in a 1973 report by the U.S. Department of Health, Education, and Welfare. Among these principles is a “purpose specification” principle restricting use: “There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.” Whether this is accurately described as a principle of privacy, as is widely suggested, is question to which I will return below.

---

179 See Elizabeth E. Joh, Policing by Numbers: Big Data and the Fourth Amendment, 89 WASH. L. REV. 35, 63 (2014) ("The Fourth Amendment is primarily interested in the legitimacy of how information is acquired. If the acquisition is permissible, how the police use that information thereafter is generally not subject to an additional Fourth Amendment challenge.").


Second, even within the limited set of laws that adopt the purpose specification principle, use itself is not always restricted. For example, the Gramm-Leach-Bliley Act of 1999 has a section titled “limits on reuse of information,” but this section actually only restricts access, limiting the parties to whom personal information may be disclosed.\footnote{183} Furthermore, many statutes that do restrict use connect this restriction to an access restriction.\footnote{184} There are only a few statutes that impose access-independent use restrictions.\footnote{185}

Third, while it has been suggested that these use restrictions provide rights against unconsented use, embodying the idea of privacy-as-control,\footnote{186} this characterization misses an important point: the use and transfer of the data is often not under the person’s control.\footnote{187} Although unconsented uses beyond those authorized by the statutes are not permitted, the data subject is not in control of the uses that are authorized. For example, under the Fair Credit Reporting Act, consumers are not provided with the opportunity to opt-out of the creation, disclosure, and use of credit reports about them,\footnote{188} which suggests that the use restrictions are really about protecting fairness.

Fourth, the claim that these statutes provide rights against unconsented use is undercut by the fact that the restrictions are eliminated by anonymization (including in limited forms, such as pseudonymization and data perturbation). This is the case with the Freedom of Information Act.\footnote{189}

\footnote{\textsuperscript{183} 15 U.S.C.A. § 6802(c). Likewise, the Video Privacy Protection Act of 1988 only imposes restrictions on the parties to whom records may be disclosed, and the Cable Communications Policy Act of 1984 only restricts data collection and storage. 47 U.S.C.A. § 551.  
\textsuperscript{184} For example, under the Fair Credit Reporting Act, a consumer reporting agency can provide a credit report to a third party only for limited purposes (an access restriction), and any subsequent use must be in accordance with one of these permissible purposes (the use restriction). See 15 U.S.C. §§ 1681b(a), 1681e(e) (2000). The same structure can be found in the Driver’s Privacy Protection Act. See 18 U.S.C.A. § 2721 (the access restriction), § 2724 (the use restriction).  
\textsuperscript{185} For example, the Health Insurance Portability and Accountability Act regulations impose a wide range of restrictions on the use of medical information (beyond those necessary for treatment, payment, and health care operations), 45 C.F.R. § 164.508, and the Federal Election Campaign Act states that documents filed with Commission “may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes,” 52 U.S.C.A. § 30111.  
\textsuperscript{187} Paul M. Schwartz, \textit{Beyond Lessig’s Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices}, 2000 Wis. L. Rev. 743 (2001) (stating that the FIPP framework is an alternative to privacy-as-control).  
\textsuperscript{189} Am. Civil Liberties Union v. Dep’t of Def., 543 F.3d 59, 85 (2d Cir. 2008); Dep’t of the Air Force v. Rose, 425 U.S. 352, 381 (1976).}
Privacy Act of 1974, Health Insurance Portability and Accountability Act, Fair Credit Reporting Act, Video Privacy Protection Act, and many state genetic privacy laws. Further, this is not only a feature of these specific statutes, but rather a core part of the underlying FIPP framework. As Barocas and Nissenbaum explain, the framework provides two options: consent or anonymize. Thus, this approach only provides limited rights of control when the information is connected to the individual—when use would entail access. It does not provide a right against mere unconsented use.

Furthermore, as a normative matter, there are good reasons why privacy law should not include rights that protect against mere unconsented use. To do so would be to reinforce the mistaken conflation of autonomy and privacy. The conflation of these issues dates back at least as far as the Supreme Court cases describing constitutionally-protected rights to contraception and abortion as “privacy rights.” This categorization of these rights was widely criticized as creating conceptual confusion, and the Supreme Court has recently remedied this error. It now characterizes these reproductive rights (and other related rights) in terms of autonomy rather than privacy. Informational law should not re-introduce the confusion.

To state that privacy and autonomy should not be conflated is not to deny that there is a connection between them. For example, it is clear that autonomy interests provide one strong justification for granting privacy rights. As discussed in Part I, autonomy is at the core of most accounts of why privacy rights are important. But it is a mistake to then interpret these privacy rights as protecting a broader set of informational autonomy interests. This reasoning is similar to a common logical error, the “fallacy of the converse,” in which one starts with a true proposition and then invalidly infers its converse. In this case (stated simply), “protecting autonomy requires protecting privacy” is mistakenly taken to imply “protecting privacy requires protecting autonomy.” Likewise, the fact that autonomy justifies privacy rights does not mean that these privacy rights should take the form of a right to prevent unconsented use. As Paul Schwartz explains: “Protection of the capacity for self-determination requires a setting of limits on the collection of

---

193 In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 279 (Third Cir. 2016).
196 See sources cited supra note 39.
197 See generally Greene, supra note 38.
personal data, but it does not call for privacy-control as a central means of achieving these limits.”

In arguing that the unconsented use of personal information should not be restricted by privacy rights, I am not arguing that it should not be restricted on other grounds. For example, while the Fair Information Practices Principles have often been classified as an aspect of privacy law, it seems to me that they are actually (as the name suggests) about fairness. This is not, however, merely a linguistic point. Classification here has normative significance: when the interests implicated by unconsented use are properly identified, we will likely find that they do not justify rights as expansive as privacy rights.

C. The Status of Inferences

Having argued that the aggregation and unconsented use of personal information do not themselves violate privacy rights (independently of violating an access restriction), I will now turn to a final question that emerges from this analysis: the question of whether inferences violate privacy rights.

It is clear that the analysis of disclosed personal data can reveal personal facts that were not knowingly disclosed. Perhaps the most often-cited example of this is the case of Target correctly inferring the early-stage pregnancy of customers based on their purchasing pattern of items that were not explicitly linked to pregnancy, such as unscented lotion. This example will soon seem quaint, however, as machine learning algorithms are used to infer significantly more complex personal traits from seemingly-irrelevant data collected across disparate domains of life.

It is often said that these types of discoveries violate privacy rights, but this conclusion relies on the unexplored assumption that inferences can do so. Perhaps the fact that inferences can clearly cause significant privacy losses—and in ways that are often not reasonably foreseeable—makes it seem equally clear that they can violate privacy rights. As my analysis has highlighted, however, what privacy rights protect is not a reasonable expectation that privacy will be maintained; rather, they protect reasonable expectations that privacy will not be lost in certain ways.

Thus, the core unexplored question is whether privacy rights currently restrict inferences, and whether they should. This section will argue

198 Schwartz, supra note 187, at 759.
that inferences do not violate established privacy rights in the ways that have been widely stated, and furthermore, that the creation of privacy rights that could be violated by inferences would raise significant normative concerns that would (at the very least) justify restricting such rights in ways that have received insufficient attention.

1. The Fourth Amendment

It is often stated that the Supreme Court’s decision in *Kyllo v. United States* held that the Fourth Amendment can be violated by the inference of information in which one has a reasonable expectation of privacy or by the acquisition of data that allows for such inferences. In fact, the Court reached the opposite conclusion in this landmark case, which appears to be the only case of privacy law that explicitly addresses the status of inferences in privacy violations. It seems that significant confusion has arisen from the Court’s conclusion that an inference cannot “insulate” a search—a conclusion that it reiterates, without much discussion, in its recent ruling in *Carpenter v. United States*. In order to understand what the Court means by this, and the status of inferences more generally, it is necessary to clarify some of the significant complexities of *Kyllo*. Although the case is nominally about thermal-imaging, which might seem low-tech, the Court addresses complex epistemological issues that are directly relevant to the machine-learning algorithms of today.


201 There are a few cases that discuss whether the ability to draw an inference can eliminate a reasonable expectation of privacy. *Compare* Walter v. United States, 447 U.S. 649, 657 (1980) (holding that the defendants had a reasonable expectation of privacy in pornographic films, even though their boxes had allowed by government to “draw inferences about what was on the films”) with Arkansas v. Sanders, 442 U.S. 753, 764–65 n. 13 (holding that some containers, such as gun cases, “by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance”).

The core question in the case is whether the use of a thermal-imaging device to detect heat within a home violates a reasonable expectation of privacy protected by the Fourth Amendment. The Court holds that it does, but the case is decided in a 5 to 4 split with the disagreement focusing on the role of inferences in the case and in the law. This disagreement starts with a claim made by the dissent, which accuses the Court of ignoring “a distinction of constitutional magnitude between ‘through-the-wall surveillance’ that gives the observer or listener direct access to information in a private area” and “off-the-wall surveillance” that allows one “to draw inferences from information in the public domain.” According to the dissent, the Court’s finding of a search establishes “for the first time in its history….that an inference can amount to a Fourth Amendment violation.” In response, the majority accuses the dissent of adopting “the novel proposition that an inference insulates a search,” which it states is “blatantly contrary” to well-established precedent. From these statements, it might seem that the majority and dissent reach opposing conclusions about the legal status of inferences. But in fact, they do not. In order to understand their positions—and what the Court actually holds—it is necessary to unpack several issues.

To start, it is important to recognize that while the dissent seems to attach legal significance to the distinction between direct “through-the-wall” and indirect “off-the-wall” data gathering—which could be relevant to the operation of many algorithms (which are arguably “off the wall”)—it cannot be the case that the distinction has constitutional relevance in and of itself. As the majority notes, this position would be incompatible with well-established precedent: for example, the impermissibility of using directional microphones to listen to conversations inside the house, even though they measure sound from “off the wall.” In addition, it would be incompatible with the dissent’s position that a more sophisticated thermal-imaging device that reveals activities in the home would be impermissible, even though such a device would also only measure heat “off-the-wall” rather than “through-the-wall.”

For these reasons, the direct/indirect distinction must be relevant only to the extent that it maps onto the access/inference distinction that the dissent also highlights. This is a core issue that the government raised at oral

---

204 The opinion of the Court was written by Justice Scalia and joined by Justices Souter, Thomas, Ginsburg, and Breyer. The dissent was written by Justice Stevens and joined by Chief Justice Rehnquist and Justices O’Connor and Kennedy.
205 Id.
206 Kyllo, 533 U.S. at 44 (Stevens, J., dissenting). See also id. at 49 (“[T]he Court effectively treats the mental process of analyzing data obtained from external sources as the equivalent of a physical intrusion into the home. As I have explained, however, the process of drawing inferences from data in the public domain should not be characterized as a search.”).
207 Kyllo, 533 U.S. at 36.
argument, when the Deputy Solicitor General highlighted that police could not learn “directly from the imager” that heat was being generated inside the house. Rather, he explained, the police had to infer this, as it was possible that the heat had been produced in some other way: for example, the walls could have been “unduly heated up by the sun.”\footnote{\textit{Kyllo} v. U.S., 2001 WL 168056, 41-42 (U.S. Oral. Arg., 2001).} This reduced the “specificity and directness, the linearity of any inference” that could be drawn from the heat sensor.\footnote{\textit{Id.}; see also \textit{id}. (“There isn’t a one-to-one correspondence between heat on the exterior of the structure and heat on the interior of the structure.”).} Likewise, the dissent highlights that “the only conclusions the officers reached concerning the interior of the home were at least as \textit{indirect} as those that might have been \textit{inferred} from the contents of discarded garbage.”\footnote{\textit{Kyllo}, 533 U.S. at 44 (Stevens, J., dissenting).} This feature of the technology—the fact that inferences were required to gain knowledge of the inside of the home—provides the best explanation of why the dissent concludes that the technology “did not obtain any information regarding the interior of the home.”\footnote{While the dissent does not spell this out explicitly, this seems to be the best explanation of this conclusion. This feature also underlies the dissent’s comparison of the technology with other practices that were permissible under well-established precedent: “the only conclusions the officers reached concerning the interior of the home were at least as \textit{indirect} as those that might have been \textit{inferred} from the contents of discarded garbage… or pen register data… or, as in this case, subpoenaed utility records.” \textit{Kyllo}, 533 U.S. at 44 (Stevens, J., dissenting).}

In drawing this conclusion, however, the dissent fails to recognize the difference between two different questions, which is worth highlighting because it will be relevant to many technologies. The first is the question of whether one accesses a piece of information. The second is the question of whether one knows that one has done so. In this case, the police might not have known with certainty that the technology was revealing heat inside the house. Because of the potentially confounding factors, any conclusion about the inside of the home was an uncertain inference. But this does not mean that the technology was not in fact measuring heat from the interior of the home. One is a question of what they knew; the other is a question of what they did.

Unfortunately, this crucial distinction is not recognized by either side, which has resulted in significant confusion about key matters of law. This starts with the majority thinking that the dissent was making the “extraordinary assertion that anything learned through ‘an inference’ cannot be a search,” to which it replied: “The novel proposition that inference insulates a search is blatantly contrary to \textit{United States v. Karo}, where the police ‘inferred’ from the activation of a beeper that a certain can of ether was in the home. The police activity was held to be a search, and the search was held unlawful.”\footnote{\textit{Kyllo}, 533 U.S. at 36–37.} But as the dissent clarifies, this is not what it was saying:
Although the Court credits us with the ‘novel proposition that inference insulates a search,’ our point simply is that an inference cannot be a search, contrary to the Court’s reasoning. Thus, the Court’s use of United States v. Karo to refute a point we do not make underscores the fact that the Court has no real answer (either in logic or in law) to the point we do make. Karo itself does not provide any support for the Court’s view that inferences can amount to unconstitutional searches.\(^{213}\)

In order to unpack the disagreement here, it is necessary to first clarify a point about Karo. While the police in this case did infer that the ether can was in the house, as the majority’s comment highlights, Karo did not hold that this inference constituted the search. Rather, it held that the “monitoring of a beeper in a private residence” (i.e., the acquisition of raw data underlying the inference) violated the Fourth Amendment.\(^{214}\) Thus, the Kyllo majority’s discussion of inferences in Karo was not meant to establish that an inference can constitute a search, but rather that the acquisition of the raw data can constitute a search even if inferences are required to interpret it.

Unfortunately, the majority’s description of the holding in Karo did not only cause confusion in the dissent, but also in the literature on the legal status of inferences. It has led many to conclude that an inference can constitute a search and turn the underlying collection of data into a search. For example, Leslie Lunney concludes that the thermal scan in Kyllo was a search “because it made technology-assisted inferencing about the interior of a home possible,”\(^{215}\) and this interpretation of the majority’s statement is widespread.\(^{216}\) However, as should now be clear, this is not what the majority meant. The majority further clarifies this point in a footnote about its “insulate a search” comment:

The dissent asserts that we have misunderstood its point, which is not that inference insulates a search, but that inference alone is not a search. If we misunderstood the point, it was only in a good-faith effort to render the point germane to the case at hand. The issue in this case is not the police’s allegedly unlawful inferencing, but their allegedly unlawful thermal-imaging measurement of the emanations from a house. We say such measurement is a search; the dissent says it is not, because an inference is not a search. We took that to mean that, since the technologically enhanced emanations had to be the basis of inferences before anything

\(^{213}\) Kyllo, 533 U.S. at 44 n.3 (Stevens, J., dissenting).
\(^{215}\) Lunney, supra note 200, at 855.
\(^{216}\) See sources cited supra note 200.
inside the house could be known, the use of the emanations could not be a search. But the dissent certainly knows better than we what it intends. And if it means only that an inference is not a search, we certainly agree.\textsuperscript{217}

Here, the Court’s reference to what is “known” about the inside of the house points to the actual nature of the disagreement between the majority and dissent, which I touched on earlier. It is a disagreement about the level of epistemic warrant that is needed to cause a privacy violation. Whereas the dissent asks if the technology provides the police with knowledge about the inside of the house, the majority asks if it provides them with data about the inside the house.

Further, because they start with different questions without recognizing it, the majority misinterprets the minority’s legal position and vice versa. First, the majority: because the majority focuses on data acquisition and concludes that the technology does provide data about the inside the house (as a factual matter), it believes that dissent’s denial of a search relies on the assumption that an inference can insulate a search (as a matter of law). This is the only way the majority is able to understand how the dissent reaches the conclusion that there is no search. Second, the dissent: because the dissent focuses on knowledge and concludes that the technology does not provide knowledge of the inside of the home (as a factual matter), it believes that the majority’s finding of a search relies on the assumption that an inference can constitute a search (as a matter of law). This is the only way the dissent is able to understand how the dissent reaches the conclusion that there is search.

Thus, while it might appear that the majority and dissent reach different legal conclusions in the case because they disagree about matters of fact, it is actually because they disagree on a matter of law. They disagree about the epistemic status that is required for a search, and therefore ask different questions about the facts. While a complete analysis of this issue is outside the scope of this paper, I will make one brief observation, as it parallels my earlier argument about the “epistemic merit” criterion for privacy losses (Part III.B): although a means of access does not need to provide knowledge to violate the Fourth Amendment, as the Kyllo dissent assumes, it seems that the dissent was right to think that there is an epistemic requirement. Under Karo, at least, it seems that a means of access can only violate a reasonable expectation of privacy if it provides one with grounds for forming a true belief about the data at issue—that the mere fact that data is acquired by a technology is insufficient.\textsuperscript{218}

\textsuperscript{217} Kyllo, 533 U.S. at 37 n.4.

\textsuperscript{218} This epistemic requirement is implicit in the Court’s decision in Karo, where the police not only tracked the can of ether when it was inside a home (as discussed above), but also when it was inside a locker in a warehouse. While the Court held that the tracking in the home was
In sum, despite their disagreements and contrary to a widespread reading of the case, both the majority and dissent in Kyllo agree that an inference cannot violate a reasonable expectation of privacy. Further, neither opinion supports the claim that an inference of personal information from data can transform the underlying collection of that data into Fourth Amendment violation.

2. Beyond the Fourth Amendment

It is unclear whether other sources of privacy law, including the various sources that have adopted a version of the “reasonable expectation of privacy” test, will reach the same conclusion as the Supreme Court in Kyllo. But it is clear from the privacy literature that many would argue that this approach is mistaken and that inferences can violate privacy rights. There is insufficient space to properly address this issue here. I will merely identify three reasons to think that a privacy right against inferences would, at the very least, need to be more limited than has been recognized.

First and most importantly, a privacy right that restricted one’s ability to infer private facts about others would impose restrictions on purely mental activity. This would violate foundational principles of ethics and law. Even indirect means of mind control have been found unconstitutional. Thus, if privacy law were to recognize a right to prevent inferences, the scope of the right would clearly need to be limited to exclude mental inferences. Some distinction between human and non-human inferences would need to be drawn and justified.

Second, even if the right only restricted computer-assisted inferential analysis, it would impose limits on free inquiry, independently of any material harm. There are strong normative grounds, and potentially constitutional

---

a search (as discussed above and in Kyllo), it held that the tracking in the warehouse was not. The reason was that “the beeper informed the agents only that the ether was somewhere in the warehouse; it did not identify the specific locker in which the ether was located.” Karo, 468 U.S. at 720. The locker “was identified only when agents traversing the public parts of the facility found that the smell of ether was coming from a specific locker.” Id. The monitoring of “the beeper revealed nothing about the contents of the locker… and hence was not a search of that locker.” Id. at 720-721. Thus, although the beeper was in fact transmitting its location from inside the locker, it provided the police with no way to form a belief about its location inside the locker, and for this reason was insufficient to constitute a search.

219 These include the common law privacy torts, the Freedom of Information Act, the Privacy Act of 1974, the constitutional right of information privacy, and various evidentiary privileges. Lior J. Strahilevitz, A Social Networks Theory of Privacy, 72 U. CHI. L. REV. 919, 985–86 (2005).


221 Mendlow, supra note 220, at 2369–70.
grounds, to be concerned about such liberty restrictions. To determine whether these interests are outweighed by the privacy interests, it is necessary to differentiate between two different types of inquiry: data gathering versus data analysis. Restrictions on the freedom to engage in data gathering might be well-justified by privacy interests, but many of these justifications (for example, those based in a conception of private spaces) do not apply to restrictions on data analysis. Thus, there may be a stronger basis for limiting a right to prevent inferences—just as the First Amendment imposes significant limits on the right to prevent disclosure.

Third, the affirmative basis for recognizing a right to prevent inferences is limited in ways that have been obscured by the failure to differentiate between the different types of interests at stake. Imagine, for example, that a company’s HR department uses a sophisticated algorithm to predict health problems from non-health data in job applications. While the applicants in this case certainly have an interest in preventing the inferences, this is only partly an interest in preventing access to their health information (i.e., a matter of privacy). It is also—and arguably more so—an interest in preventing the use of this information in making a hiring decision (i.e., a matter of fairness). But to protect the latter type of interests, the law should grant rights that target this harmful conduct (e.g., a right against health-based discrimination), not a right to prevent the inferences. Of course, there may be cases in which it is difficult to prevent the harmful conduct, in which case preventing the inferences might be a justifiable second-best solution. But in this case, the right against the inferences would not be properly classified as a privacy right.

CONCLUSION

It is widely thought that the core problems posed by new technologies of personal data mining and analysis, as well as their solutions, can be explained in terms of privacy. There is also growing agreement that a unified theory privacy is unattainable. Both of these conclusions are misguided and derive from a failure to differentiate between the descriptive and normative dimensions of privacy—between privacy losses and privacy violations. The

---


223 Concerns about information gathering might also provide a better explanation of the concerns that people have articulated in terms of inferences. Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 GEO. L.J. 1147, 1223 n.119 (2017) (suggesting that although algorithms allow new kinds of inferences, “the underlying privacy problems that others have flagged appear to have been raised more by the collection of big data than by the use of machine-learning algorithms”).
difference is that a privacy loss occurs when a person or fact about a person is accessed epistemically, whereas a privacy violation occurs when a restriction on the permissible means of generating such access is breached. This theory of privacy fits and justifies our best judgements about when privacy is lost and violated, and it unifies privacy along its descriptive dimension, allowing for normative disagreement on questions such as which means of access are impermissible. At the same time, however, it has a critical edge that reveals that data aggregation, the unconsented use of personal data, and the inference of private facts do not violate privacy rights—at least not in ways that have been widely stated. It is possible that these practices should be restricted on other grounds. But when the actual interests at stake are identified, it will become clear that they do not always justify restrictions that are as expansive as those imposed by privacy rights. For all who are concerned about the ever-expanding uses of our personal data, this may appear to be a cost of the theory. If so, it should be accepted as the cost of coherence. Recognizing the difference between losses and violations reveals the unity and limits of privacy.