Res Publica (2021) 27:287–302
https://doi.org/10.1007/s11158-020-09473-1

Too Much Info: Data Surveillance and Reasons to Favor the Control Account of the Right to Privacy

Jakob Thrane Mainz[1] · **Rasmus Uhrenfeldt**[1]

Published online: 16 July 2020

Abstract
In this paper, we argue that there is at least a pro tanto reason to favor the control account of the right to privacy over the access account of the right to privacy. This conclusion is of interest due to its relevance for contemporary discussions related to surveillance policies. We discuss several ways in which the two accounts of the right to privacy can be improved significantly by making minor adjustments to their respective definitions. We then test the improved versions of the two accounts on a test case, to see which account best explains the violation that occurs in the case. The test turns out in favor of the control account.

Keywords Privacy rights · Surveillance · Ethics of surveillance · Control account · Access account

Introduction

This paper is about the right to privacy. We offer a range of specific suggestions as to how the two most popular accounts of the right to privacy can be improved, by adjusting their respective definitions slightly. The first account is the Control Account (CA), and the second is the Access Account (AA).[1] We will call the proponents of these accounts 'control theorists', and 'access theorists' respectively. After

[1] The CA, broadly conceived, has been developed by Warren and Brandeis (1890), Westin (1970), Fried (1968), Moore (2003, 2010), Gross (1971), Parker (1974), Parent (1983), Allen (2003), Rössler (2005), Bezanson (1992), Goldberg et al. (2001), Altman (1976), Ryan and Calo (2010), Margulis (1977), Miller (1971), Scanlon (1975), Inness (1992), and many more. The AA, broadly conceived, has been developed by Thomson (1975), Gavison (1980), Bok (1989), Allen (1988), van den Haag (1971), Macnish (2018), and others. Note that some theorists have contributed to both.

✉ Jakob Thrane Mainz
jtm@hum.aau.dk

Rasmus Uhrenfeldt
ru@hum.aau.dk

[1] Aalborg University, Kroghstræde 3, 9220 Aalborg, Denmark

having improved the accounts, we test them on a thought example to see which account best explains the violation in the example. This reveals a pro tanto reason to favor the CA over the AA.

There are both *descriptive* and *normative* versions of both accounts. Descriptive accounts explain the necessary and/or sufficient conditions for *having* or *losing* privacy. The normative accounts explain the necessary and/or sufficient conditions for *violations* of the moral *right* to privacy (whatever that is) to occur.[2] A descriptive account is, as Adam Moore suggests, an account that describes *a state* or *condition* of privacy while normative accounts refer to moral obligations and rights (Moore 2008, pp. 212–213). Imagine that an individual invites strangers to observe her while she is at home. This individual is now in a lessened *state of privacy*, but since she herself invited the observers, her right to privacy has not been violated.

In this paper, we focus on the normative accounts, unless specified otherwise.[3] According to the control theorists, control is a crucial feature of the right to privacy. If, and only if, I lose control over access to the relevant information,[4] is my right to privacy violated. The access theorists, on the other hand, argue that a loss of control of the access to the information in question is not sufficient for a violation of the right to privacy to occur. They argue that the information in question must also in fact be accessed, in order for the right to privacy to be violated.

When we say that a person has a right to privacy, we do not subscribe to any particular theory of what it means to have a right to something. All our arguments are compatible with all of the most common theories of rights. For example, according to the interest theory of rights, the function of a person's right to privacy is that having such a right furthers her interests. According to the will theory of rights, on the other hand, the function of a person's right to privacy is to give that person control over the duties of other persons with regards to her privacy. Since nothing in our arguments hangs on which account of rights is the correct one, we will remain agnostic about this. However, we will assume—uncontroversially—that a right to privacy is a waivable, non-absolute right.

Why does it matter whether the control or the access account of the right to privacy is the correct one? As the access theorist Kevin Macnish has recently pointed out, it matters a great deal for our normative evaluations of many cases related to surveillance. For example, it matters for our evaluation of the case of the National Security Agency (NSA) collecting significant amounts of personal data about American citizens, and our evaluation of Edward Snowden's revelations of this practice (Macnish 2018, p. 2). It seems that if the CA is correct, millions of citizens' right to privacy is violated when the NSA collects data about them. This is so, because the citizens lose control over the access to information about them. If, on the other hand, the AA is correct, then it seems that citizens' right to privacy has not been violated

[2] We write 'moral right' to distinguish it from a legal right.

[3] It is frustratingly difficult to determine which accounts are meant to be descriptive, which are meant to be normative, and which are both. Among the theorists we discuss in this paper, we count Adam Moore's account as a normative CA, and Judith Jarvis Thomson's and Kevin Macnish's accounts as normative AAs.

[4] In this paper, we focus on *informational* privacy, although many have argued persuasively that privacy also concerns other things like spaces or bodies (See e.g. Moore 2010, pp. 25–26).

by this practice. The right to privacy has been violated on the AA only if persons at the NSA (or others) actually access the information (ibid.). So, this is not only an interesting theoretical discussion about definitions. It potentially has very important and wide-reaching implications for national security policy and surveillance policy.

The paper is structured as follows. In 'The Control Account of the Right to Privacy' section, we provide an initial definition of the CA. In 'The Access Account of the Right to Privacy' section, we provide an initial definition of the AA. In 'Improving the CA and the AA' section, we present and discuss several ways in which the definitions of the two accounts can be improved. We then provide a test case, to see which account, in its improved version, best explains the violation in the test case. Finally, in 'Concluding Remarks' section we make a few concluding remarks.

The Control Account of the Right to Privacy

Let us now consider a definition of the CA. There is no universal consensus among the control theorists about how exactly the CA should be defined. The key idea is, though, that a loss of control over access to the relevant information is necessary and sufficient for privacy violations to occur. The definition we will provide in this section is meant to capture what most control theorists would subscribe to. In the following section, we will then try to improve this initial definition on the control theorists' behalf. The initial definition which seems to catch the crux of what most control theorists have in mind is this:

> **CA**1: For any agent A to have her right to privacy violated, there is a necessary and sufficient condition that must be satisfied: Agent A has involuntarily lost control over unwanted access to personal information P about agent A.[5]

We do not suggest that all control theorists use the exact wording of CA1.[6] But we do think that any control theorist needs to accept that losing control over access to personal information is a necessary and sufficient condition for a violation of the right to privacy to occur. Otherwise, such a theorist does not count as a (normative) control theorist.

Moore is an example of a recent and prominent control theorist. According to Moore, '*A right to privacy is a right to control access to and uses of—places, bodies, and personal information*' (Moore 2010, p. 27). As this quote indicates, Moore thinks that privacy is not exclusively concerned with *informational* privacy. His definition also covers 'locational privacy' and 'physical privacy', and it not only covers

[5] Some control theorists do not include the access-part. See Schoeman (1984, pp. 2–3).

[6] Despite the fact that it is very difficult to determine which control theorists think of their respective accounts as normative accounts, we think it is fair to say that the CA1 can at least be distilled from the accounts of Allen (1999), Parker (1974), and Moore (2008), but probably many more. Allen, for example, writes: '"privacy" means personal data control or rights of data control; that the right of privacy is a right of personal data control; and that enhancing personal data control by individuals is the optimal end of privacy regulation' (p. 875).

control rights, but also *use*-rights. Nonetheless, Moore seems to endorse the CA1 when it comes to informational privacy.

To illustrate that, for Moore, a loss of control over access is a *sufficient* condition for a violation of the right to privacy to occur, he provides two cases:

> **Zone Intrusion**: Suppose you look in my safe with your X-ray device to see what it holds—there could be a stolen photo, a borrowed photo, or nothing….
> **Mere Zone Intrusion**: Just like the first zone intrusion case although the person looking has no short-term memory and will forget any fact learned immediately.
> In the case of zone intrusion a right to control access has been violated even though nothing except a bare fact has been seized. This is further illustrated by the example of mere zone intrusion. In the second case, nothing has been taken—no facts have been learned—all that has happened is that a zone or boundary has been unjustifiably crossed. (Moore 2003, p. 423)[7]

In Mere Zone Intrusion, Moore thinks that a violation of the right to privacy has occurred, because control over access to information has been lost.[8] The loss of control over access is thus sufficient for the violation of the right to privacy to occur.

To illustrate that, for Moore, a loss of control over access is also a *necessary* condition, consider the following case:

> **The Loud Fight**: Suppose that Fred and Ginger are having a fight - shouting at each other with the windows open so that anyone on the street can hear. (Moore 2003, p. 421)[9]

Moore thinks that no violation of the right to privacy has occurred in The Loud Fight:

> In the loud fight case it would seem that Fred and Ginger have waived the right to privacy - they have via their actions allowed others who are in a public space to hear the fight. (Moore 2003, p. 421)

In The Loud Fight, information has been accessed by the people on the street, but no violation of the right to privacy has occurred, according to Moore. Fred and Ginger still have control over the people on the street's access to the information, because Fred and Ginger could simply choose to close the windows. Moore thus thinks that a loss of control of the access is a necessary condition for the violation of the right to privacy to occur. Similar quotes can be found in the works of other control theorists, but we will let Moore serve as a canonical example.

[7] Moore borrows the Zone Intrusion case from Thomson (1975, p. 298).

[8] One might argue that information has indeed been accessed, although the person forgets the information immediately. That might be so, but it seems that this is not what drives Moore's intuition that a violation has occurred. What drives his intuition seems to be that control over access has been lost.

[9] Moore borrows The Loud Fight case from Thomson (1975, p. 296).

The Access Account of the Right to Privacy

Let us now turn to the AA. The key motivator for the access theorists seems to be that the CA is too broad, since it, counterintuitively, allows for violations of the right to privacy in cases where control has been lost, but no actual access to information has occurred (Thomson 1975, p. 305). The access theorists therefore add the extra necessary condition that the information in question must actually be accessed, in order for a violation of the right to privacy to occur. The definition we will provide in this section is meant to capture what most access theorists would subscribe to. In the following section, we will then try to improve this initial definition on the access theorists' behalf. The initial definition which seems to catch the crux of what most access theorists to have in mind is this:

> **AA**1: For any agent A to have her right to privacy violated there are two each necessary and jointly sufficient conditions that must be satisfied: (1) Agent A has involuntarily lost control over unwanted access to personal information P about A, and (2) agent B (or someone else) actually accesses P.

Understood this way, the AA adds a necessary condition to the CA, namely the condition (2). We do not suggest that all access theorists use the exact wording of AA1. But we do think that any access theorist needs to accept that losing control over access to personal information—in conjunction with actual access to this information—are each necessary and jointly sufficient conditions for a violation of the right to privacy to occur.[10] Otherwise, such a theorist does not count as an (normative) access theorist.

Kevin Macnish has put it this way: '*In contrast to the control account, the access account holds that information needs to be accessed for there to be an actual violation of privacy*' (Macnish 2018, p. 4). Macnish is an example of an access theorist who defends the view that access is a necessary condition for a violation of the right to privacy to occur.[11] In order to demonstrate this point, Macnish provides the following example:

> … imagine that I leave my diary on a table in a coffee shop and return to that shop 30 min later to retrieve it. When I enter the shop I see a stranger with my diary on her table, a different table from the one at which I was sitting. I therefore know that she, or someone, has moved my diary, but have they read it? I have not been in control of my diary for half-an-hour, in which time anything might have happened to it. (Macnish 2018, p. 4)

[10] This means that access and control accounts overlap in some cases. This is so because the AA *adds* a necessary condition to the CA.

[11] It is very difficult to determine which access theorists think of their respective accounts as normative accounts, but according to the access theorist Macnish the position that access is necessary for a violation of the right to privacy to occur is held by Allen (1988), Bok (1989), Gavison (1980), Gross (1971), Thomson (1975), and van den Haag (1971). The AA1 can at least be distilled from the accounts of these theorists.

In this diary case, there is definitely a loss of control over access to the information in the diary. But, according to Macnish, no violation of the right to privacy has occurred. In order for a violation to occur, someone must open the diary and read it. If no one does so, no violation has occurred:

> Imagine that I have returned to the coffee shop after a 30 min interval to find my diary on the table. It is unopened. I panic for a moment, but on seeing me the stranger smiles and hands me the book. She explains that she has not opened it, but saw me leave without it and collected it to await my return. She knows how intimate her own diary is, so she respected my privacy and kept it shut, as well as making sure that no one else would be able to read it. I feel an enormous sense of relief, thank her and leave with my dignity intact. In this case, I do not think that my privacy has been lessened. When I see my diary in another's possession, I fear that my privacy has been violated, and indeed it might have been. However, as long as the diary is not actually opened and read no reduction in privacy has occurred. Note that this is true even though the diary was not under my control for 30 min. (Macnish 2018, pp. 4–5)

Note that Macnish writes that privacy has been neither 'lessened', 'violated', nor 'reduced' in this quote. We interpret this to mean that Macnish thinks that the diary example applies to *both* the descriptive *and* the normative AA. So, in relation to the normative AA, Macnish seems to think that, in addition to a loss of control over access, the information in question must be accessed in order for a violation of the right to privacy to occur. Similar quotes can be found in the works of other access theorists, but we will let Macnish serve as a canonical example.

It is important to stress that on the AA, there must be an *actual* access, and not just an *ability* to access, in order for there to be a violation of the right to privacy. Alan Rubel has suggested the following rough summarization of the descriptive version of AA: 'Privacy has to do with others' actual access, or *ability* to access, a person' (Rubel 2011, p. 296 [our emphasis]). In relation to the *normative* version of the AA, it seems that access must be interpreted solely as *actual* access, and not the *ability* to access. The reason is that the latter seems to be similar to a lack of *control* on the claimant's side, which will collapse the AA into something close to the CA. If Jones has the *ability* to access information about Smith, but chooses not to make use of it, then in some way, Smith does not have *control* over the access. Jones's ability to access is a sufficient condition for Smith not having control over the access. Conversely, Smith not having control over the access is a necessary condition for Jones having the ability to access the information. In order to distinguish their position sufficiently from the CA, the access theorists therefore need to include only *actual* access in their definition.[12]

[12] By 'actual access', the access theorists seem to mean something like 'actual *epistemic* access'. A person must have formed an epistemic relation to the information in question in order for actual access to obtain.

Improving the CA and the AA

Given that the only thing that distinguishes the two accounts is an extra necessary condition in the AA, it is not surprising that much of the criticism that applies to one of the accounts, also applies to the other. This will be evident throughout this section, when we address new issues, some of which apply to both accounts, and suggest ways to accommodate these issues by making adjustments to the definitions. The first issue we will discuss concerns the meaning of the word 'control'.

Positive Control Versus Negative Control

The word 'control' seems to mean different things to different people in the privacy literature. The plausibility of the CA and the AA depends to a significant extent on which interpretation of control is at play. Let us introduce a distinction between 'Positive Control', 'Negative Control':[13] and 'Republican Control':[14]

> **Positive Control**: Agent A enjoys Positive Control over the access to relevant information P, if, and only if, A tries (or could try) to give agent B actual access to P, and succeeds.
> **Negative Control**: Agent A enjoys Negative Control over access to relevant information P, if, and only if, A is capable of preventing agent B, who attempts to access, from accessing P.
> **Republican Control**: Agent A enjoys Republican Control if, and only if, agent B does not have the ability to get access to relevant information P about A.[15]

Only the distinction between Positive Control and Negative Control is of relevance for this section. Later, we will explain how the distinction between Negative Control and Republican Control offers an effective rejoinder to Judith Jarvis Thomson's famous objection against the Control Account, and against Macnish's diary case introduced in the previous section.

Let us first make a point about the definition of Negative Control. It is tempting to think that the definition of Negative Control implies that any loss of Negative Control results in an access of information, since a loss of Negative Control always comes with an attempt to access. This would make it difficult to conceptually separate the CA from the AA. However, as we shall see in 'A Test Case' section, there are cases in which the lack of access is due to contingent circumstances, and in such

[13] The distinction between Positive Control and Negative Control is inspired by Isaiah Berlin's famous distinction between 'positive liberty' and 'negative liberty' (Berlin 1969, pp. 121–122). However, there is a crucial difference: negative liberty has a contrafactual definition, while Negative Control does not.

[14] This is inspired by Philip Pettit's idea of 'republican freedom'. See Pettit (1999).

[15] We are not the first ones to consider the combination of republicanism and privacy. See, for example, Newell (2018), Roberts (2014), van der Sloot (2018), and Hoye and Monaghan (2015). However, all of these authors write about how privacy is important for retaining republican freedom. Our idea is different. We interpret control in a republican manner in order to improve the control account, so that it can escape certain objections.

cases, Negative Control over certain information can be lost, while no access to that information occurs.

Let us now try to explain why the distinction between Positive Control and Negative Control is important. Our claim is that *if* the control account should be taken seriously, it must explain all violations of the right to privacy in terms of Negative Control, and only Negative Control. A loss of Positive Control cannot plausibly violate the right to privacy. To see why, consider the following example:

> **Too Much Info #1**
> Suppose that Smith and Jones are co-workers. Smith likes to share personal information about his sex life. One day, as Smith is about to tell Jones something personal again, Jones simply puts his fingers in his ears before Smith starts talking. Smith finishes his story anyway.

If control is interpreted as Positive Control, Jones has violated Smith's right to privacy by putting his fingers in his ears, since Smith then loses Positive Control over the access to the information. But clearly, it would be absurd to maintain that a violation of the right to privacy has occurred in Too Much Info #1.[16] Nonetheless, the interpretation of control as Positive Control can be found in the works of prominent privacy scholars, although they have not used the term 'Positive Control'. Take for example Jeffrey Reiman's use of the term in his influential critique of the control theorist Charles Fried: '*… in our culture one does not have control over who gets to observe one's performance of the excretory functions, since it is generally prohibited to execute them in public*' (Reiman 1995, p. 30).[17] Here, it seems, Reiman's interprets control as Positive Control. Reiman's point is that if person A wants person B to have access to person A's performance of the excretory functions, but person A does not succeed, then person A lacks a relevant form of control. Contrast this form of control with the one in Moore's 'Zone Intrusion' and 'Mere Zone Intrusion' in 'The Control Account of the Right to Privacy' section. In Moore's cases, control seems to be interpreted as Negative Control.

In order to avoid the strange implication of Too Much Info #1, and thus avoiding an accusation of the CA being too broad, the control theorist might want to specify that control should be interpreted as Negative Control, and only Negative Control. So, a revised definition of the CA could look like:

> **CA2**: For any agent A to have her right to privacy violated, there is a necessary and sufficient condition that must be satisfied: Agent A has involuntarily lost *negative* control over unwanted access to personal information P about agent A.

On CA2, no violation occurs in Too Much Info #1, since no one has lost Negative Control. Note that Too Much Info #1 is not a problematic counterexample for

[16] Joel Feinberg has argued that in a case like this, Smith has actually violated Jones's right to privacy by divulging private information unto Jones (Ferinberg 1985, p. 23). As Feinberg would probably agree, this hinges on an interpretation of privacy, which conflates privacy with liberty or autonomy.

[17] For another example, see Farber (1993, p. 515).

the access theorist, since Jones does not get access. However, we can make a slight alteration of Too Much Info #1, so that Jones does in fact get access. Call this example Too Much Info #2:

> **Too Much Info #2**
> The same as Too Much Info #1, but this time Peter has been standing in the same room as Smith and Jones without anyone noticing. After Smith has left the room, Peter tells Jones what Smith was trying to tell.

If control is interpreted as Positive Control, there is a violation in Too Much Info #2 on the AA1. This is so, because Smith does not have Positive Control over whether Jones has access, and Jones does in fact access the information. But it seems very implausible that Jones has violated Smith's right to privacy in Too Much Info #2. It seems more plausible that *Peter* violates at least Smith's right to privacy, due to Peter's eavesdropping. This violation can be explained as a loss of Negative Control on Smith's part. In order to rule out Positive Control, we suggest the same adjustment to the definition of the AA, as we did to the definition of the CA:

> **AA**2: For any agent A to have her right to privacy violated there are two each necessary and jointly sufficient conditions that must be satisfied: (1) Agent A has involuntarily lost *Negative* Control over unwanted access to personal information P about A, and (2) agent B has access to P.

Note that A does not need to lose *all* of her Negative Control over P in order for her right to privacy to be a violation. A can have full Negative Control with regards to some agents, while having lost Negative control with regards to others. To see this point, consider Futuria.

> **Futuria**
> In Futuria each person at the age of 20 is forced by law to let one of 50 private companies have access to certain very personal information. Sarah has just turned 20 and therefore needs to choose which of these companies she wants to give her information to. She actively dislikes 48 of the companies and therefore uses her Negative Control to withhold her information from these companies. She is agnostic about giving her information to the remaining two companies, so she chooses one at random.

In Futuria, it seems that Sarah enjoys a substantial degree of control, but her right to privacy is still violated. The reason is that Sarah does not have control with regards to *all* of the companies. We cannot point to any of these companies and say 'Sarah was coerced to give information to this particular company'. However, what matters is if Sarah is in control over whether *any* agent has access to information about her.[18]

[18] Note that this implies that many modern democratic states are constantly engaged in infringing on privacy rights, when relevant state authorities gain access to personal finances, medical records, etc. People may have differing intuitions in this case. Our intuition is that such states do in fact infringe on people's right to privacy, but that doing so can be justifiable on weightier non-privacy related grounds.

Wanted Versus Unwanted Access

Both control theorists and access theorists have claimed that privacy is concerned with *unwanted* access. In fact, no one in the literature seems to dispute this. Consider this quote from the control theorist Beate Rössler:

> Something counts as private, if one can oneself control the access to this 'something'. Conversely, the protection of privacy means protection against unwanted access by other people. (Rössler 2005, p. 8)

Or, this quote from the access theorist Sissela Bok: 'The condition of being protected from unwanted access by others—either physical access, personal information, or attention' (Bok 1989, pp. 10–11).

The notion of 'unwanted' can be spelled out in at least two different ways: (1) Either as a description of some actual or possible psychological state, such as the *absence* of a desire, ambition, unconscious or conscious wish (or an *active* disfavoring of this psychological state), or (2) as a more abstract normative concept, which is supposed to do some normative work on its own.

Let us first explain why it is not conceivable to understand unwanted as (2). On (2), unwanted is supposed to do some normative work on its own, and presumably refer to the importance of being able to exclude someone from having access. But on that interpretation, it is a bit unclear what normative work it does that is relevantly different from what the control theorists mean by (negative) 'control'; If Smith has full control over the access, and Jones has access, it must at least be the case that Jones's access is not unwanted by Smith. So, we assume that unwanted should be understood as (1) or something close to it.

If we understand unwanted as (1), then there are cases in which an intrusion is *wanted* by the claimant, and yet there is a violation of the right to privacy. Consider Apology:

> **Apology**
> Person A has hurt the feelings of person C. Person A is truly regretful and wishes to give C a heartfelt apology. A is very nervous about giving the apology to C, and therefore, before giving the apology, A tells a close friend, B, how A wants to apologize to C. Unbeknownst to A, C eavesdrops on their conversation out of vengeance, in the hope of gaining knowledge of A's personal information so she can tell others about it. C tells A that she has heard the apology, and A is truly relieved that she no longer has to deliver the apology face-to-face to C.

In this thought experiment, it seems that the intrusion is indeed wanted, since person A, had she been asked beforehand, would have wished that C would eavesdrop. But, C still clearly violates A's (and possibly B's) right to privacy. If this is correct, it demonstrates that it cannot be a necessary condition that the access is *unwanted* by the claimant, in order for a privacy violation to occur. For that reason, both control theorists and access theorists must accept that there are cases where the right to privacy is violated by an access that is, at least to some extent,

wanted by the claimant.[19] In order to recognize this, the control theorist and the access theorists could simply exclude 'unwanted' from their respective accounts. The definitions would then read:

> **CA**3: For any agent A to have her right to privacy violated, there is a necessary and sufficient condition that must be satisfied: Agent A has involuntarily lost Negative Control over the access to personal information P about agent A.
> **AA**3: For any agent A to have her right to privacy violated there are two each necessary and jointly sufficient conditions that must be satisfied: (1) Agent A has involuntarily lost Negative Control over the access to personal information P about A, and (2) agent B actually accesses P.

Before turning to the test case, let us first discuss the issue of who, or what, can cause a loss of control of the kind that is relevant for a violation of the right to privacy to occur.

The Loss of Control

Kevin Macnish has recently argued that the descriptive AA is preferable to the descriptive CA. He writes:

> I argue that the control account does not capture significant aspects of what is meant by privacy, demonstrating that privacy and control can come apart. Hence control is neither necessary nor sufficient for privacy. By contrast, privacy and access do not come apart. As such, I hold that the access account is preferable to the control account. (Macnish 2018, p. 1)

However, as we saw in Macnish's diary case in 'The Control Account of the Right to Privacy' section, he also talks of *violations*. He claims that there is no violation in the diary example, even though there is a loss of control. Thus, he seems to prefer the normative AA over the normative CA.[20]

The diary case demonstrates that control cannot be a necessary and sufficient condition for a privacy violation, since control is lost in that example while no violation has occurred. We agree that no violation occurs in the diary case. However, we will argue that this is not due to a lack of access. Rather, it is due to the fact that the loss of control is the claimant's own fault, since he forgot the diary on the table. To see this more clearly, consider another example: you are walking outside in a storm with your diary in your bag. Unfortunately, you forgot to zip the bag completely, so

[19] Thanks to Beate Rössler for pointing out the following to us: what is wanted by A in Apology is not the intrusion itself, but to give C the apology. But then let us change the example so that A wants C to intrude, because then A would feel that they were even, and that A no longer had to feel bad about what she did to C. Or, change it so that A has voyeuristic tendencies and likes to be watched or listened to by others. In these cases, A's right to privacy would be violated (a right is not automatically waived just because the claimant likes that others occasionally violates the right), and yet the intrusion would be wanted.

[20] If Macnish did not intend this to be a discussion of privacy *rights*, he should have made that more explicit, and probably abstained from using the word 'violation'.

the wind blows your diary out of the bag. It lands on the sidewalk with the pages facing up. Another pedestrian is kind enough to pick it up for you, but as he does so, he cannot avoid reading some of the content. In this case, there is clearly no violation, even though someone gets access to information in the diary, while there is a loss of control. This shows that the lack of access itself does not explain the lack of violation in Macnish's diary example. What explains the lack of violation, is the fact that the loss of control is not due to the action(s) of another agent, of which that agent is responsible.[21]

Adam Moore has an example which can be used to demonstrate that the loss of control must be due to the action(s) of another agent in order for a violation of the right to privacy to occur.[22] Moore's example is this:

> **The Accidentally Amplified Quiet Fight**: A married couple, X and Y, are having another quiet fight behind closed doors. But this time an unanticipated gust of wind sweeps through the house, knocking down the front door, carrying and amplifying the couple's voices so that Stuart, who is washing his car in his driveway across the street, hears at least some of what X and Y have been saying.
> In the accidentally amplified quiet fight case the right to privacy is not waived and it also appears not to be violated. (Moore 2003, p. 423)

Although X and Y have lost control over the access to the information, and the information has indeed been accessed, no violation of the right to privacy has occurred, according to Moore. The loss of control, and Stuart's access to the information, is merely due to an accident, and for that reason, no violation has occurred. And, since no violation would have occurred if X and Y had given Stuart access voluntarily, it seems that the access must be due to the action(s) of another agent in order for a violation to occur. This is of interest for at least two reasons: (1) given how much work the diary example does for Macnish, it is problematic for him if it turns out that it is not the absence of access that explains the absence of a violation, and (2) it suggests a new adjustment of both definitions. The adjustment consists in adding that the loss of control must be due to the action(s) of another agent, of which that agent is responsible. The definitions then read:

> **CA**4: For any agent A to have her right to privacy violated, there is a necessary and sufficient condition that must be satisfied: Agent A has involuntarily lost Negative Control over the access to personal information P about agent A, *due to action(s) of agent B, of which B is responsible*.
> **AA**4: For any agent A to have her right to privacy violated there are two each necessary and jointly sufficient conditions that must be satisfied: (1) Agent A has involuntarily lost Negative Control over the access to personal information

[21] This does not mean that no violations will occur downstream. For example, publicizing the forgotten diary on the Internet would still constitute a violation. See Moore (2018) for a discussion on issues of forfeiting and waiving rights.

[22] Moore gets this example from Rickless (2007).

P about A, *due to the action(s) of agent B, of which B is responsible,* and (2) agent B (or someone else) actually accesses P.

A Test Case

Let us now consider a test case to see which of the improved accounts best explains the violations that occurs in this case. Call the test case Wiretapping:

Wiretapping
Smith and Jones are neighbors. Unbeknownst to Jones, Smith wiretaps Jones's telephone, using a fancy device which allows Smith to listen in on Jones's conversations without violating Jones's property rights. As it happens, Jones is on vacation for several months, and therefore does not use the telephone in that time period.

Our intuition is that Smith clearly violates Jones's right to privacy in Wiretapping. But which account best explains this violation? Let us first consider the improved version of the CA. According to CA4, it is a necessary and sufficient condition that Smith has lost negative control over the access to information, and that this loss of control was due to the action(s) of another agent, of which that agent is responsible. This seems satisfied in Wiretapping. Jones has lost negative control over the access, since Smith can now listen to Jones's telephone conversations. And, this loss of control was due to action(s) of Jones, for which Jones was responsible, since he was the one who chose to wiretap Smith's phone.

What about the AA? According to AA4, it is a necessary condition that Smith *actually accesses* Jones's information. But in Wiretapping, it seems that Smith does *not* access information about Jones, since Jones does not use the telephone. It could be argued that Smith does in fact access some information about Jones, namely the information that Jones did not use the particular telephone in that particular period. We grant that Smith has access to this information. But we find it hard to see that the access to *that* information alone is what drives the strong intuition that Jones's right to privacy is violated by Smith. Even if the wiretap had randomly malfunctioned unbeknownst to Smith, so Smith did not get access to the information that Jones did not use the telephone, Smith would clearly still have violated Jones's right to privacy. This counts against the AA, since it is too narrow to account for the violation in Wiretapping.

Wiretapping shows that, pace the access theorists' arguments, access is not a necessary condition for a violation of the right to privacy. Moreover, since there would be no violation if Jones had voluntarily given Smith access, it cannot be a sufficient condition either. This is a genuine problem for the access theorists, and a problem that we do not see how they can escape by simply adjusting the definition of the AA.

The access theorist might object that we are stacking the deck of cards in favor of the CA. After all, since there is no actual access in Wiretapping, it is not surprising that the AA cannot account for the violation. Our response to this objection is that none of the examples or thought experiments provided by the access theorists in the literature so far seem to count decisively in favor of the AA, like Wiretapping

counts decisively in favor of the CA. We cannot think of an example, which stacks the deck of cards in favor of the AA, so we invite the access theorists to provide such an example. A possible candidate for such an example is Judith Jarvis Thomson's seminal X-ray case:

> If my neighbor invents an X-ray device which enables him to look through walls, then I should imagine I thereby lose control over who can look at me: going home and closing the doors no longer suffices to prevent others from doing so. But my right to privacy is not violated until my neighbor actually does train the device on the wall of my house. (Thomson 1975, p. 304)

Thomson points out that your right to privacy has not been violated just because you no longer have control over whether your neighbor looks through your wall or not. It would only be violated, when the neighbor *actually*[23] trains the X-ray device on the wall (Thomson 1975, p. 305). Access theorists often turn to the X-ray case in order to show why the AA is preferable to the CA. We will show that the improved version of the CA can easily handle the X-ray case.

Let us first compare Wiretapping to the X-ray case. We agree that there is no violation in the X-ray case, unless the neighbor actually trains the X-ray on the wall. It might seem, prima facie, that on the CA4, there is a violation in the X-ray case, since control is lost due to the neighbor's actions (the invention of the X-ray device). But recall that the relevant form of control on the CA4 is Negative Control. In order for Negative Control to be lost, someone must *attempt* to get access, and in Thomson's case, the neighbor does *not* attempt to get access. To see clearly how this is an effective rejoinder to Thomson, let us return to the distinction between Negative Control and Republican Control which we introduced in an earlier section.

Republican Control is lost simply by virtue of someone else having the ability to access your information. They do not need to use this ability.[24] In Thomson's case, Republican Control is lost when the neighbor invents the X-ray device, but Negative Control is not lost. In Wiretapping, on the other hand, someone tries to get access, so Negative Control is lost. Thus, Thomson's attempt to make a reductio on the CA does not cut any ice against CA4.[25] Note also that Macnish's diary example does cut any ice against the CA4 either, since the loss of control in this example is also a loss of Republican Control, not a loss of Negative Control.

It seems that when we compare the improved versions of the two accounts, we have at least a pro tanto reason to prefer the CA over the AA. Only the CA can explain the violation in Wiretapping. This does not mean, however, that the CA is

[23] Note that this counts in favor of our earlier point that the access must be *actual* access, not only the *ability* to access.

[24] In 'The Access Account of the Right to Privacy' section, we argued that if the access in the AA is the *ability* to access, it would collapse into a *type* of CA. The type of CA it would collapse into is a republican CA.

[25] The distinction between Negative Control and Republican Control saves the control theorists from several objections in which the access theorists seem to think that a loss of Republican Control must be a violation on the CA. This shows the importance of specifying that the CA should only be concerned with losses of Negative Control.

preferable to the AA, all things considered. It might be that there are other problems with either of these accounts, which need to be accounted for, and that doing so reveals that in fact the AA comes out on top.

Concluding Remarks

In this paper, we have offered several ways in which both the control account and the access account of the right to privacy can be improved. We then tested the improved versions of the accounts to see which of them best explains the violation in Wiretapping. It turned out that the CA could explain the violation, while the AA could not. This gives us a pro tanto reason to favor the CA over the AA.

In the introduction, we claimed, following Kevin Macnish, that the discussion about which account of the right to privacy is the correct one is of tremendous importance for our normative evaluations of state surveillance. For example, when discussing the potential wrongdoing associated with the NSA's collection of data about people, and the Edward Snowden's subsequent whistleblowing, a lot hangs on whether the CA or the AA is correct. Macnish argued that if the CA is correct, then the NSA is violating citizens' right to privacy, but if the AA is correct, there is no such violation. This remains true with the adjustments we have suggested for the two definitions. On the CA4, the NSA's violation consists in a loss of negative control, by undermining people's ability to prevent the NSA (and others) from getting actual access to the information. When the information is stored in the NSA's database, the NSA has definitively undermined people's ability to control the access to the information, even if no employee of the NSA (or others) ever looks at the information. On the AA4, no violation occurs until an employee actually looks at the information.

What we have argued in this paper does not resolve the dispute between the control theorists and the access theorists decisively. But, if we are correct, then there is a pro tanto reason for saying that many instances of surveillance do in fact constitute violations of the right to privacy, even when the information in question is not actually accessed. As with any pro tanto reason, this one may be overruled by other reasons.

References

Allen, Anita. 1988. *Uneasy Access: Privacy for Women in a Free Society*. Lanham, MD: Rowman & Littlefield Publishers.

Allen, Anita. 1999. Coercing Privacy. *William and Mary Law Review* 40(3): 723–757.

Allen, Anita. 2003. *Why Privacy isn't Everything: Feminist Reflections of Personal Accountability*. Lanham, MD: Rowman & Littlefield Publishers.

Altman, Irwin. 1976. Privacy: A Conceptual Analysis. *Environment and Behavior* 8(1): 141.

Berlin, Isaiah. 1969. *Two Concepts of Liberty*. Oxford: Clarendon Press.

Bezanson, Randall P. 1992. The Right to Privacy Revisited: Privacy, News, and Social Change, 1890–1990. *Northwestern University* 80(5): 1133–1175.

Bok, Sissela. 1989. *Secrets: On the Ethics of Concealment and Revelation*. New York: Vintage Books.

Farber, Daniel A. 1993. Book Review: Privacy, Intimacy, and Isolation by Julie C. Inness. *Constitutional Commentary* 10: 510–519.
Feinberg, Joel. 1985. *Offence to Others*. Oxford: Oxford University Press.
Fried, Charles. 1968. Privacy. *Yale Law Journal* 77(3): 475–493.
Gavison, Ruth. 1980. Privacy and the Limits of Law. *Yale Law Journal Article* 89(3): 421–471.
Goldberg, Ian, Austin Hill, and Adam Shostack. 2001. Trust, Ethics and Privacy. *Boston University Law Review* 81(2): 407–422.
Gross, Hyman. 1971. Privacy and Autonomy. In *Nomos XIII: Privacy*, pp. 169–181.
Hoye, Matthew, and Jeffrey Monaghan. 2015. Surveillance, Freedom and the Republic. *European Journal of Political Theory* 17(3): 343–363.
Inness, Julie C. 1992. *Privacy, Intimacy, and Isolation*. Oxford: Oxford University Press.
Macnish, Kevin. 2018. Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. *Journal of Applied Philosophy* 35(2): 417–432.
Margulis, Stephen T. 1977. Conceptions of Privacy: Current Status and Next Steps. *Journal of Social Issues* 33(3): 5–21.
Miller, Arthur R. 1971. *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: University of Michigan Press.
Moore, Adam D. 2003. Privacy: Its Meaning and Value. *American Philosophical Quarterly* 40(3): 215–227.
Moore, Adam. 2008. Defining Privacy. *Journal of Social Philosophy* 39(3): 411–428. https://doi.org/10.1111/j.1467-9833.2008.00433.x.
Moore, Adam D. 2010. *Privacy Rights: Moral and Legal Foundations*. University Park: Pennsylvania State University Press.
Moore, Adam D. 2018. Privacy, Interests, and Inalienable Rights. *Moral Philosophy and Politics* 5(2): 327–355.
Newell, Bryce Clayton. 2018. Privacy as Antipower. In Pursuit of Non-Domination (Foreword). *European Data Protection Law Review* 4(1): 12–16.
Parent, W. A. 1983. Privacy, Morality, and the Law. *Philosophy and Public Affairs* 12: 269–288.
Parker, Richard. 1974. A Definition of Privacy. *Rutgers Law Review* 27: 275–296.
Pettit, Philip. 1999. *Republicanism: A Theory of Freedom and Government*. Oxford: Oxford University Press.
Reiman, Jeffrey H. 1995. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. In *Privacy*, ed. Eric Barendt, 159–176. Dartmouth: Ashgate.
Rickless, C. Samuel. 2007. The Right to Privacy Unveiled. *San Diego Law Review* 44(4): 809–846.
Roberts, A. 2014. A Republican Account of the Value of Privacy. *European Journal of Political Theory.* 14(3): 320–344.
Rössler, Beate. 2005. *The Value of Privacy*. Cambridge: Polity Press.
Rubel, Alan. 2011. The Particularized Judgment Account of Privacy. *Res Publica* 17(3): 275–290.
Ryan, M., and M. R. Calo. 2010. The Boundaries of Privacy Harm. *Indiana Law Journal* 86: 1131.
Scanlon, Thomas. 1975. Thomson on Privacy. *Philosophy and Public Affairs* 4(4): 315–322.
Schoeman, Ferdinand. 1984. *Philosophical Dimensions of Privacy*. Cambridge: Cambridge University Press.
Thomson, Judith Jarvis. 1975. The Right to Privacy. *Philosophy & Public Affairs* 4(4): 295–314.
van den Haag, Ernst. 1971. On Privacy. In *Privacy: Nomos XIII*, pp. 149–168.
van der Sloot, B. 2018. A New Approach to the Right to Privacy or How the European Court of Human Rights Embraced the Non-domination Principle. *Computer Law and Security Review* 34(3): 539–549.
Warren, Samuel D., and Louis D. Brandeis. 1890. Right to Privacy. *Harvard Law Review* 4(5): 193–220.
Westin, Alan F. 1970. *Privacy and Freedom*. London: Bodley Head.