

# Claims to Privacy and the Distributed Value View

ALAN RUBEL\*

## TABLE OF CONTENTS

I.	INTRODUCTION .....	922
II.	WHAT IS PRIVACY?.....	923
III.	PRIVACY'S VALUE.....	925
	A. <i>Privacy as Instrumentally Valuable</i> .....	926
	B. <i>Privacy as Constitutively Valuable</i> .....	930
	C. <i>Reductionism</i> .....	935
IV.	THE DISTRIBUTED VALUE VIEW.....	936
	A. <i>Constitutive Value</i> .....	937
	B. <i>Privacy's Oddness</i> .....	939
V.	CIRCUMSCRIBING THE DISTRIBUTED VALUE VIEW:	
	CLAIMS TO PRIVACY.....	940
	A. <i>Privacy with Respect to Other Individuals</i> .....	942
	B. <i>Privacy with Respect to Organizations</i> .....	946
	C. <i>Privacy with Respect to State Actors</i> .....	948
	D. <i>Generalizing Claims to Privacy</i> .....	954
VI.	CONCLUSION .....	956

---

\* Department of Philosophy, University of Wisconsin-Madison. I appreciate the very helpful comments and discussion on this paper from Fred Harrington, Claudia Card, Russ Shafer-Landau, Harry Brighouse, Robert Streiffer, and the participants at the Institute for Law and Philosophy's conference on privacy, held at the University of San Diego School of Law in April 2007.

## I. INTRODUCTION

Consider three cases. In the first, a distracted customer leaves his credit card behind in a restaurant, where an opportunistic fraud artist finds it. In the second, an employer begins closely monitoring an employee's home and family life without her knowledge or consent, and with only the most spurious justification. In the third, as a person walks down her city street, she passes by dozens of people who notice her presence. In each case, the person's privacy decreases. In the first two cases, it seems clear that the loss to privacy impinges a claim.<sup>1</sup> It is equally clear that in the third case the loss impinges no claim at all. Moreover, the sort of claim implicated in the first two cases appears markedly different. The claim to privacy in one's credit card number primarily protects individuals from financial harm—it is a claim based on instrumental value. The claim to privacy in one's home and family life with respect to one's employer, however, is not clearly based on instrumental value, especially where the surveillance is surreptitious and unlikely to lead to adverse actions. The value of privacy in each of the three cases is different: instrumentally good, noninstrumentally good, and morally neutral.

This creates a puzzle with respect to claims to privacy. If privacy has very different value in different contexts, it will be difficult to determine where persons have claims to privacy. That is, if privacy does not have a unified value, it will not make sense to simply argue that a person has a claim to privacy solely in virtue of the fact that her privacy has been diminished. Compare this with other classic liberties: the diminution of one's freedom of conscience or freedom of speech is not morally neutral and is problematic independent of the instrumental value of that liberty. That justifies the view that people have claims to freedom of conscience and freedom of speech, and that diminution of those liberties demands at least some justification. This is not so with privacy.

My contention is that privacy's value is not unary, but distributed, and that whether privacy has value, and what kind of value it has, will depend on the privacy relation involved. However, I think that particular *sorts* of privacy relations do have value, and that such relations may be constituent parts of intrinsically valuable states of affairs. Accordingly, I

---

1. By claim, I just mean something short of an all-things-considered judgment of one's moral due. In that sense, one's having a claim is a necessary but insufficient condition for one to have a right, where a right is a valid claim of one's moral due. This follows Joel Feinberg's view in *The Nature and Value of Rights*. See JOEL FEINBERG, *The Nature and Value of Rights*, in *RIGHTS, JUSTICE, AND THE BOUNDS OF LIBERTY* 143, 143–58 (2d ed. 1997).

think that we can articulate some general principles regarding the conditions under which the value of privacy underwrites claims to privacy.

This paper is organized as follows. In Part II, I briefly explain my view of what privacy is—the particularized judgment account. I then turn to the question of privacy’s value in Part III, where I examine several views prominent in the literature. In Part IV, I outline my view of privacy’s value. I argue that, at its strongest, privacy has constitutive value, which is to say that privacy is a constituent part of intrinsically valuable states of affairs. However, in many cases, privacy’s value is not morally weighty. Unlike other goods to which privacy is compared, I argue that we must examine the particular features of privacy in each context to determine whether it has value. This makes it difficult to establish whether persons have claims to privacy. Nonetheless, in Part V, I provide some principles that guide claims to privacy based on its constitutive value.

## II. WHAT IS PRIVACY?

Although the central questions in this paper concern the value of privacy, it is crucial to be clear just what privacy means. In another paper, I develop what I call the particularized judgment account of privacy.<sup>2</sup> I describe it in brief here.

To begin, privacy necessarily involves a three-part relation between a person (or group of people), an object, and another person (or group of people): Person (*P*) has privacy about object (*O*) with respect to another person (*Q*);  $P_{OQ}$  will denote such a relation. Thus, to simply say “*P* has privacy” will always be incomplete. We can fill in the meaning of “*P* has privacy” by (1) pointing out a piece of information (for example, *P*’s thoughts), a view (for example, of *P* indisposed), or an action (for example, *P*’s decision to use birth control); and (2) by pointing out others who stand in some relation to *P* and *O*, for example, everyone, everyone but one’s confidants, or the state. Thus, to say that one’s medical care is private is to say, of a person (*P*) who receives medical treatment (*O*), some other person or persons (*Q*)

---

2. The full account of this view can be found in Alan Rubel, *The Particularized Judgment Account of Privacy* (Apr. 2, 2007) (unpublished manuscript), [http://papers.ssrn.com/sol3/cf\\_dev/AbsByAuth.cfm?per\\_id=353895](http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=353895).

either do not know of that treatment, do not interfere with that treatment, or may not interfere with that treatment.<sup>3</sup>

One area of contention in the privacy literature is what can properly be an object of privacy.<sup>4</sup> While there is no dispute that privacy may concern information, and there is little question that privacy may concern observations, there is a deep divide as to whether one may have privacy with respect to decisions in the following sense: *P* has privacy about her decision to have an abortion (*O*) with respect to the state (*Q*) insofar as the state may not prevent *P* from having an abortion. The three-part relation I describe may accommodate decisions as objects of privacy, but it need not. The focus of this paper, however, is on informational privacy, and to a lesser extent, observational privacy.<sup>5</sup> Thus, whether one may have privacy with respect to decisions does not bear on my analysis here.

The particularized judgment account of privacy draws on the view that privacy is such a three-part relation. It is based on the following two claims:

*Claim 1:* *P*'s having informational privacy about *O* with respect to *Q* means that *Q*'s ability to make a particularized judgment about *P* regarding *O* is limited.

*Claim 2:* *P*'s having observational privacy about *O* with respect to *Q* means that *Q*'s ability to observe *O* is limited.

It is fairly clear who may count as a *P* or a *Q* in a particular *P*<sub>*OQ*</sub> relationship. *P* must be a person or persons, and *Q* must be a person, group of persons, or an entity that stands in relation to *P* as another person could—for instance, an organization, a company, or the state. What can constitute *O*, however, is less clear. What sort of information can be an

---

3. *Id.* at 2. Note that this is a descriptive sense of privacy. There is also a normative sense of privacy. For example, we often say that something (*O*) is private, for example, one's naked body, voting decisions, or financial information, in the sense that a person ought to be able to prevent others from learning, seeing, or controlling *O*, or that *Q* ought not pay excessive attention to *O*, or that *P* ought to keep *O* out of *Q*'s view. Thus, *P*<sub>*OQ*</sub> might express a proposition about the way *P* or *Q* ought to act, regardless of the way *P* or *Q* actually acts. For the purposes of this paper, *privacy* and its cognate terms are used in the descriptive sense. *Id.* at 2–3.

4. See JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 26–27 (1997); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980), reprinted in PHILOSOPHICAL DIMENSIONS OF PRIVACY 346, 356–58 (Ferdinand David Schoeman ed. 1984); W.A. Parent, *Privacy, Morality, and the Law*, 12 PHIL. & PUB. AFF. 269, 271–74 (1983).

5. This sort of privacy is sometimes called physical privacy. Anita L. Allen, *Constitutional Law and Privacy*, in A COMPANION TO PHILOSOPHY OF LAW AND LEGAL THEORY 139, 148–49 (Dennis Patterson ed., 1999); William A. Edmundson, *Privacy*, in THE BLACKWELL GUIDE TO THE PHILOSOPHY OF LAW AND LEGAL THEORY 271, 272–73 (Martin P. Golding & William A. Edmundson eds., 2005).

object of *P*'s privacy? On the particularized judgment view, the only requirement is that the information pertain to *P*. Where *O* is merely a fact about the world, such as a distant historical fact, then *P* may not have privacy about *O* with respect to *Q*.<sup>6</sup>

The feature of the particularized judgment account of privacy that is crucial for this paper is that it takes an expansive view of what counts as a decrease in privacy. Anything that allows *Q* to make a more particularized judgment about *P* decreases *P*'s privacy about *O* with respect to *Q*. Thus, where *Q* learns a trivial piece of information about *P*, such as that *P* is walking down the sidewalk, *P*'s privacy about his whereabouts (*O*) decreases with respect to *Q*, though of course it does not decrease *much*.<sup>7</sup>

### III. PRIVACY'S VALUE

Presumably claims to privacy will have to be underwritten by privacy's value. To address the question of privacy's value, it will be useful to demarcate a couple of ways in which something can be valuable.<sup>8</sup> First, something is instrumentally valuable when its value comes from making some other good thing more likely to happen, or if it helps cause some other good thing to happen. Instrumental value depends on consequences. In contrast, where something is valuable, independent of its consequences (or its likely consequences), it is intrinsically valuable.<sup>9</sup> Intrinsic value may be further divided. First, there are things that are valuable in themselves, whose value is independent of whatever else exists.<sup>10</sup> Hedonists would place pleasure in this category, and Kantians would place the rational will in this category. But there are a number of goods that one might consider valuable in themselves: the good life, health, virtue, aesthetic experience, or intimate relationships. Things that are valuable in themselves may be complex, such that parts of those things are also valuable. Those parts are *constitutively* valuable. Thus, *X* is constitutively valuable when *X* is part of the reason why some intrinsically valuable thing, or some valuable state of affairs, *Y*, is valuable. And *Y* is valuable—at least in part—in virtue of having *X*. Joseph Raz explains this distinction by using art as an example. One might posit that a life in which one experiences

---

6. See Rubel, *supra* note 2, at 16.

7. *Id.* at 24.

8. Here I follow closely Joseph Raz's account in JOSEPH RAZ, THE MORALITY OF FREEDOM 200–01 (photo. reprint 1990) (1986).

9. *Id.* at 200.

10. *Id.*

art is valuable in itself, in which case, art would be constitutively valuable. Notice that in this case, art is not just likely to result in something intrinsically valuable; rather, art is part of the intrinsically valuable thing itself.<sup>11</sup> This description contrasts with a standard hedonistic utilitarian account, where only pleasure is intrinsically valuable. On the hedonistic account, a life in which one experiences art is good insofar as it generates pleasure, and art itself is instrumentally valuable—and only instrumentally valuable—because its existence causes pleasure, or makes pleasure more likely.<sup>12</sup>

There is little reason to think that privacy is valuable in itself in the way a hedonist considers pleasure valuable in itself. However, there are a number of possibilities for privacy's instrumental and constitutive value.

#### A. Privacy as Instrumentally Valuable

A number of accounts attribute broad value to privacy and justify generalized claims to privacy based on its instrumental effects. One such view is that privacy is instrumentally valuable insofar as it cultivates important relationships. Different sorts of relationships involve varying degrees of intimacy and revelation of different types of personal information. Charles Fried argues that publicizing intimate information decreases the moral capital necessary to share intimate information within relationships.<sup>13</sup> The idea, I take it, is that sharing personal information requires an emotional investment and risk. If the information is already out there—if *Q* already knows personal information (*O*) about *P*—then *P* takes no risk in relating the information. Publicity therefore causes some harm to relationships that depend on members taking emotional risks.<sup>14</sup> Similarly, losing control over information makes it more difficult to form those relationships that require a certain distance. It is harder, for example, to have merely cordial professional relationships when one's most personal information is

---

11. *Id.* at 201.

12. *Id.* The distinction is even clearer, and the reason constitutive value differs from instrumental value is clearer, in cases where a constitutive good is instrumentally bad. For example, the existence of art may be a constituent of the life with art, which is good in itself. But at the same time art might distract one from certain relationships that are good in themselves, causing them to founder, or making them less likely to flourish. This would suffice to make art instrumentally bad, independent of its being constitutively good. Of course, the same thing might be both instrumentally good and instrumentally bad as well, if it makes some good outcomes more likely and also makes other bad outcomes more likely. This example simply aims to make the contrast between constitutive value and instrumental value clearer.

13. Charles Fried, *Privacy [A Moral Analysis]*, 77 *YALE L.J.* 475, 475–93 (1968), reprinted in *PHILOSOPHICAL DIMENSIONS OF PRIVACY*, *supra* note 4, at 203, 211–212.

14. *Id.* at 207–12.

widely known. This leads James Rachels to argue that privacy is important “to maintain the variety of social relationships with other people that we want to have.”<sup>15</sup>

This view captures important features of privacy. One thing that distinguishes close relationships is the degree to which people in them share information, and it would be hard to consider someone who never shared much to be a close friend. Similarly, being unable to withhold information might make arm’s-length business relationships and casual friendships difficult or burdensome. However, this view is an unsatisfying account of privacy’s value and provides a weak foundation for privacy claims because, while privacy is instrumentally valuable in having many and varied good relationships (genuinely intimate relationships, arm’s-length business relationships, et cetera), it is also useful in having many and varied bad relationships. Just as the fact that *P*’s privacy about information allows him to decide whether and to what extent *P* will reveal that information to others, it allows *P* to decide who he will pretend to reveal himself to. Similarly, while such control of information allows one to conduct business at arm’s length by keeping personal matters outside the purview of transactions, it may also allow withholding information that other parties consider important to their businesses.<sup>16</sup>

A related view considers the instrumental value of privacy for people other than the one who has privacy.<sup>17</sup> Easy interaction is important for a variety of social goods. If *P*’s views about the fecklessness of her supervisors or the incompetence of her coworkers becomes widely known, it would be exceedingly difficult for work to go smoothly. Similarly, where people learn salacious facts about others, it becomes harder for them to focus on much else, thus stifling normal interactions. This view also provides a poor foundation for arguing that privacy is itself strongly instrumentally valuable. First, it largely depends on our facility in ignoring certain information. That some information makes normal social interaction difficult may be a reason to change our mores and mindsets rather than a

---

15. James Rachels, *Why Privacy Is Important*, 4 PHIL. & PUB. AFFAIRS 323 (1975), reprinted in PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 4, at 290, 292.

16. Richard Posner argues that personal privacy imposes substantial costs where people withhold potentially discrediting information. Richard A. Posner, *An Economic Theory of Privacy*, REGULATION, May–June 1978, at 19, reprinted in PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 4, at 333, 337–38.

17. See, e.g., Thomas Nagel, *Concealment and Exposure*, 27 PHIL. & PUB. AFFAIRS 3, 3–13 (1998).

prescription for reticence and privacy.<sup>18</sup> Moreover, this view is less an account of the instrumental value of privacy than it is an account of the instrumental value of inoffensiveness or politeness. There are a host of topics that can cripple normal interactions, but only some of them bear on privacy. It is hard to see, for example, how telling scatological or racist jokes is contrary to privacy, but the social effect of doing so is often similar to discussing personal matters: it is simply hard to get past.<sup>19</sup> The relevant fact about such a case is not privacy, then; it is shock value, perhaps, or offensiveness.

Another possibility is that privacy is valuable for the effective function of democratic processes. One such view is that privacy facilitates people's entry into positions of responsibility. Thus, if potential officeholders think that the likelihood and magnitude of disclosing embarrassing claims is great enough to outweigh whatever benefits public office confers, the pool of people from which officials are drawn will become smaller.<sup>20</sup> And if the pool of people from which we draw elected and appointed officials shrinks, the argument runs, then opportunities for good governance decrease because some well-qualified candidates will be among those culled.<sup>21</sup>

Such a view might be right, so far as it goes: protecting privacy generally may protect the pool of candidates for public office, which ultimately results in better officers. To the extent that it is speculative, though, it is a very weak justification for claims to provide. More importantly, such a view overestimates the importance of having the best qualified people hold public office. Certainly this is *desirable*, but it is

---

18. It is worth pointing out just how significant this can be. People may not wish to know of—or be able to get past in the way Nagel describes—things that are deeply important, and that would be better off in the open than concealed. Sexual orientation is like this. Some people do not wish to know whether others are gay, and knowing that others are gay makes social interaction difficult for them. A convention favoring reticence, though, has the consequence of making homosexuality less noticeable and easier to marginalize, which in turn reinforces the convention. Thanks to Claudia Card for pointing out this example.

19. Of course doing so reveals information about the joke teller, and responses reveal something about the audience, and to this extent they bear upon privacy. That is, *P*'s privacy with respect to disposition and sense of humor (*O*) decreases with respect to the audience (*Q*) when *P* tells an off-color joke. But this does not fully account for the impact of such a joke on social interaction. We may take it on good authority that *P* is crude and racist, and enjoys telling crude, racist jokes, but knowledge of that fact does less to social interaction than hearing him tell such a joke. Thus, the privacy/informational issue is ancillary.

20. Nagel argues, for example, that the enormous attention paid to Clarence Thomas and Anita Hill and to Bill Clinton and Monica Lewinsky had such an effect on people's beliefs about the possibility of disclosure, even if such scandals do not evince a greater likelihood of disclosures. Nagel, *supra* note 17, at 26–27.

21. Gavison, *supra* note 4, at 370.



only one of many justifications for democratic processes. Democratic governance is justified by consent of the governed, and because such consent requires information, privacy will take a subordinate role. It is no doubt unfortunate when people shy from service or when citizens focus on trivial matters. Avoiding that misfortune does count in privacy's favor. However, such considerations will pale next to citizen autonomy in political choices when it comes to making all-things-considered judgments about the value of privacy.

Another possibility is that privacy facilitates processes important for democracy. So, for example, privacy may facilitate democratic processes by fostering political associations. Interest groups, political parties, labor unions, and nongovernmental organizations play an important role in modern democracies, and the internal deliberations of such groups often provide the foundations for arguments made in public forums. That such deliberations are done internally and privately may allow good, but inchoate, ideas a chance to develop without attention from the broader public, which might stunt such development.<sup>22</sup> Certainly political associations themselves will often benefit from privacy. But it by no means follows that what benefits such associations also benefits democratic processes overall. Consider, for example, the contemporary U.S. practice of such associations writing, or helping to write, large swaths of legislation, which often passes with little opportunity for public deliberation. If the legislation is bad, then the inability for the public—including other associations—to examine it with sufficient time for public deliberation is instrumentally bad.

Instrumental accounts of the value of privacy are compelling in the sense that if the goods posited by an instrumental account (for example, certain types of relationships or better democratic structures) are in fact more likely to come about with greater privacy, then privacy is in fact valuable. But this is precisely their weakness as well. If privacy's value is merely instrumental, it is unlikely to provide a foundation for the broad privacy claims or the stringent privacy protections that many people think are warranted.

---

22. As Gavison writes, "Privacy is crucial to democracy in providing the opportunity for parties to work out their political positions, and to compromise with opposing factions, before subjecting their positions to public scrutiny." *Id.*; see also *NAACP v. Alabama ex rel. Patterson*, 357 US 449, 460 (1958) (holding that First Amendment freedom of association includes privacy of political association in order to guarantee effective expression of political views). See generally ALLEN F. WESTIN, *PRIVACY AND FREEDOM* 23–51 (1967) (analyzing the relation between privacy and democracy).

A second limitation of instrumental views of privacy's value is that they will tend to underdetermine the scope of valuable privacy. For example, the view that privacy is valuable for maintaining many and varied relationships gives us some reason to think that people having privacy about information in their day-to-day lives with respect to the general public is a good thing. However, it does not give us a reason to think that having privacy about medical information with respect to employers or insurers is a good thing. And the view that privacy facilitates democratic governance by incubating the inchoate policy views of political organizations may give us a reason to limit the availability of information about and observation of those organizations' internal deliberations, but it tells us nothing about whether individuals' privacy—other than facts about their participation in such organizations—is valuable.

A more significant problem for instrumental views has to do with the *relative* merits of privacy protection. That privacy is instrumentally valuable means that privacy makes some other good more likely to occur. This is a comparative judgment: Privacy makes a good more likely to occur than if privacy were absent. However, there may be other possibilities. Things other than privacy might facilitate that further good just as well as privacy does. In such cases there will be no reason to favor protecting privacy—and no reason to posit *claims to privacy*—rather than an alternative instrument.<sup>23</sup>

### *B. Privacy as Constitutively Valuable*

One appeal of the instrumental accounts is their conceptual plausibility; they are easy to make sense of. This is especially so because the view that privacy is noninstrumentally valuable is initially implausible. Privacy does not seem to resemble archetypical intrinsic goods, such as pleasure, intimate relationships, aesthetic experience, and virtue. It would be a mistake, though, to conclude that if privacy is valuable at all, it must be so only instrumentally. Another possibility is that privacy is closely and noninstrumentally tied to other goods that are themselves intrinsically valuable. That is, privacy may be constitutively valuable.

---

23. Adam Kolber raises the question of whether my approach of considering and discarding a series of potential instrumental benefits misses the possibility that privacy is overall instrumentally beneficial based on its combined value across many domains. This is an important point. I think it is correct that privacy will have various instrumental benefits across domains. However, as the discussion above suggests, I am uncertain of privacy's value in each context. I am therefore uncertain of privacy's cumulative value as well. In addition, note that I acknowledge that instrumental value will remain as a ground for privacy claims where privacy is of positive instrumental value. However, my task here is establishing claims to privacy that are not based on indeterminate instrumental value.

There are three accounts that are plausible constitutive value views: (1) privacy is a constituent of personality; (2) privacy protects meaning-conferring goods; and (3) failure to preserve privacy may be a failure to respect persons. Consider them in turn.

There is a cluster of views that take privacy to be fundamentally related to personhood,<sup>24</sup> personality,<sup>25</sup> or personal dignity.<sup>26</sup> Certainly personality, identity, and dignity are plausible candidates for intrinsic value; they are the sorts of things that one typically values in a way that goes beyond the utility they afford. Where one has little privacy, which is to say where others have unfettered access to information about a person and where that person is usually under observation, the opportunity to uniquely develop one's personality diminishes.<sup>27</sup> The extent to which one is responsible, in her own right, for who she is is diminished where there is no privacy—consider institutional settings such as prisons, the military, or boarding schools.<sup>28</sup>

A related and more promising view concerns the impact of privacy loss on the way persons view themselves and their relationships. Here I wish to draw on Ferdinand Schoeman's view of state intervention into family matters.<sup>29</sup> Schoeman argues that the reason parents ought to be

24. Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFFAIRS 26, 37–40 (1976), reprinted in PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 4, at 300, 310. Anita Allen refers to this cluster of views as *personhood accounts*. ANITA L. ALLEN, *UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY* 43 (1988).

25. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890), reprinted in PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 4, at 75, 82.

26. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. REV. 962 (1964), reprinted in PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 4, at 156, 187–88.

27. Reiman calls it conferring “[moral] title to one's existence.” Reiman, *supra* note 24, at 310. The idea, I take it, is that when one is responsible for one's personality or, as Reiman puts it, “self” (for example, when one's personality is mostly of one's own making), one can actually take credit or blame (“moral title”) for it. Insofar as privacy makes one responsible for one's personality or self, then, privacy allows one to take credit or blame for it.

28. This is not to say that one's decisions to enter such institutions, when voluntary, are not aspects of one's personality, and it is not to say that there are neither important instrumental reasons for such settings or some different measure of intrinsic value to shared or institutional identity. The claim is merely that some object of intrinsic value necessarily decreases with a thorough dismantling of privacy, viz., a personality that is to a greater degree one's own making.

29. Ferdinand Schoeman, *Rights of Children, Rights of Parents, and the Moral Basis of the Family*, 91 ETHICS 6 (1980). Thanks to Harry Brighouse for pointing out this view.

able to raise their children without state involvement (except in abusive situations) stems from the nature of intimate relationships, which are a source of much of life's meaning.<sup>30</sup> State intervention in family affairs changes people's view of family relationships from intimate, meaning-conferring goods to social goods, thus depriving people of a source of meaning. Schoeman's idea seems to be that self-monitoring, or viewing one's self and family as the kind of thing that is subject to intervention on social policy grounds, changes the nature of one's family relationships. Implicit in this view is that relationships' meaning stems in part from how people view those relationships.

Schoeman's idea is compatible with the view that privacy *per se* is a constituent part of the intrinsic value of intimate relationships. It adds the claim that not viewing a relationship as public is important as well, for its meaning as primarily an intimate relationship rather than a social good turns in part upon people not viewing it as a social good. This view runs into the problem of not explicitly distinguishing between privacy and the belief in privacy. As long as people in intimate relationships believe they are private, and therefore do not view the relationships as mere social goods, their meaning-conferring role is unharmed. This tension, though, points to another value in which privacy plays a role. It is important that our beliefs in privacy be well justified. Where we believe that we have privacy, but do not in fact have privacy, there is a harm. It is intrinsically valuable for our expectations to match reality, at least with respect to things we consider meaningful.<sup>31</sup>

Another way in which privacy may be intrinsically valuable is its relation to other things of intrinsic value. That is, it may be that impinging privacy necessarily undermines some other thing that is intrinsically valuable. On this view, a state of affairs is not valuable in virtue of *P*'s having privacy. Rather, it is valuable in virtue of some other facts, but *P*'s loss of privacy will entail that the intrinsic value of that state of affairs decreases. This view is not that privacy makes such states of affairs more likely—in other words, that privacy is instrumentally valuable in facilitating such states of affairs. Rather, it is that failure to respect privacy entails a failure to respect persons.

The clearest example of this approach is the view that privacy is valuable as the object of autonomous choice. There are two primary ways that this might be the case. First, there is the fact that people often prefer, and autonomously choose to retain, privacy about many things. When people so prefer, and especially when people so choose, loss of privacy

---

30. *Id.* at 14–15.

31. I develop this view more fully in Alan Rubel, *Privacy and the USA PATRIOT Act: Rights, the Value of Rights, and Autonomy*, 26 *LAW & PHIL.* 119, 153–54 (2007).

contravenes their autonomous choices. This is a weak foundation for the value of privacy. There can be any number of things that people autonomously choose that have no independent moral weight, and they are valuable only to the extent that people happen to value them—for example, consumer goods. Without some further reason to think that privacy is a more important object of such choice, it would be wrong to attribute special value to it just because people prefer and value it.

The more interesting possibility focuses on the importance of respect for persons as choosers who are able to develop their own sense of what is of value, and shape their lives according to that sense of value. That capacity, the argument runs, creates a reason to respect such choices, at least within certain domains. Thus, in *Privacy, Freedom, and Respect for Persons*, Stanley Benn argues that respecting others as persons demands, first, that one be conscious of himself as “capable of having projects, and assessing his achievements in relation to” those projects, and second, that one conceive of each other person as “actually or potentially a chooser, as one attempting to steer his own course through the world . . . and correcting [his] course as he perceives his errors.”<sup>32</sup> Understanding the other person in this way demands that we see what happens to that other person as important and valuable according to the terms she has chosen to guide her life by, in the same way that one measures the importance and value of one’s own life according to the terms one has set for oneself. In other words, we measure our own lives according to the projects we have chosen and terms we have set, and respecting others’ demands that we recognize others’ choices of projects and benchmarks. This respect, Benn argues, demands that we pay others a degree of consideration in their attitudes, choices, and projects.<sup>33</sup> The mere fact that others value something, of course, does not suffice to give one a reason to weigh that value. After all, *P*’s desire for free beer does not give *Q* much reason to provide it. Rather, others’ valuations are relevant when they “make a difference to the conditions under which [the other person] makes *his* choices, either denying him an otherwise available option . . . or changing the significance or meaning for [that person] of acts still open to him.”<sup>34</sup> *P*’s valuing privacy is relevant in this way, for where *P*

---

32. Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in NOMOS XIII: PRIVACY I (J. Roland Pennock & John W. Chapman eds., 1971), reprinted in PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 4, at 223, 228–29.

33. *Id.*

34. *Id.* at 229.

lacks privacy, it is likely to impact the way *P* pursues whatever it is that she values. And *Q*'s infringement of *P*'s privacy is a failure of respect for that valuation.

The constitutive value accounts are in many ways more satisfactory than instrumental accounts. Unlike the instrumental accounts, they do not depend on a causal story about the relation of privacy to some further value, and if privacy is constitutively valuable, other goods will not provide a substitute for privacy protections. However, the constitutive views still have important weaknesses. One is that the constitutive views do not fully cover the scope of valuable privacy. That is, certain aspects of privacy are clearly only instrumentally valuable (for instance, privacy in one's credit card numbers). Thus, privacy per se cannot be constitutively valuable. Rather, what is valuable are the goods furthered by privacy, or the goods of which privacy is a constituent part.

Another important concern with the constitutive value approach is that if privacy is valuable because impinging it in certain circumstances entails a failure to respect persons, it suggests that privacy is of derivative, rather than primary, value.<sup>35</sup> By this I just mean that privacy may be valuable generally, but privacy's value will be justified by its value in a variety of contexts, which together render privacy itself valuable. However, the direction of justification will be from specific varied instances in which privacy is valuable to the general proposition that privacy is valuable, rather than the other way around. Compare this with free speech. We take free speech to be a matter of right in a variety of contexts: political discussion, commercial advertising, artistic expression, active participation in one's communities. If free speech is justified in each of the circumstances by a general right to free speech, each of those instances of free speech rights will be derivative of that general right. On the other hand, if the general proposition that people have free speech rights is justified by each of the particular instances in which people have such rights, those instances will be primary and the general proposition derivative.<sup>36</sup> If the value of privacy—that is, the justification for any privacy claims—is that impinging on it in certain contexts entails disrespecting persons, it would seem that whatever general right to privacy

---

35. See, e.g., Richard Wasserstrom, *Rights, Human Rights, and Racial Discrimination*, 61 J. PHIL. 628, 629–30 (1964); see also J. Raz, *On the Nature of Rights*, 93 MIND 194, 197–98 (1984).

36. Raz helpfully illustrates this contrast with the example of a person's ownership of a block of real estate. If the person buys the block one parcel at a time, his rights of ownership in the block are derivative of the rights of ownership in the individual parcels. But if the person inherits the whole block in one transaction, his rights of ownership in the block are the primary, or core, rights, and his rights of ownership in the individual parcels are derivative. Raz, *supra* note 35, at 197–98.

we have will be justified by appealing to a number of those contexts. It will follow that privacy has no unique, independent value. This is not necessarily problematic; however, it is an important consequence to note.

### C. *Reductionism*

Because privacy has different value in different contexts, and because the constituent value views may render privacy of derivative value, it may be that we should take a reductionist approach to privacy's value, by which I mean that whatever value privacy appears to have is really the value of other goods. The most notable reductionist view of privacy comes from Judith Jarvis Thomson.<sup>37</sup> Thomson takes as a starting point the claim that there is little agreement about what privacy rights are, and the particular privacy rights that are widely agreed upon are quite disparate. She argues that privacy rights are in fact a cluster of other rights, including property rights, the right not to be looked at, and the right not to have certain pieces of one's information gathered.<sup>38</sup> Thus, whatever privacy rights we have are derivative of those other rights. Thomson is specifically concerned with rights to privacy, rather than the value of privacy, which is my focus here. However, if we take the view to be that different values underlie our various rights, and that only in combination do those various rights constitute a right to privacy, it seems plausible, if not necessary, that the values underlying privacy are also varied.

There are at least a couple of problems with this view. The first is that even if we can describe privacy rights as a cluster of other rights, this is not sufficient to say that the right to privacy is derivative of those rights rather than those rights being derivative of privacy rights.<sup>39</sup> Whether a right is derivative of other rights is a matter of its justification; that is, a right is derivative of other rights if, and because, those other rights provide the justification for the first right. The same is true of values. Whether the value of privacy derives from the goods of having one's property respected or not having one's information gathered does not follow from the fact that we can dissect privacy's value into distinct

---

37. Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. & PUB. AFFAIRS 295, 310–11 (1975), reprinted in PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 4, at 272, 284–85.

38. *Id.*

39. See ALLEN, *supra* note 24, at 41; Rachels, *supra* note 15, at 297–98; Reiman, *supra* note 24, at 300–02.

parts. It is at least as plausible that those parts are valuable just because privacy is valuable. The second problem is that, even if privacy's value is derivative from other goods, there may be something common to the goods that together comprise privacy's value.<sup>40</sup>

So, there are some reasons to think that the value of privacy is derivative of other values, and that the value of privacy at base relies on other values. The question becomes whether that suffices to show that a reductionist account is correct. I think that it does not. Contrast with other liberties, claims to which may be underwritten by several values. For example, individuals' freedom of conscience may be instrumentally valuable in maintaining a stable, pluralistic society, and it may be the case that impinging freedom of conscience entails disrespecting persons' autonomy. That is, there are a cluster of values that underwrite freedom of conscience. However, it need not follow that the value of freedom of conscience is reducible to those other values, or that the value of freedom of conscience is derivative of those other values. Rather, it only follows that the value of freedom of conscience includes those other values, perhaps in addition to whatever unique intrinsic (or constitutive) value it has.

#### IV. THE DISTRIBUTED VALUE VIEW

In the preceding part I considered a number of accounts of privacy's value. I argued that while instrumental views do account for some cases in which privacy seems valuable, they are a weak foundation for generalized privacy claims. I also considered three types of constituent value accounts, and argued that they were plausible, but incomplete. Finally, I argued that there is some merit in a reductionist account of privacy's value, but that such an account is ultimately unsatisfying. We are pulled in opposing directions. On the one hand, we have powerful, broadly held, and resilient intuitions that privacy matters and that people have some claim to privacy at least in some contexts. On the other hand, attempts to provide a justification for such claims are unsatisfying.

The way to proceed, it seems, is to revisit the particularized judgment account of privacy. If that view is correct and speaking of privacy without specifying a particular  $P_{OO}$  relation is necessarily incomplete, then it should not be surprising that the different conceptions of privacy's value are unsatisfying. After all, those conceptions fail to specify particular  $P_{OO}$  relationships. Indeed, it would be surprising if a unified view could provide a cogent case for the value of all, or even most, such relationships. This becomes even clearer if we take into account my expansive view of

---

40. Reiman calls the first criticism the "little non sequitur" and the second the "large non sequitur." Reiman, *supra* note 24, at 301.



what counts as a decrease in privacy. The particularized judgment view entails that privacy loss happens persistently and in mundane ways. An example I used above concerned *P* walking down the sidewalk where *Q* could see. On my view, this decreases *P*'s privacy about her whereabouts (*O*) with respect to *Q*. Such decreases in privacy happen frequently. Attributing value to privacy *simpliciter*, however, would commit us to either regretting the decrease or explaining why that decrease is an exception and therefore not of consequence.

As an alternative, I offer the distributed value view. On my view, the value of privacy will depend on the privacy relationships involved. That is,  $P_{OQ}$  may be valuable for one reason,  $P_{OQ'}$  may be valuable for a different reason, and  $P_{OQ''}$  may have no value at all. Thus, we cannot attribute any value, or any type of value, to privacy per se. This, I believe, motivates the reductionist impulse. Indeed, the distributed value view is reductionist in the following sense: whatever value privacy *simpliciter* has is just a function of the value of various subsets of privacy relations—for example,  $P_{OQs}$ . However, on the distributed value account, in contrast to the reductionist view, *types* of privacy relations—that is, privacy properly construed—will have value that is not similarly reducible.

#### A. Constitutive Value

In Part III, I set out the basics of a constitutive value approach to privacy's value. My task in this part is to expand on those ideas in order to better understand privacy as a constitutive value. Recall that there are two aspects of a thing having constitutive value: (1) it is part of some other good that is valuable in itself; and (2) the other good will be valuable in itself in virtue (in part) of the thing that is of constitutive value. To help illustrate why privacy may be of constitutive value, I begin by considering a few cases that illustrate the point, where a state of affairs is valuable in virtue of its being private.

The clearest examples concern privacy in intimate relationships. Suppose, for example, that two people are discussing something deeply important to them as an intimate pair—what is important to them in and about the relationship, perhaps. Unbeknownst to the couple, a police surveillance team, having trained its listening device on the apartment across the hall where legitimate criminal suspects reside, but picking up

more signal than they expect, is listening to every word.<sup>41</sup> Because the couple believes they have privacy—with good reason, given the constraints upon surveillance and the fact that they are not suspicious people—their loss of privacy is not instrumentally bad for their relationship. Moreover, the police in this case do not obviously violate a right or fail to respect the couple; the eavesdropping was accidental and came from good intentions. And yet it still seems as though something of value is diminished. I submit it is that the couple's conversation is no longer private, and its being private is a constituent part of the value of that conversation. One might argue that what is intrinsically bad in this case is the fact that the couple's belief in their privacy does not match reality. However, the fact that we all have mistaken beliefs of one sort or another makes this less important to the case. After all, the couple might also mistakenly believe that it is still daylight out as they converse, but this does not seem at all bad. The reason that the mistaken belief in privacy is important is that privacy is a constituent part of the value of their conversation; light conditions outside are not.

Why, though, should we think that privacy is important here? That is, what supports the assertion that privacy is a constituent element of the intrinsic value of the relationship and the conversation? There are two possibilities in the surveillance case; either the subjects are aware of the monitoring, or they are not. If they are aware of the monitoring, it will inevitably change the nature of their interactions. If, on the other hand, they are unaware of the monitoring, then they are acting under an important misconception. In either case, the value of the interaction itself diminishes, which is to say that privacy is a constituent part of the interaction, and it is a constituent in virtue of which the interaction has value.

Next, consider friends sharing a secret. The secret is not about something that would be harmful if revealed, and the friends do not really worry about the secret being exposed. However, the fact that they have privacy with respect to that secret seems good, even absent an instrumental benefit to sharing it. It is part of what defines the friendship, part of what constitutes the friendship, and therefore is intrinsically valuable. Note that the belief that they share secrets is not what helps define the friendship; it is the fact, if it is a fact, that they do so.

In addition to the intuitive cases, another reason to think that privacy is constitutively valuable concerns persons' expectations of privacy.

---

41. One can of course quibble with the example: Do the police violate rights—and therefore fail to respect persons—by not better calibrating their device? Do police have an obligation—legal or moral—to stop listening once they realize that the conversation is not relevant? Neither should impact the example, for the example can be modified to account for such objections.

Recall from Part III Schoeman's argument that state intervention in family matters is problematic because it treats families as a social good rather than a meaning-conferring good, which in turn leads people to view their own families as social goods rather than meaning-conferring goods, which has the effect of diminishing the extent to which families actually do confer meaning.<sup>42</sup> Privacy may have a similar feature—where something being public makes it more spectacle and less meaning-conferring. This, though, will depend upon people's beliefs about privacy rather than their actual privacy. Even so, I think that there is still reason to think that privacy itself is valuable here. It is valuable for things to confer meaning *for the right reasons*. So, if one takes an event's meaning to be in part constituted by it being private—for example, a shared secret or unobserved moments—but only because one is mistaken about it being private, that meaning is not well supported. It seems intrinsically good that the meaning we derive from events be well supported, and in those cases where privacy is part of that meaning, *actually* having privacy, rather than a mere belief of privacy, is a constituent part of that good.

#### *B. Privacy's Oddness*

The important features of the distributed value view thus far are, first, that it relates the descriptive view of privacy as a three-part relation with the question of value, and second, it accommodates the disparity in the values that seem to underwrite privacy claims. There is another important feature that I alluded to in the introduction, namely, that it is markedly different from other, classic liberties. As I set out the distributed value view, privacy will have value only in some cases, and will therefore only underwrite claims to privacy in some cases. This, though, contrasts with other types of goods to which people have claims. Compare claims to autonomy, freedom of conscience, freedom of speech, and freedom from harm. Each of these has some instrumental value, and there are many cases in which claims to each may be overridden. However, none has morally neutral instances, and each is more consistently a constituent part of something else that is itself intrinsically valuable. Thus, each of those goods serves to underwrite a claim fairly directly. So long as we can recognize a state of affairs as a decrease in freedom of conscience,

---

42. See *supra* notes 29–31 and accompanying text.

for example, a person losing that freedom has a claim.<sup>43</sup> That is emphatically *not* true with respect to privacy. Once we determine that *P*'s privacy about *O* with respect to *Q* has decreased, it is a further question whether *P* has even a prima facie claim that the privacy not decrease. This feature makes it difficult to determine just when people have claims to privacy. In the next part, I try to provide guidelines on that issue.

#### V. CIRCUMSCRIBING THE DISTRIBUTED VALUE VIEW: CLAIMS TO PRIVACY

The distributed value view holds that privacy's value is variable and will depend on the circumstances surrounding a privacy relationship. Depending on the circumstances, privacy may be morally neutral, of positive or negative instrumental value, or of constitutive value. Presumably, though, the point of discussing privacy's value in the first place is to determine whether and to what extent people have *claims* to privacy. But where privacy decreases are morally neutral, which is often true, one has no claim to that privacy. To the extent that privacy has weak or negative instrumental value, or where its instrumental value is offset by the instrumental value of a lack of privacy, it will fail to underwrite claims to privacy.

As I mentioned in the introduction, this creates a puzzle with respect to claims to privacy. If privacy has very different value in different contexts, it will be difficult to determine where persons have claims to privacy. That is, if privacy does not have a unified value, it will not make sense to simply argue that a person has a claim to privacy solely in virtue of the fact that her privacy has diminished. The purpose of this part is to help specify the conditions under which *P* has a claim to privacy about *O* with respect to *Q* based upon the constitutive value of that particular *P<sub>OO</sub>* relationship.

There are two points about this project that are important to make clear. First, the need for specificity derives from my view of privacy and its value, as recounted in Part IV. Second, instrumental value will always be a potential ground for privacy claims. However, as I argued in Part III, the instrumental value of privacy is often indeterminate. Certainly there are some instrumental benefits to a broad range of privacy relationships, but whether those relationships are instrumentally valuable overall is unclear. Relying on instrumental value, then, will be a weak foundation for privacy claims. But the distributed value account is in part a constitutive value account, and may therefore draw on

---

43. Again, this is something short of an all-things-considered judgment of one's moral due.

privacy's constitutive value to underwrite claims. Thus, in accord with the constitutive views outlined in Part III, we can say, as a general matter, where privacy has constitutive value, there will be claims to privacy.

First, *P* will have a claim to privacy about *O* with respect to *Q* where *O* is a meaning-conferring good, where *P*'s ability to derive meaning from *O* depends on *P*'s not viewing *O* as a public good, and where *P*'s loss of privacy about *O* with respect to *Q* tends to make *P* view *O* as a public good. The idea is that as it becomes possible for others to make more particularized inferences about a personal relationship, or about the way in which one pursues projects, or about the way in which a small group interacts, the degree to which those in the relationship, pursuing the project, or participating in the group see those things as public will increase, and the type of meaning that those people will draw from the relationship, project, or group will change.

Second, *P* will have a claim to privacy about *O* with respect to *Q* where *O* plays an important role in *P*'s shaping her personality and actions, and where *P*'s loss of privacy about *O* with respect to *Q* would lead *P* to alter *O*. One example that runs through the privacy literature concerns people's choices regarding what they read, write for their own consumption, watch, and listen to. *P* will have a stronger claim to privacy about *O* with respect to *Q* where *Q*'s learning about the things *P* reads, writes for her own consumption, and listens to leads, or is likely to lead, *P* to alter her habits.

Third, people will have claims to privacy where privacy is important in respecting their choices and valuations. This principle tracks the view that respecting persons demands taking seriously their choices and values in the projects and relationships that shape their lives. People care about, guard, and expect privacy. That concern may be a constitutive part of intrinsic value in the ways discussed above, and privacy itself may be part of people's conceptions of a good life. Moreover, because people place particular value on privacy in the domains they place at the center of their lives, respecting persons demands respecting privacy. Because of privacy's constitutive role, and because of the breadth and depth of the sentiment in favor of privacy, that concern and expectation are not unreasonable. Thus, *P* has a claim to privacy about *O* with respect to *Q* where *O* is an object that plays a central feature in shaping *P*'s life, and in which *P* has a reasonable concern for and a reasonable expectation of privacy with respect to *Q*.

But these are very general, and simply track the ways privacy may be constitutively valuable. We can glean other principles guiding claims by examining some examples, which I have organized according to the persons involved in the privacy relation; that is, according to the  $Q$  in the  $P_{OQ}$  relation.

#### *A. Privacy with Respect to Other Individuals*

As noted above, the particularized judgment view of privacy commits one to saying that Pete ( $P$ ) walking down the sidewalk where Jeff ( $Q$ ) can see diminishes Pete's privacy about his whereabouts with respect to Jeff. Generally, even if Jeff actively watches Pete, further decreasing Pete's informational privacy as well as his observational privacy, it is hard to see that Pete has lost something of value.<sup>44</sup>

Things are less clear in the case where Jeff finds Pete interesting, and starts to seek out information about him. That is, rather than casually observing Pete's walk, suppose that Jeff follows Pete around, keeping detailed notes about all of Pete's actions: where he stops, who he talks to, what he talks to them about, and so forth. Suppose further that Jeff photographs the walks, plots their course on a map, and compiles detailed data about the walks. Jeff begins to record other aspects of Pete's life: his work habits, his genealogy, and his friends and their habits. He picks Pete's paper coffee cup out of the garbage to get a saliva sample from which to analyze Pete's DNA, retrieves a hair sample from Pete's barber's floor to run a quick drug test, and purchases a list of calls to and from Pete's cell phone. Jeff takes all of this information and analyzes it in painstaking detail, trying to discern everything he can about Pete.

Jeff's actions clearly decrease Pete's privacy in many aspects of his life, and the situation is creepy, even if we stipulate that Jeff has no inclination or ability to physically harm, steal from, defraud, or defame Pete.<sup>45</sup> The questions are whether Pete has lost something of value, and whether Jeff has impinged a claim. One possibility is that it depends on Pete's point of view. If Pete discovers the extent to which Jeff has gathered and analyzed information, it is likely that Pete would be disconcerted,

---

44. There may be exceptions, though. Perhaps Pete is in some way disfigured, such that Jeff's attention is particularly intrusive, or perhaps Jeff is somehow menacing. Establishing such claims, however, would require arguments about why the particular case gives rise to a claim, as in the disfigurement case, and whether the claim is really about privacy at all, as in the menacing gaze case.

45. While stalking is criminal in all fifty states, persistent information gathering is generally not sufficient to constitute stalking under the relevant laws. The statutes generally require a credible threat to the victim or victim's family, and many require that the stalker have the intent to cause fear or that the victim actually fear injury or death. See Mark Irving, *Domestic Violence*, 4 GEO. J. GENDER & L. 451, 455-62 (2002).

even if he does not feel threatened. That kind of attention might lead Pete to monitor his activities to guard against embarrassing incidents and behavior patterns, or it might distract him from things he would rather be thinking about. Now, any of the various accounts of privacy's value can explain why this loss of privacy is at least *prima facie* problematic. The instrumental accounts can point to its effect on Pete's other valuable activities. The constitutive value views can argue that, first, Jeff has failed to respect Pete as a person who values doing things unmonitored, and, second, that Pete has lost something of value with his self-monitoring.

Neither of these views is satisfactory, though, for the instrumental view may get the calculation wrong—Pete's loss may be minimal, and Jeff's gain may be considerable. More importantly, if the constitutive value account relies on Pete's actual self-monitoring to underwrite claims to privacy, then Pete would have no claim if he failed to learn of Jeff's monitoring. And Pete would not have a claim if he did not particularly mind the privacy loss, nor would he have a claim if he minded, but was too preoccupied for the loss to affect his perceptions of his actions. Yet it seems clear that Pete's claim, if indeed he has a claim, exists independent of how Jeff's actions actually affect him.

One possibility to consider is that Pete does not have a claim to privacy about the various aspects of his life with respect to Jeff. There are a couple of ways to develop this possibility. First, one might say that Pete has some claim or other, but that the claim is not a claim to privacy. Thus, Pete might have a claim not to be followed, not to have his movements tracked, not to have his coffee cups and hair picked out of the trash and examined, and so forth.<sup>46</sup> One problem with this view is that it is not at all clear that Pete has a claim to each of the atomic parts of the larger claim. Many of Jeff's actions may themselves be morally neutral. For example, merely noting how Pete moves through the grocery store would not seem to give rise to any claim on Pete's part. And yet when such information gathering is combined with other privacy-impinging actions, it would seem to impinge upon a claim. Moreover, each of the discrete claims would need some explanation; the most plausible view is that they are based on claims to privacy. That is, it seems more plausible that Pete's privacy claim explains the individual claims (to not be followed, to not have his movements archived, et cetera) than that the individual claims explain Pete's claim that Jeff not monitor him.

---

46. See Thomson, *supra* note 37, at 284–85.

Another possibility is that Jeff's actions are problematic because Pete has not consented to being followed and his data being analyzed. But this would be question-begging, for one needs consent to get around doing something that would otherwise be morally problematic. It is generally wrong, for example, to stick a needle in a person's arm; thus, a medical provider needs a patient's consent to do so. But absent a reason to think that Jeff has done something wrong, consent is beside the point. Similarly, one might argue that Pete could simply ask Jeff to refrain from gathering information, and that would give rise to a claim. Perhaps it would, but that would depend on the strength of Pete's claims with regard to the underlying action. That is, Pete would have no claim that Jeff refrain from noting to himself what time Pete walks down the street, even if Pete requests that he do so. There may be an independent reason that Jeff ought to do as Pete asks—perhaps it is a virtue to be accommodating of such requests. But that is different from saying that Pete has a claim that Jeff do so. In contrast, if Pete has a claim to privacy in the first place, his asking Jeff to refrain from gathering information will indeed have normative force.

One might object that I have not differentiated observational and informational privacy clearly enough, and that the view that Pete has a privacy claim is based in part on Jeff's observation of Pete rather than Jeff's compiling information about Pete. Suppose, for example, that Jeff kept all of his findings in a computer file, which Kate finds and opens. Pete's loss of informational privacy with respect to Kate is just as great as his loss of informational privacy with respect to Jeff, and yet it is not at all clear that Pete has a privacy claim with respect to Kate. While it would be correct to say that part of our uneasiness with Jeff's actions comes from his close observation, we can easily imagine a case where Jeff does little actual observation, but still gathers a great deal of information about Pete. He might, for example, use cameras, surrogates, or listening and tracking devices to gather information. We cannot say that the surrogates observing Pete do something wrong, for each observation of Pete occurs in a place where such observations occur all of the time. Recall that a single surrogate watching Pete in the grocery store or on the street is morally neutral. It is hard to see why Jeff causing a morally neutral action to happen runs afoul of any claim. And yet the compilation itself still seems problematic.

The important difference between Kate and Jeff, moreover, seems to be the compiling. This variation points to something else worth noting: Jeff's actions do not merely decrease Pete's privacy with respect to Jeff. Because potential dissemination of information and the likelihood that others will be able to make judgments about a person both bear upon privacy, Jeff's information gathering decreases Pete's privacy with



respect to *all* people—or in any case, many people besides Jeff. Kate’s mere viewing of the assembled information therefore does not constitute as substantial a loss of privacy as Jeff’s compilation does. That is, Pete’s privacy about his life (*O*) with respect to everyone (*Q*) decreases substantially with Jeff’s actions, but Pete’s privacy about his life with respect to everyone decreases only modestly with Kate’s discovery.

The strength of Pete’s claims to privacy will also depend on the type of information gathered and domain of inferences underwritten in Jeff’s investigations. Compare the following two situations. In the first, Jeff follows Pete as he completes various errands; he records Pete’s grocery store deliberations and purchases, watches his driving habits, and so forth. In the second, Jeff follows Pete as he spends time with his friends and family, for example, by watching their interactions at a restaurant, listening in as best he can. The argument that Pete has a claim in the second case seems stronger than the argument that he has a claim in the first case. Thus, the number and particularity of inferences underwritten is not the only thing that matters with respect to one’s claims to privacy, but the subjects of inferences matter as well. One has less of a claim to privacy about commercial transactions with respect to other individuals than one has to privacy about friendly and familial relationships with respect to other individuals.

Supposing that this intuitive case is reasonable, it still demands some justification to be persuasive. The case for privacy claims based on constitutive value provides such a justification. Jeff’s actions fail to respect Pete’s reasonable desires for privacy, and the extent of Jeff’s surveillance is likely to draw Pete’s attention away from his projects and relationships in themselves and see them as open to viewing. This explains why Pete has a stronger privacy claim against incrementally greater surveillance *by Jeff* than he does against a privacy loss of similar magnitude carried out by Kate; Pete is more likely to engage in the sort of self-monitoring that conflicts with the meaning-conferring function of projects and relationships with incrementally greater surveillance by a single person than he is with smaller, discrete privacy losses about the same objects with respect to multiple others. It also explains Pete’s greater claims to privacy in matters regarding projects, relationships, and other meaning-conferring goods.

### *B. Privacy with Respect to Organizations*

While there are cases of people picking out individuals and fanatically finding out about them, and even publishing information about them, those circumstances are rare. Much more common is the collection of data from commercial transactions. Consider the case of commercial data brokerages, which compile, analyze, and trade substantial information about people's purchases, credit history, and public records. Much of this information comes from credit card purchases, use of store discount cards, magazine subscriptions, and so forth.<sup>47</sup> Such transactions by their very nature convey information about *P* to other *Q*s; moreover, those transactions depend on their being linked to other transactions by *P* and distinguished from all other people's transactions. For *P* to get her, and only her, subscriptions and credit card bills, and for *P* to establish good credit so that she can finance a mortgage, sign a lease, or finance an automobile requires that there be records that allow others to make particularized judgments about *P*'s financial circumstances, address, and other basic information. Thus, *P* consents, at least implicitly, to the accumulation and sharing of her information with the parties and institutions that are necessary in making the transactions possible.

One might object that inferring *P*'s consent to *Q*'s information gathering from *P*'s use of an institution that depends on information gathering is problematic. After all, when *P* applies for a credit card, mortgages a house, or buys things with a credit card, *P* may very well not realize what sorts of information are necessary to support her actions. Regardless, there are good reasons to infer consent. The first reason is that any credit user encounters a surfeit of evidence for such information sharing. One actually has to apply for credit, for example. More importantly, monthly bills contain itemized lists of purchases, and those lists come in the mail addressed to the credit user. Second, it is reasonable to think that credit users would consent to the information sharing necessary to support the institution of consumer credit, if asked. In contrast, it seems less reasonable to assume that consumers would consent to commercial data brokers sharing their information for purposes that are unnecessary for a functioning credit institution, for example, sharing the information with direct marketers. Finally, the larger issue is about *P*'s privacy claims. The fact that *P* may not give explicit, fully informed, and fully aware consent to information sharing does leave many of *P*'s claims intact. *P*'s explicit, fully informed, and fully aware consent to information sharing would clearly be sufficient for her to relinquish privacy claims with respect to that information. But

---

47. See generally ROBERT O'HARROW, JR., NO PLACE TO HIDE 42–52 (2005).

it is not reasonable to suppose that it is necessary to relinquish privacy claims, for *P* would be remiss to think that credit use involved *no* information sharing.

Suppose that a consumer, Pat, uses her credit card, store discount cards, and so forth for almost every purchase. She has the usual presence in public records, her address and phone number are in public directories, she subscribes to various newspapers and magazines, and so forth. Suppose, too, that she is well aware that those transactions are recorded and tagged as hers—and as noted above, the very existence of such transactions presupposes that kind of information collection. Over the course of several years, commercial data brokers have an extensive record of Pat's actions, which reveal patterns and proclivities. They have also used her public records to gather demographic information. Pat's address, for example, provides a number of clues to her socioeconomic status. In turn, brokers can use those records to make some predictions about the sorts of products Pat is likely to buy, the sort of advertising that is most likely to appeal to her, and so forth. It is hard to see how Pat would have a claim that data brokerages not compile, combine, and analyze such data. That Pat lacks a claim to privacy in this case is in line with the sketch of principles provided above. There is little reason to think that data brokers learning of her purchases, subscriptions, and public records would conflict with her drawing meaning from important relationships or projects, for example. Notice that this contrasts with similar levels of information gathering by individuals. Further, *ex hypothesi*, Pat is aware of the information that others gather, and presumably has no expectations otherwise.

Things are much less clear with respect to broader information sharing, as when a broker sells information to third parties. One possibility is that one has no claim at all to privacy about information revealed in public records and commercial databases. On this view, *P* has no claim to privacy about *O* with respect to any *Q*, so long as *O* is information in, or derived from, a commercial database, public records, or both. This view seems too strong for a couple of reasons. First, the broader sharing begins to conflict with Pat's expectations of privacy. While Pat may expect that others will compile some of her information, the downstream uses of her data will in all likelihood outrun those expectations.<sup>48</sup> If she has a

---

48. Note that on the particularized judgment view, *P*'s privacy decreases as more *Q*s have access to such information, and may thereby make more particularized judgments regarding *P*.

concern about that compilation, or if she would have a concern were she to learn of it, it becomes more plausible that she has a claim to that privacy.

While we can infer consent to some degree of information sharing from a person's taking advantage of institutions that depend on that sharing, as a broker puts information to broader and broader uses, the claim that a person has consented to its use becomes strained. Recall that the reason some degree of information sharing is permissible is not because there is explicit, informed consent to such sharing, but rather because one can legitimately infer consent from the fact that the consumer takes advantage of an institution that relies on information sharing for its existence. However, where the consumer does not take such advantage, that hypothetical consent is dubious. Suppose, for example, that a commercial data broker begins a program that analyzes its data so as to pick out people who work for one company or organization, but patronize competitors. The broker then markets the listing to companies as a tool to assess particular employees' loyalty. Now suppose that Pat uses her credit card and store discount card to pay for her weekly groceries at FoodStore, despite the fact that she works in marketing for GroceryMart, FoodStore's competitor. When GroceryMart learns of Pat's habits, it demotes or fires her.

In the same way that we can infer *P*'s consent to the information sharing necessary for the existence of the institution she participates in, we can infer that a consumer would *not* consent to certain types of information sharing, viz., those that are likely to harm the subject in normal circumstances. In the example, the decrease in privacy runs contrary to Pat's projects, which is something she could not have reasonably consented to, and the decrease in privacy therefore appears to be a failure of respect for her as chooser of such projects.<sup>49</sup> One might point out here that Pat's participation in information-sharing practices may in fact have a form of consent attached, as when creditors, magazines, warrantors, and so forth actually publish information regarding their privacy sharing practices. Notice, though, that relying on such policies to argue that Pat has no claim presupposes such a claim exists in the first place.

### *C. Privacy with Respect to State Actors*

In the previous two parts, I identified several factors that bear upon the question of whether *P* has a claim to privacy about *O* with respect to *Q*. One factor in determining *P*'s privacy claim is whether *Q* is another individual or a commercial organization. There are a number of reasons

---

49. Thanks to Fred Harrington for this point.

why the answer could make a difference. Organizations have fewer reasons to pick out a single individual to watch and analyze closely, and much of the information held in commercial databases is there because of implicit consent by the subjects or the information is not subject to privacy claims in the first place.

The next question I would like to consider is whether it matters that *Q* is a state entity when determining whether *P* has a claim to privacy about *O* with respect to *Q*. To begin, it seems clear that people have some claim to privacy with respect to the state. Police have limits on the degree to which they may follow, monitor, or keep tabs on us, and administrative agencies may not collect information about us without justification.<sup>50</sup> There are, of course, many cases in which state actors are justified in collecting information about individuals; but nonetheless, some justification is required. Moreover, it is certainly the case that one's legal claims to privacy depend upon whether it is the state or a private entity gathering information. Search and seizure law, for example, is replete with examples of searches that are permissible when performed by private parties, but impermissible with even slight government agreement, encouragement, or cooperation.<sup>51</sup> The question here, though, is whether

---

50. I mean this as primarily a moral claim, which I think is uncontroversial. Absent moral limits on the degree to which police and administrative agencies may collect and disseminate our information, we would have no grounds for complaint with unfettered searches and information collection, and no justification for restricting such searches and collection. There are also legal restrictions on police and administrative agency information gathering and dissemination, which are justified, I take it, by the moral claim. See, e.g., 18 U.S.C. §§ 2510–22 (2000) (limiting use of wiretaps); 5 U.S.C. § 552a(b) (2000) (“No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . . .”); 5 U.S.C. § 552a(e)(1) (2000) (requiring that each agency maintaining records shall “maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.”); 20 U.S.C. § 1232g(b)(1) (2000) (prohibiting the release of federal funds to educational agencies or institutions that release education records without consent).

51. See, e.g., *Burdeau v. McDowell*, 256 U.S. 465, 475–76 (1921) (holding search by private party did not violate Fourth Amendment even though information obtained in search was turned over to government prosecutors); *United States v. Walther*, 652 F.2d 788, 791–93 (9th Cir. 1981) (holding that an airline employee who had previously given, and been paid for giving, evidence to federal agents violated the Fourth Amendment when he opened a suspicious package looking for evidence of a crime); see also *Walter v. United States*, 447 U.S. 649, 658–59 (1980) (holding that tapes were permissibly seized by independent third party, but the FBI's subsequent screening of the films violated the Fourth Amendment); *Stapleton v. Superior Court*, 447 P.2d 967, 970 (Cal.

such differences are justified. I think that they are, based on three important differences between state and commercial privacy infringement. First, there is a difference in the amount of information use that individuals implicitly consent to in private transactions versus the amount they consent to in state information collection. Second, there is a difference in the degree to which state and commercial actors may act arbitrarily. Third, the reasons that support privacy's constitutive value are particularly salient with respect to state information gathering.

First consider the difference in consent. In Part V.B, I argued that much of the information collected and analyzed commercially comes from consensual transactions that are part of a practice requiring information sharing and analysis for its very existence. Participating in, and taking advantage of, an institution that demands substantial information sharing for its very existence—for example, consumer credit—implies that one consents to having her transactional information shared. Moreover, that consent takes place amid choice, for one can opt out of transactions that require particularized information, at least to a degree.

This is not true in the case of state-collected information. The state has an enormous power to collect information about income and finances, education, property, travel, et cetera. Having one's information collected in this way is impossible to avoid; indeed, much of it is compelled.<sup>52</sup> There is a sense in which people have consented to certain types of information gathering, in that democratically enacted laws and democratically created administrative agencies provide for information collection.<sup>53</sup> However, there is an important difference in democratic consent to certain sorts of information collection, and the consent implicit in consumer transactions. Consent to commercial information gathering is general, in that participating in, for example, credit card transactions, presupposes that the information generated from that transaction will be aggregated with all sorts of other information to verify that the person entering the transaction is legitimately entitled to the credit, as discussed above. But democratically based consent to state information gathering need not, and generally will not, take that form. So, for example, the information the state collects about students in public schools likely does not get

---

1968) (holding evidence inadmissible when a private citizen acts as an agent of the police and seizes private property as part of a joint operation with the police).

52. For an overview of federal and state government information gathering, see Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1141–48 (2002); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1400–03 (2001).

53. See Joel Feinberg, *Legal Paternalism*, in PATERNALISM 3, 16 (Rolf Sartorius ed., 1983); Robert Streiffer & Alan Rubel, *Democratic Principles and Mandatory Labeling of Genetically Engineered Food*, 18 PUB. AFF. Q. 223, 236–38 (2004).

aggregated with income tax information, unless a student is applying for financial aid; information gathered by the census is not aggregated with driver's license information, and so forth.

Moreover, unlike consumer credit, which is an institution that demands for its existence substantial amalgamation of information about particular individuals, much state information does not demand substantial amalgamation. One can, for example, run effective vehicle and driver's licensing programs without people's educational or income tax records. And when there is a need for a nexus of varied public sector information, people can provide consent to such consolidation. For example, we might make income tax records available to police during criminal investigations, but not otherwise. Thus, the consent given for state information collection will not underwrite the same degree of information amalgamation as the consent given to private information collection.

The second difference between state and commercial data collection concerns arbitrary action. I argued in the previous part that much of the data collection and analysis done by commercial data brokers is not problematic on the grounds that the subjects of the information implicitly consent to the collection and analysis. But of course people do not literally consent to every imaginable use of their data; rather, they consent to a reasonable range of data uses. The precise scope of that consent is not clear, but not important here. The important issue is that within that reasonable range, we think that commercial entities have latitude to analyze and use that data however they wish. In other words, individuals and commercial entities can for the most part act according to whatever reasons they see fit, with comparatively few restrictions. This is not true for state action. Any state action, and especially state action that bears upon something people consider deeply important, such as privacy, needs to have some justification, which is to say that state action ought not be arbitrary. This is important in that even within a government organization that collects information, the information should not be used for reasons that differ from the reasons that justify the collection in the first place. It is even more important across government agencies that keep their own data discrete.

To illustrate, consider ordinary police actions in the United States. We generally recognize that police have some discretion to stop people and investigate suspicious circumstances. However, that discretion is circumscribed. Police in the United States may not detain or seize a person without a reasonable suspicion based upon articulated facts, and

even then, their inquiries must be limited.<sup>54</sup> They may only pat down a subject to assure that the subject is not armed if there is reasonable suspicion that the detainee is armed and dangerous, but they may not fully search him for contraband without a higher standard of evidence.<sup>55</sup> Until recently, it was unclear whether police could demand that a person whom police reasonably suspect of wrongdoing had to identify herself;<sup>56</sup> even now, police cannot demand a person to identify herself without reason to suspect that the person is involved in criminal activity.<sup>57</sup> Those barriers seem correct, regardless of the constitutional precepts they rest upon. That is, the degree to which a police officer ought to be able to make particularized judgments about a person will depend on the degree to which the police officer's suspicions are warranted. In other words, police may not arbitrarily access personal information in the first place, and the mere fact that they may access some information does not underwrite their accessing all information available from all state sources.

So, for example, the fact that Pierre makes multiple furtive exchanges with a variety of passersby in an area known for drug trafficking might arouse enough suspicion in police officer Quinn to justify Quinn's detaining Pierre and asking him questions, but more would be required for Quinn to pat Pierre down for weapons. He might be warranted in asking Pierre for identification, and using Pierre's identification to search for outstanding arrest warrants.<sup>58</sup> However, that level of suspicion and contact with police by itself ought not allow Quinn to access *any* sort of record that the state keeps on Pierre. The state is likely to have income tax, employment assistance, social service, educational, property, driving, birth, family, and marriage records, and certainly Quinn's having access to such records could be useful in some circumstances—for instance, finding tax delinquents. However, actually making those records available to any police officer in routine interactions would require a fairly powerful justification. That is, while Pierre may not have a claim to privacy about his name, whether there are weapons in his pockets, and his record of outstanding arrest warrants with respect to Quinn, he does have claims to privacy with respect to Quinn about his school record, his visits to a public hospital, his income tax returns, his military record, his social security payments, the nonweapon items in his pockets, and so

---

54. See *Terry v. Ohio*, 392 U.S. 1, 21 (1968); see also *Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177 (2004); *Brown v. Texas*, 443 U.S. 47 (1979).

55. *Terry*, 392 U.S. at 28–29.

56. *Hiibel*, 542 U.S. at 185 (citing *INS v. Delgado*, 466 U.S. 210, 216 (1984)).

57. See *Brown*, 443 U.S. at 52.

58. Even these are controversial. The point, though, is that there is some level of suspicion that would warrant such impingements of privacy, but no more. That level of suspicion is all I am trying to pick out in this example.



forth. To allow Quinn access to that information absent some substantial justification would be arbitrary.

Such limitations are not limited to police access to records. Rather, people have privacy claims about any information collected by a state agency with respect to other agencies. Consider how things would look if there were no limitations on the information shared across agencies. To take one example, educational institutions would have unfettered access to records about income, finances, employment, involvement with the court system, driving records, property, and so forth. Similarly, departments of revenue would have unfettered access to educational and medical records, court records, and travel records (for example, customs records, electronic road toll records, et cetera). Sometimes, there are very good reasons for one agency to have access to information kept by other agencies. Criminal investigators may have good reason to access tax records, and the substantial overlap between health and human services agencies and education administrations may provide a reason for them to share information. But this underscores the primary point. People have claims to privacy about information held by state agencies with respect to other state agencies, and access across agencies demands a justification.

The third difference between state and commercial actors speaks to the underlying explanation of privacy claims. First, one is more likely to see one's projects or relationships as public goods due to state information gathering than as a result of commercial information gathering, both because of the reach and role of the state. And second, failures to respect persons seem particularly acute when executed by state actors.

To reiterate, people have claims to privacy with respect to the state. In many cases they provide consent, via democratic processes, to state agencies collecting and analyzing information. However, that consent does not imply that any state agency should be able to access any information collected by any other state agency, though people may use those same democratic processes to explicitly consent to such sharing. Rather, information sharing across agencies requires its own explicit consent or some other justification for overriding persons' privacy claims. This situation is different than the case of commercial data brokerages that may use the information they collect with implicit consent for their own even arbitrary purposes, so long as those purposes do not violate some other claim, for example, a use to which one could not reasonably consent.

#### D. Generalizing Claims to Privacy

At the start of this part, I articulated several general principles to help determine whether *P* has a claim to privacy about *O* with respect to *Q*. In Parts V.A to V.C, I outlined a number of cases to help illustrate the ways in which *P* will have different claims to privacy based on different *Q*s. With those cases in mind, some generalizations about claims to privacy based on constitutive value can be made. First, *P* is more likely to have a claim to privacy about *O* with respect to *Q* where *P*'s privacy has decreased substantially with respect to *Q*. This falls out of the Pete and Jeff example in Part V.A. Where Jeff zealously collects information about Pete, Jeff impinges a claim. Moreover, it may be the case that many particular instances of Jeff's information collection would impinge no claim and diminish nothing of value (for instance, noting Pete's habit of arriving to work at a particular time) in isolation, but those same actions do seem to impinge a claim against the background of Jeff's pervasive information gathering. That is, there seems to be some kind of threshold at work. This holds true across different sorts of *Q*s. Consider police actions. For the most part, *P* has no claim to privacy over his actions in a public place with respect to police officers who happen to be nearby. However, if the police pay particular attention to *P*—following, watching, filming, and so forth—the attention impinges a claim.<sup>59</sup> Note that this criticism differs from *P*'s claim against arbitrary state action. Where the police have legitimate reason to follow *P*, but that reason only warrants a modicum of information gathering, substantial information gathering impinges a privacy claim. But the existence of legitimate reasons means that the information gathering is not arbitrary.

It does not follow, however, that *P* has a claim to privacy beyond a certain threshold. In fact, there is no limit on the degree to which *P*'s privacy can decrease, so long as those decreases are accompanied by adequate consent. Consider the commercial data broker cases. If *P* gives implicit consent for *Q*, a data broker, to collect and analyze his data, and gives further, explicit consent to having that information shared, and other information collected, then *P* will have no claims to privacy even where the amount of information, and the degree of particularity of judgment underwritten, becomes enormous.

This leads to the next generalization. Consent to privacy decreases can be inferred from the nature of the process by which information is gathered. Taking advantage of institutions that depend for their existence on information collection and analysis implies that one consents to the

---

59. To be clear, impinging a claim does not mean that it is, all things considered, improper. Rather, it just means that the action demands an adequate justification.

degree of information collection and analysis necessary for that institution to exist. One cannot infer consent to uses for which one would never reasonably give consent—as when a broker amasses information that can be used for discriminatory purposes. That would be a failure of respect for the person to whom the information pertains.<sup>60</sup>

We can also make some generalizations concerning the sorts of information that are more likely to be the subject of a privacy claim, as described in Part III and at the beginning of this part. *P* is more likely to have a claim to privacy about *O* with respect to *Q* where *O* is a particularly meaning-conferring good and diminishing privacy detracts from *O*'s ability to confer meaning. Similarly, *P* will have a claim to privacy about *O* with respect to *Q* where *O* plays an important role in *P*'s shaping her personality and actions, and where *P*'s loss of privacy about *O* with respect to *Q* would lead *P* to alter *O*. And *P* will have a claim to privacy about *O* with respect to *Q* where *O* is an object that plays a central feature in shaping *P*'s life, and in which *P* has a reasonable concern for and a reasonable expectation of privacy with respect to *Q*.

Finally, we may make some generalizations about the nature of the information gatherer. I suggested that the likelihood of privacy loss with respect to state actors and individuals is more likely to implicate the constitutive values on which the distributed value account relies; we are more likely to have claims to privacy with respect to those actors. Further, because state actors ought to act with justification (unlike nonstate actors),

---

60. There are important remaining issues here. The institution of consumer credit requires a certain amount of information collection and sharing to function; however, it requires much more information sharing to function effectively, still more to function effectively and cheaply, and yet still more to function effectively, cheaply, and exceedingly profitably. The degree to which consumers consent to information sharing by using some form of consumer credit is unclear. Note that if selling information makes credit or consumer goods cheaper to the benefit of consumers, it does not follow that people consent to those sales. After all, it might make clothing cheaper if stores sold videotapes of people trying the clothing on, but it does not follow that anyone purchasing the clothing for the lower price consents to such a sale.

Michael Fromkin argues that because aggregation of data adds value for the data broker, the marginal value of any bit of information is less than the average aggregate value of all information available to data brokers, and consumers will therefore not bargain to maintain privacy. Perhaps more persuasively, he argues that consumers are generally unaware of the extent to which their information is aggregated and analyzed, and therefore do not avoid information-revealing transactions or bargain for privacy protections. A. Michael Fromkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1502–05 (2000).

we will have greater claims against information amalgamation with respect to state actors.

## VI. CONCLUSION

My task in this paper has been to provide an account of privacy's value, and how such value might give rise to claims to privacy. I argued that privacy's value is not unary, but distributed, such that whether privacy has value will depend upon particular aspects of the three-part relation involved. At its strongest, privacy is valuable as a constitutive part of states of affairs that are valuable in themselves. Often, however, privacy is morally neutral, or weakly instrumentally valuable. Because of this, determining where persons have claims to privacy is problematic. While I cannot offer an algorithm for assessing claims to privacy, I outlined a number of plausible generalizations.

If I am correct about the distributed nature of privacy's value, and if some of the generalizations I have made are accurate, there remains a great deal to be said about what those generalizations mean for how information ought to be managed. Two current issues illustrate this point. The first concerns surreptitious information gathering. If we have claims to privacy regarding certain information with respect to, for example, the state, does that give rise to claims that we know, or have the opportunity to know, of that loss? I think it does, largely because we have claims to information important in ordering our lives.<sup>61</sup> Second, the boundaries I have drawn around generalizations are exceedingly vague. State actors often rely upon nonstate data brokerages to compile information, such that the *Q* in a privacy relation is far from clear.<sup>62</sup> Similarly, whether information implicates meaning-conferring goods, one's ability to act as an autonomous chooser of one's life, or one's ability to have a personality of one's making will vary widely. Nonetheless, I think that being clear about privacy's tripartite structure, viewing privacy's value as distributed rather than unary, and thinking of claims to privacy as being a function of particular features of privacy relationships is the right mechanism by which to analyze the more complex problems out there.

---

61. See Rubel, *supra* note 31, at 151–54.

62. See Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 636 (2004); U.S. GOV'T ACCOUNTABILITY OFFICE, PERSONAL INFORMATION: AGENCY AND RESELLER ADHERENCE TO KEY PRIVACY PRINCIPLES 4–7 (2006), available at <http://www.gao.gov/new.items/d06421.pdf>.