AI and Ethics
https://doi.org/10.1007/s43681-023-00270-z

ORIGINAL RESEARCH

Convergence of the source control and actual access accounts of privacy

Haleh Asgarinia[1]

Received: 1 October 2022 / Accepted: 20 February 2023

Abstract
In this paper, it is argued that, when properly revised in the face of counter-examples, the source control and actual access views of privacy are extensionally equivalent but different in their underlying rationales. In this sense, the source control view and the actual access view, when properly modified to meet counter-examples, can be metaphorically compared to 'climbing the same mountain but from different sides' (as Parfit [1] has argued about normative theories). These two views can equally apply to the privacy debates and, thus, resolve a long-standing debate in the literature.

Keywords Access account of privacy · Control account of privacy · Descriptive aspect of privacy · The convergence of the access and control views

1 Introduction

Privacy has been defined through several theories in the philosophical literature; for example, it has been described as the right to be alone [2], a Wittgensteinian approach of family resemblance [3], control over information [4], and limited access to information [5]. Among these competing definitions, two views figure prominently: 'access' and 'control', which I find the most convincing. The access account of privacy holds that privacy is a function of the extent to which people can access a person or information about him or her (as held by, e.g. Reiman [6]). The control account of privacy holds that privacy is about the control one has over access to oneself (as held by, e.g. Roessler [7] and Westin [8]). This paper does not aim to define privacy, whether as a redundant (or single concept) or as a pluralist concept [9], but rather to contribute to one aspect of the debate, focusing on the two most popular accounts—control and access—and provide new insight into them.

Those who define privacy as a matter of control argue that a loss of control over one's information constitutes a loss of privacy. However, those who define privacy as a matter of access argue that a loss of privacy only occurs when one's information is accessed. These earlier, classical approaches to privacy did not clarify the meaning of control and the requirement for obtaining access in their theories. Recently, however, two privacy scholars have done so. Menges [10, 11], who defends the source control account of privacy, argues that privacy loss occurs when agent A loses the *source control* over his/her personal information flow. Concurrently, Macnish [12, 13], who defends the actual access account of privacy, argues that privacy loss occurs when another agent B *actually accesses* personal information about agent A. In this paper, I focus on Menges' and Macnish's theories, as these accounts go beyond the existing descriptions of the control and access accounts, and argue that losing a new version of control—that is, source control—and understanding of that which is accessed—that is, actual access—are required for a loss of privacy, respectively. Moreover, although some hold that privacy includes non-informational aspects [14]—such as bodily privacy or behavioural privacy—here, I focus on information privacy because both the actual access and source control accounts of privacy are related to this aspect.

Throughout this paper, I refer to a loss or diminution of privacy. I use this deliberately non-pejorative terminology to avoid being side-tracked into the question of when privacy may be waived, invaded or violated, or whether the loss of privacy leads to the violation or sustenance of a right to privacy. I do not discuss a right to privacy or whether a loss of privacy is morally wrong, which would call for a

✉ Haleh Asgarinia
h.asgarinia@utwente.nl

[1] Department of Philosophy, University of Twente, Drienerlolaan 5, 7522DB Enschede, Netherlands

Published online: 07 March 2023

different paper. My aim is to provide an answer to the question of which accounts of privacy capture significant aspects of what the term means: source control or actual access. My answer is that neither account is preferable; both are extensionally equivalent.

It is important to note that focusing on the descriptive conception of privacy does not rule out the possibility of normative accounts; rather, searching for a philosophical definition of privacy can help make sense of normative debates that arise within moral or legal traditions. As Gavison rightly notes, the value of privacy can only be determined after a discussion of what privacy is and when—and why—losses of privacy are morally or legally wrong [5, p. 452]. Accordingly, the importance of concentrating on a descriptive conception of privacy can be defended by stating that it enables us to build a layer on top of it using criteria to determine how much privacy is good or required [5, 15]. As such, the degree to which the descriptive conception can be articulated is critical. As a contribution to recent debates concerning the descriptive conception of privacy, this paper specifies what a loss of privacy consists of, regardless of its legal or moral significance.

The paper is structured as follows. In Sect. 2, I provide an initial definition of the source control account of privacy developed by Menges [10, 11]. In Sect. 3, I discuss the problem with this account and present an alternative way to revise it in light of potential problems. Similarly, in Sect. 4, I provide an initial definition of the actual access account of privacy developed by Macnish [12, 13]. In Sect. 5, I then discuss the problem of the actual account of privacy and present another way to revise it in light of potential problems. In Sect. 6, I provide *paradigmatic cases* that address whole comparable scenarios to see which revised versions explain the loss of privacy in the test cases. As I argue, both versions can explain the loss of privacy in the test cases. Hence, I show that the two alternatives actually converge on the same view—on an extensionally equivalent account. Finally, in Sect. 7, I suggest a *theoretical argument* to show that the two accounts of privacy from Sect. 6 are extensionally equivalent. I conclude that source control and actual access accounts of privacy can equally apply to the privacy debates and, thus, resolve a long-standing debate in the philosophy of privacy.

2 Menges' account of privacy: privacy as source control

Menges [10, 11] argues in favour of the control account of privacy by developing a new way to understand the relevant kind of control. In doing so, he relies on the distinction between two different kinds of control [16]. One is understood as the ability to do otherwise, which Menges calls leeway control, and the other is understood as having a desire or intention[1] to act in a certain way, which he calls source control. I explain leeway and source control through detailed examples in the following paragraphs. Menges contends that privacy should be analysed in terms of source control, which provides a novel view for conceptualising privacy. This new account of control implies that an agent A's privacy is not diminished when exercising source control, even when A does not maintain leeway control. This differs from that of traditional accounts of control—being able to effectively choose *whether or not* something happens—emphasising the importance of leeway control for privacy. The conclusion is, then, that as long as A maintains source control over his/her personal information, s/he has privacy, despite losing leeway control [11, pp. 34–35]. To understand Menges's view, I now turn to the underlining principles as Frankfurt originally used them in arguing for moral responsibility.

Frankfurt cases (see Frankfurt [16]) aim to show that agent A can be responsible for what s/he does because s/he can have the control which is necessary to be responsible for an action even if s/he cannot do otherwise. The main idea associated with Frankfurt cases is that the factors that explain why an agent A acts as s/he does differ from the factors that explain why A cannot act otherwise. By themselves, the latter factors do not undermine the agent's responsibility. For instance, other agents, devices, or any other external factors make it the case that A cannot effectively choose whether an event or action happens. In contrast, features of A themselves, namely their beliefs, desires, and intentions, explain why A is responsible for an action. The idea is that we do not need the ability to do otherwise to be responsible for our actions. Rather, what we need is to be the right kind of source of our actions [11]. The following case clearly shows the distinction between different kinds of control.

Jones resolves to shoot Smith. Black has learned of Jones's plan and wants Jones to shoot Smith. Black would prefer that Jones shoot Smith on his own; however, concerned that Jones might waver in his resolve to shoot Smith, Black secretly makes arrangements such that, if Jones shows any sign at all that he will not shoot Smith (something Black has the resources to detect), Black will be able to manipulate Jones so that he shoots Smith. As things transpire, Jones follows through with his plans and shoots Smith for his own reasons. No one else in any way threatened or coerced Jones, offered Jones a bribe, or even suggested that he shoot Smith. Jones shot Smith of his own accord, and Black never intervened [17, Sect. 3.2].

[1] It should be noted that I use the terms 'desire' and 'intention' in a technical sense. My view applies regardless of the specific propositional attitude or mental state that is relevant to a choice.

Jones lacks leeway control because Black can coerce him into shooting Smith. That is, Black would make Jones shoots Smith even if he decides not to. Nonetheless, we still hold Jones responsible because he exercises source control over what he does when he shoots Smith, although he does not have an effective choice over whether he does it. He wants to do it, and it happens without any intervention, while he cannot do otherwise because of Black. Concurrently, if Jones did not have the desire to shoot Smith, Black would have made him do so regardless. In this case, Jones would lose source control if his action had not been related to his desire. Thus, we can have an important kind of control over what we do, although it is not possible for us to do other than desiring to do certain things—in this case, shooting Smith [11].

Just as Frankfurt cases regarding moral responsibility distinguish between leeway and source control over actions, Menges distinguishes between leeway and source control over information. In this manner, Menges applies the distinction between leeway control and source control, which are typically discussed in non-informational contexts, to informational contexts. He contends that source control, not leeway control, is the kind that relates to privacy. The nature of privacy, according to the source control account, is being the right kind of source of information flows, if information flows at all. Being the right kind of source of information means that A has source control over information. Being the source control over information requires that, if the pieces of information flow to another person, this is the result of A's desire that it do so and A's desire that s/he desires to let it flow in this way [10, 11]. The following case clarifies this discussion.

Case 1: 'Imagine that I leave my diary on a table in a coffee shop and return to that shop 30 minutes 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? Imagine that the stranger has not yet read it but wants to know what my last entry says. She has firmly decided to read it before 3 pm and she would read it even in my presence (imagine that she is very strong and I would not be able to prevent her from reading it). I come back at 2.55 pm and tell her: "It's terrible, I'm forgetting everything these days! I hope I'm not getting ill. Actually, I wrote about it in my diary this morning. Please, look at the last pages". In response to this, the stranger reads my last entry in the diary'. [11, pp. 35–36]

In this case, I lost leeway control because I lost an effective choice of whether the stranger learns or has access to certain information. I cannot do anything to stop her from accessing or learning the information. Nonetheless, an alternative to the leeway control account, namely the source control account, says that I have source control because I have the desire to give the stranger some information about myself. Accordingly, I still have privacy because the flow of information is grounded on my desire; I am thus the right kind of source of information flow. The stranger would diminish my privacy if she learned about the last entry, even though my desires opposed this flow of information [11].

The above discussions indicate that the key idea is that a loss of source control over personal information flow is necessary and sufficient for a loss of privacy to occur. Given that a descriptive definition of privacy aims to specify what a loss of privacy consists of [15], the *initial* definition of the source control account of privacy is as follows:

Definition 1 A's privacy is lost iff: a has lost source control over the personal information P about agent A, if information flows at all.

For Menges, a loss of source control over information flows is a *sufficient* condition for a loss of privacy to occur. Consider the following case:

Case 2: Imagine that 'you are walking outside in a storm with your diary in your bag. Unfortunately, you forgot to zip the bag completely, so the wind blows your diary out of the bag. It lands on the sidewalk with the pages facing up. Another pedestrian … picks it up for you, but as he does so, he reads some of the content'.[2] [18, pp. 297–298]

In this case, as the flow of information is *not* grounded in what I desire; I am not the right kind of source for the information flow, and my privacy is thereby diminished. Menges thinks that a loss of privacy has occurred because source control over information flows has been lost. That is, if source control is lost or diminished, then privacy will be lost or diminished. The loss of source control over the information flow is, thus, sufficient for the loss of privacy to occur.

For Menges, a loss of source control over information flows is also a *necessary* condition for privacy loss. Menges argues that, in Case 1, I have privacy because I am the right

[2] One might argue that this case shows more than merely a loss of source control, as the pedestrian has actual access to the information, as well. According to Menges's view, 'privacy essentially consists in being the right kind of source of information flow to another agent if the information flows at all. … The information does not flow to another agent as long as nobody actually accesses the data and learns something about the relevant citizens. … The source control is diminished as soon as an agent accesses the data before the relevant citizen tells them about it' [11, 45–46]. In this case, if I freely and knowingly had asked the pedestrian—'who has not read my diary and does not plan to read it'—to read my diary, my privacy would not have been diminished, as no diminution of source control has occurred [11, 39]. The source control view only says that accessing information is relevant for privacy only if and because it diminishes being the right kind of source of an information flow. Thus, Menges says that accessing information is relevant for diminishing privacy and that the most important thing about privacy is having source control.

kind of source for the information flow. This is equivalent to saying that if privacy is diminished or lost, then the source control will be lost or diminished. The loss of source control over the information flow is, thus, necessary for the loss of privacy to occur.

3 Revising the source control account of privacy

Menges [10, 11] applies the split-level theory of control used in the discussion about moral responsibility to privacy. He then distinguishes between leeway and source control over information and emphasises A's desire in determining whether privacy loss has occurred. I posit that Menges has situations like Case 3 in mind when he theorises about the source control of privacy:

Case 3: 'Imagine Annabel. … She suffers from a rare and very hard-to-diagnose genetic disorder, a piece of information about herself she wishes to keep private. One day, Annabel agrees to take part in a new medical initiative. The primary purpose of the initiative is to' [4, 19] find various factors related to a different, more prevalent disease. As a participant in the initiative, Annabel donates her DNA intentionally to medical science. Suppose that Brian is a researcher trained in genetic medicine and works on medical research. He infers from Annabel's DNA profile that she has a specific gene on chromosome 6, which is related to Type 1 diabetes.

In this case, Menges would argue that no privacy losses occurred because Annabel is the right source of control over the information flow. I agree with Menges that no loss of privacy occurs in Case 3 because Annabel has a desire to share her information with Brian, and Brian infers information that Annabel has no desire to keep private.

In each case Menges (see [10, 11]) discusses, he only focuses on information-sharing without taking into account what will happen when the shared information is analysed or processed. Accordingly, Menges considers the *origin* of the information flow to be important in determining whether a loss of privacy has occurred. As Menges emphasises, once the flow of a piece of information is grounded on the desire of agent A, whose information is shared with another agent(s) B, no privacy loss occurs (see the voluntary divulgence cases, [10]). The focus on the origin of the information flow, I believe, implies that, according to Menges, A can be the right kind of source for the flow of information inferred from an initial piece of information only if A is the right kind of source for the flow of that initial information. Thus, the flow of information which results from an intentional action by A does not lead to a loss of privacy, regardless of any information that may be inferred from it. I argue, however, that this feature of Menges's theory—that it is indifferent to potential inferences—gives rise to a counter-example. Consider the following:

Case 4: This case is identical to Case 3 (Annabel donates her DNA for research purposes), with the only difference being that Brian infers from Annabel's DNA profile that she suffers from her rare genetic disorder.

For Menges, if A is the right source of control over P, then their privacy is not lost. Concentrating merely on the origin of the information flow, as Menges does, implies that information P^* inferred from other information P can never be privacy-diminishing if P is not. Hence, it might be argued that, in Case 4, Annabel has a desire to share her information P with Brian, so inferring P^* from that information does not lead to her loss of privacy in Menges's view. However, I note that, if P^* follows from P in some sense, then P^* should be privacy-diminishing under some circumstances; this is a property that I think must be clarified in Menges's view. In Case 4, Annabel has a desire to share her information with Brian for the defined purpose, but she does not have a desire to share some potential information inferred from her information which does not comply with the initial purpose. Hence, Annabel's privacy is, in my view, essentially lost.

It might be argued that if Annabel does not want this information (P^*) to be shared, then her privacy is diminished in Menges's view. She has lost source control. I agree that her privacy is lost, but the reason for that cannot be grounded on Menges's view because Menges merely argues for having an initial desire to share information with others and does not discuss a person's desire to infer information from that shared information. I argue that Annabel's privacy has been lost because information that Annabel does not desire Brian to have ultimately flows to him. The desire related to the information inferred is not clarified in Menges's view.

As mentioned in previous paragraphs, the problem with Menges's view is that the propositional content of the relevant information-releasing desire does not include the content of the inference. Therefore, the initial version of the source control view of privacy is wrong about Case 4 because Annabel's privacy is diminished, although she has an intention to share her information, and the origin of the information was grounded on her desire. Hence, *Case 4* is a *counter-example* for the initial version of the source account of privacy. That gives me good reason to revise the initial version so that Annabel's privacy has, in fact, been lost in Case 4.

Comparing cases 3 and 4 illustrates that the initial account of source control of privacy can be revised by answering the question of what makes something the 'right' source information flow. Although Menges uses desire as the standard example of how to conceptualise his view, he also notes that he remains open to what exactly constitutes source control [11, p. 37]. If the desire or intention makes it the right flow, then is s/he the right source flow for that

piece of information if A intends to keep P* private? How can one distinguish between cases in which B infers information from intentionally shared information that A intends to keep private (Case 4) and those of that A does not intend to keep private (Case 3)? In other words, it is important to determine what constitutes the relevant inferences that do not lead to a loss of privacy. A's intention determines how a piece of information flows to another agent. That is, if the flow of information changes, then A is no longer the right source of the novel flow of information. Thus, to identify whether drawing inferences (P*) from intentionally shared information (P) affects whether one is the right source of information, I focus on the flow of information, as any changes in the flow determine whether one is the right source of the information flow. I think a piece of information flows between different parties in a system to realise a specific purpose. Thus, a person whose data are processed and an agent who processes that data for a specific purpose play an important role in determining the flow of information. Thus, *who* engages in a system and their *purpose* for doing so determine the flow of information. It follows that any changes in these elements, which characterise the flow of information, will alter whether one is the right source control over the information.

As Case 3 illustrates, Annabel wants to know whether she suffers from a prevalent disease and desires to share her information with a medical research lab. Let us imagine that she should share her data with one of five institutes, some of which are public health bodies, and some of which are industry organisations. Annabel has a desire to share her data with a medical research lab. However, she has no desire to share her data with a 'big pharma' company. In this case, although Annabel should share her data and has no ability to do otherwise (i.e. preventing one institute from accessing her information), she still has privacy because she is the right source control over her information. It is important to note that, to avoid second-order conflicts, I assume that sharing data with a medical research lab does not imply sharing it with a big pharma company. Otherwise, I would have concluded that not only does she not want (first-order desire) to share her data with a big pharma company, but she might not have a second-order desire to share her data with a medical research lab because doing so implies sharing data with a big pharma company. Thus, Annabel's desire determines *who* asks her question, and she does not allow the big pharma company to answer her question. Thus, the source control account of privacy does not have any problem with the first element that characterises the flow of information.

I now turn to the second element, namely the primary *purpose*, determining the flow of information. Annabel knowingly submits her DNA sample to the research lab to find the answer to her specific question. What matters, though, is that these data contain a significant amount of information beyond her specific question. Consequently, the researcher can infer more from that information beyond what Annabel specifically asked the lab to investigate (see Case 4). In such a case, the researcher (here, Brian) can not only look for the prevalent disease Annabel asked them to identify, but they can also study whether she suffers from a rare genetic disorder. That is the kind of excessive (unintended) information derived without any reason to do so. I consider this a loss of privacy even though Annabel initially had the desire to disclose her original data. Therefore, I argue, the initial purpose for which a researcher should carry out their task identifies whether the inferences derived from the information lead to a loss of privacy. Any information derived beyond the question diminishes Annabel's privacy, as it diminishes being the right source control of information.

It is important to note that I do not claim that Annabel has the idea of the full knowledge that can be derived from her data. Moreover, I agree that the researcher may not necessarily know a priori what specific information the research requires. However, I note Annabel and Brian can only agree on the very limited purposes and limited inferences. Any other (excessive) inferences that might be drawn from that information lead to a loss of privacy. I believe that the problem with the source control account of privacy is, thus, related to the second element, namely the primary purpose.

So far, I have discussed the important elements that determine the information flow. Any changes in the elements result in a novel flow of information. If the flow of information is not grounded on A's intention (or desire), then A's privacy is lost. As discussed above, processing data or accessing information in a manner that is incompatible with the initial purpose for which data were collected alters personal information flows. Regarding the fact that agent A's desire[3] or intention, whether reasonable or unreasonable, prescribes the flow of information, any changes in the flow of information lead to a diminution of being the right source control over the flow of information. This suggests an adjustment to Menges's definition. The adjustment consists of adding that the loss of being the right source of information flow must be due to the action(s) of another agent who obtains or deduces information intended to be private. My revised definition is as follows:

Definition 2 A's privacy is lost iff: a has lost source control over the personal information P about agent A, if

[3] I believe that, in cases in which A has an unreasonable epistemic desire, their privacy is diminished, but it is not necessarily wrong. Consider A, who shares her blood sample with B for the purpose of identifying her blood type. If B uses A's information to make inferences that A is HIV positive, then A's privacy is diminished. In this case, A has an unreasonable desire that her disease will not be revealed through sharing her information with B.

information flows at all, *due to the action(s) of agent B, who obtains or infers information contrary to A's preferences*.

As I have already discussed, Case 4 is a counter-example of the initial source control account of privacy, as Menges argues that Annabel's privacy has not diminished in this case. However, my revised version of this view is correct for Case 4 because it states that Annabel's privacy has, in fact, been lost. According to the revised account of privacy, in Case 4, Annabel is not the right source control because Brian changes the flow of information by changing the initial purpose and inferring excessive (unintended) information from Annabel's data. The initial purpose was to identify various factors related to a prevalent disease, while Brian changes this purpose and acquires excessive information related to her genetic disorder. Thus, the initial purpose, which should be realised in accordance with A's (reasonable or unreasonable epistemic) desire, is the key element in identifying whether the inferences scientists make change the information flow.

4 Macnish's account of privacy: privacy as actual access

Macnish [12, 13] defends the access account of privacy against the control account. The access account holds that, for a diminution of privacy to occur, the personal information must be actually accessed. Furthermore, the information accessed must be understood by the agent accessing it. The traditional access view is then supplemented by a semantic account that describes an agent's capacity to understand the information. Accordingly, if another agent B accesses personal information P about agent A without understanding its meaning, then A's informational privacy is not diminished. Macnish concludes that privacy diminution has occurred when the information is actually accessed by those who can understand it [13, 17].

The access account of privacy holds that a loss of privacy occurs when a stranger reads my diary. For example, in Case 2, my privacy is diminished because another agent reads my diary and discovers information about me. Furthermore, this account of privacy holds that personal information which is intentionally shared with those who understand its meaning leads to a loss of privacy. A reduction in my privacy has occurred when I show someone a personal letter or invite them into my house [12]. Consider Case 1, in which I freely and knowingly ask the stranger to read the last entry of my diary. In response, the stranger reads it. According to the access account, my privacy is diminished when the stranger reads my diary in response to my valid consent for him/her to read the latest entry. Similarly, this view implies that we lose our privacy when we freely and knowingly tell our friends about our problems and secrets. According to this view, our privacy is diminished whenever someone else accesses personal information about us, regardless of whether we intend to share our personal information with another agent.

The discussions above indicate that the key idea, which is that the information in question must actually[4] be accessed, is a necessary and sufficient condition for a loss of privacy. Given that a descriptive definition of privacy aims to specify what a loss of privacy consists of [15], the *initial* definition of the access account of privacy is the following:

Definition 3 A's privacy is lost iff: B *actually accesses* personal information P about A.

For Macnish, the fact that B actually accesses personal information P about A is a *sufficient* condition for a loss of A's privacy to occur. Macnish thinks that a loss of privacy has occurred because agent B had actual access to P and learned something new about A (see Cases 2 and 1). The actual access by another agent is, thus, sufficient for the loss of A's privacy to occur.

Moreover, for Macnish, the fact that B actually accesses personal information P about A is a *necessary* condition for a loss of A's privacy to occur. He cites the following case:

Case 5: 'Imagine that I have returned to the coffee shop after a 30 minute 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'. [12, p. 420]

According to Macnish [12], my privacy has not been lessened because the diary was not actually opened and read. The actual access by another agent to personal information is, thus necessary for A to lose his/her privacy.

[4] The use of the word 'actual' is deliberate and clarifies that the privacy account discussed in this section is the access account developed by Macnish. The purpose of using this term is to emphasise that, to argue that actual access has occurred, it is necessary to understand what is accessed.

5 Revising the actual access account of privacy

Macnish [12, 13] contends that gaining access to A's personal information—for example, through a diary—leads to a reduction of privacy. I argue that a set of personal information consists of two different subsets of information: information about A that A intends to keep private and information about A that A intends to transmit or share with other agents. According to Macnish's view, when a stranger accesses the personal information I transmit, my privacy will be diminished (see Case 1). Moreover, as Macnish stresses, accessing personal information that A intends to keep private results in a diminution of privacy (see Case 6). Therefore, in Macnish's view, accessing both subsets of information leads to a loss of privacy.

Case 6: 'Imagine that Eustace keeps a private diary. Eustace talks publicly about this diary, freely describing what it looks like but not about its contents, which he holds to be private. One day Frances is in Eustace's office and sees the diary, recognising it from the description. She opens the diary and finds that she *can* read it. She reads through the diary and finds out that Eustace has been visiting George a lot recently. She does not realise it from the description, but Eustace and George are having a covert relationship. In this case, Eustace's privacy has been diminished (Frances knows something about Eustace he would rather have been kept private). However, Eustace's privacy has not been diminished as much as if Frances had been able to infer that he was in a relationship with George'. [13, 15, 16]

In this case, Macnish [13] argues that Eustace's privacy has been lost because Frances had actual access to the information P about Eustace, which Eustace attempted to keep private. I agree with Macnish that accessing information that A intends to keep private leads to a loss of privacy.

I believe, however, that my privacy will not be diminished, as I intentionally shared my information with the stranger (Case 1); 'I am including another within my realm or privacy, not lessening my privacy' [4, p. 46]. According to the actual access view, however, a diminution of privacy occurs even if an agent intentionally shares their personal information; instead, I contend that only accessing information P about A that A intends to keep private results in a loss of privacy. Nevertheless, accessing information that was once private but that A now intendedly[5] shares with other agents does not lead to a loss of privacy. Thus, Case 1 is the *counter-example* for the initial version of the actual access account of privacy because this view incorrectly interprets Case 1.[6] This gives me good reason to revise the initial version of the actual access view.

I think the initial version can be revised by making a distinction between once-private, now intentionally shared information and information kept in private. I then suggest excluding the subset of the once-private, now intentionally shared information from the set of private information. In this way, the scope of the actual access account of privacy is narrowed and only covers personal information which A intends to keep private. Accordingly, if an agent B understands the meaning of information about agent A, and A has intentionally shared it, then no privacy loss has occurred, because B has actual access to the information which was once private and is now intentionally transmitted, instead of accessing (intentionally) private information.

This suggests a new adjustment of the initial definition of the access account of privacy. The adjustment consists of adding that the actual access must occur when agent B accesses personal information P about agent A, which A attempts or intends to keep private. It is important to note that a set of personal information that A intends to keep private is a subset of personal information. This is the difference between definition 3 and definition 4 below. Hence, the problem is not related to learning something new about another person, but rather, understanding the information which A intends to keep private. My revised version is as follows:

Definition 4 A's privacy is lost iff: B actually accesses personal information P about A, *and A intends that P remain private*.

As I have already discussed, Case 1 is a counter-example for the initial version of the actual account of privacy, since Macnish argues that my privacy will be diminished if the stranger accesses my diary. However, my revised version of this view correctly interprets Case 1 by positing that my privacy will not be diminished in this case. According to the revised account, in Case 1, the stranger accesses

[5] I assume that the person has privacy-preserving intentions to share some privacy-sensitive information with others. In cases where the person has non-privacy preserving intentions, there would be a reduction in their privacy.

[6] One plausible interpretation of Case 1 is that 'my privacy is (voluntarily) diminished, but it is not important or morally wrong'. Proponents of such an interpretation might see privacy as being entirely neutral. I do not take that view, as I see privacy as prima facie good, although the discussion of its normative aspect goes beyond the scope of this paper. I only claim that accessing once-private, now intentionally shared information is not a diminishment of privacy. I have a prima facia reason to object to any action that diminishes my privacy. However, I remain impartial on whether privacy diminishment is a necessary, sufficient, or criterial condition for a right violation. I solely emphasise that privacy depreciation is part of the analysis of whether the right to privacy is violated or infringed upon.

once-private, now intentionally shared information, which does not lead to a loss of privacy.

So far, I have claimed that a loss of privacy occurs when agent B accesses personal information P about agent A, which A intends to keep P private, while no privacy loss occurs when B actually accesses P as long as P is intentionally shared. The question that may arise is how B realises that the piece of information accessed is private, or was once private and is now intentionally revealed. In responding to this concern, two different kinds of cases can be separated: first, cases in which B *knows* that the piece of information accessed is private and that A intends to keep it private; and second, cases in which B *does not know* either whether the piece of information accessed is private *or* whether A intended to share it or A was unaware that a piece of information could be accessed by B [19].

In cases where agent B knows that the piece of information accessed is private and A intends to keep it private, accessing P, and even any inferences from P, diminish A's privacy. For example, in Case 6, Eustace intends to keep the information private that she is in a covert relationship with George, and she has never talked about her relationship with Frances. Thus, Frances actually accesses personal information about Eustace, which she intends to keep private, and, consequently, Eustace's privacy has been lost.

In cases where an agent B does not know that the piece of information accessed is private *or* whether it is a piece of private information inferred from P which A intended to share, or even that A was unaware that this piece of information could be accessed by B, two different responses can be considered. First, if B is unsure whether some is private or was once private and accesses it, this leads to a reduction in A's privacy [19]. This response restricts any access to once-private information. In contrast, there might be P which A intended to share with B. This response prohibits all intentional analyses of once-private information. Second, B refrains from accessing information that they have *reason* to think was private and which A would have wanted to keep private (ibid). In this way, A's privacy depends on what B could reasonably have expected A's concerns were with regard to the piece of information now accessed.

In the case of Annabel, Case 3, Brian might reasonably expect that Annabel wanted him to understand the fact that her DNA profile illustrates a specific gene structure related to a prevalent disease—simply because the information discovered does not deviate from the initial purpose for which the data were collected. Thus, Brian has reason to think that the piece of information accessed through analysis and inference is not information that Annabel wants to keep private. Accordingly, accessing this kind of information does not constitute Annabel's loss of privacy.

According to the above discussion, I claim that Annabel's privacy in Case 3 is not lost because Brian has reason to think that the information accessed is not the kind of information that Annabel wanted to keep private. However, the initial version of the actual access account, definition 3, argues that Annabel's privacy has been lost because Brian accessed private information about Annabel. Therefore, *Case 3* is the *counter-example* for the initial version of the actual account of privacy. I believe that this account can be revised again by adding the condition that B has reason to think that A wants to keep the information that has been accessed private. I suggest the below definition, which correctly interprets Case 3 by saying that Brian has reason to think that Annabel does not intend to keep the information that has been accessed private. Thus, Annabel's privacy has not been lost.

Definition 5 A's privacy is lost iff: B actually accesses personal information P about A, and A intends that P remain private, or, *B has reason to think that A intends to keep it private*.

The above definition indicates that privacy diminishment for A is not solely about A's personal decision, but also about the contexts in which they participate. In cases where B does not know whether the information accessed is private, they make a decision on behalf of A by giving a reason why accessing that information may or may not lead to a privacy diminishment for A. This means that the context can impact and affect A's privacy. Precisely, privacy has both personal and common characteristics.

Referring to the reasonable expectation in my revised version of the actual access account of privacy seems to link the descriptive aspect of privacy to norms and values, in that there is a clear set of normative values that explains what the reasonable expectation is in a certain situation. However, norms that are characterised as the reasonable expectation are different from the moral values to which the normative conception of privacy might refer. For example, reasonable expectations might refer to legal norms (purpose limitation, such as in Case 3) or cultural norms prevalent in society, which do not necessarily constitute a normative account of privacy, which is based on moral values and norms. Moreover, the descriptive account of privacy has other parts, namely actual access and source control, that are not solely values. Thus, the descriptive aspect of privacy considers multiple elements which are not reducible to the normative concept of privacy. That is why I believe that my analysis is still related to the descriptive aspect of privacy and is not reduced to the normative one.

Table 1 Compare and contrast different versions of the source control and the actual access accounts of privacy

	Initial version of source control account of privacy	Initial version of actual access account of privacy	Revised version of source control account of privacy	Revised version of actual access account of privacy
Case 1	no privacy loss	privacy loss	no privacy loss	no privacy loss
Case 2	privacy loss	privacy loss	privacy loss	privacy loss
Case 3	no privacy loss	privacy loss	no privacy loss	no privacy loss
Case 4	no privacy loss	privacy loss	privacy loss	privacy loss
Case 5	no privacy loss	no privacy loss	no privacy loss	no privacy loss
Case 6	privacy loss	privacy loss	privacy loss	privacy loss

6 Paradigmatic cases

This section is the first piece of evidence that the revised views of control and access accounts of privacy are extensionally equivalent. To demonstrate this, I test the revised views on different sets of information to see which of the revised accounts explains the loss of privacy in the cases. I focus on the sets of information introduced by Rumbold and Wilson [19]. They provide abstract classes of information that can possibly be gained through analysis and inference regarding personal information P. In what follows, I categorise each of the cases explored in the previous section according the classes of information provided and analyse how the revised accounts explain whether privacy is diminished. The sets of information are as follows:

- Public information which has always been public,
- Private information an agent intends to remain private (Case 5),
- Once-private information an agent has intentionally shared (Case 1),
- Once-private information an agent has no intention of sharing of that they are unaware was shared (Case 2),
- Information inferred from once-private information that an agent has intentionally shared and which itself counts as a piece of information that the agent intended to share (Case 3),
- Information inferred from once-private information that an individual has intentionally shared but which does not count as a piece of information that the agent intended to share (Case 4),
- Information inferred from shared information that an agent has only shared unintentionally (Case 6).

Both source control and actual access accounts hold that not all information is subject to privacy concerns. Privacy does not concern any information about agent A. It is not a loss of A's privacy if we discover that s/he wears glasses (public information) [12]. As a result, losing source control over or accessing information that has always been public does not lead to privacy loss.

As discussed in the previous sections, both revised accounts argue that A's privacy has not been diminished in Cases 1 and 3. Previously, I also argued that A's privacy in Case 5 was not lost based on the revised version of the actual access account. Furthermore, the source control view argues that no privacy loss has occurred in Case 5. Thus, A still could be the right source control of information, and no loss of privacy has occurred.

By contrast, as I have already discussed, both revised versions of the source control and actual access views posit that A's privacy is lost in Case 2. Previously, I also argued that A's privacy was diminished in Case 4 based on the source control view. In addition, the revised access account states that A's privacy is lost in this case. Although B has reason to think that A intends to keep the information accessed private, B accesses that information, resulting in a loss of A's privacy. Furthermore, concerning the actual access account, I have already stated that, in Case 6, A's privacy is lost. Moreover, the source account of privacy argues that A's privacy is lost because the information inferred about A flows without A being the right kind of source of this flow, resulting in a diminution of A's privacy.

The results of the test of the revised versions of source control and access accounts of privacy on whole comparable cases are presented in Table 1. The first two columns highlight the differences between the initial accounts of privacy in answering the question of whether privacy is lost. The grey cells in the last two columns of the table indicate cases

in which the initial and revised versions of the accounts have different answers regarding the loss of privacy, providing a contrast between the two. Comparing the initial and revised accounts shows the changes that have been made.

Both revised versions of the source control and actual access accounts of privacy give the same answers to the question of whether privacy is diminished (see the last two columns above), while they provide different answers as to why it is diminished. Moreover, these revised versions are located somewhere between the initial ones. As Table 1 shows, according to the initial version of the Menges' account of privacy, privacy loss is rare; it is lost in two of six cases, while, according to the initial version of the Macnish's account of privacy, privacy is lost often, in five of six cases. Nevertheless, in the revised versions of both accounts, there is a loss of privacy in three of six cases. Therefore, I claim that these initial versions are two poles on a continuum, with intermediate forms in between.

7 Theoretical argument that the proposed views of privacy are extensionally equivalent

So far, I have tested the proposed views of privacy on paradigmatic cases. The test revealed that there is no case in which a person loses control over the information flow due to the actions of another if the personal information, which A intends to keep private, is not accessed. Furthermore, there is no case in which private information is accessed such that the person does not lose source control. The paradigmatic cases give us a practical reason to think that these proposed views of privacy are extensionally equivalent. This section, meanwhile, gives us the theoretical reason to think this is the case.

On the source control front, I claim that no loss of source control occurs when the information is not accessed, or that A loses source control of P when B actually accesses information P about A. The kind of control defended in the source control account of privacy, I believe, is not robust enough, which means that agent A is not in a position to decide whether B accesses his/her information or to stop B from accessing his/her personal information because A does not have the ability to do otherwise. A loss of privacy does not occur when B accesses information P about A, but rather when B actually accesses some information which A intends to keep private. Since obtaining information about A in a way which is contrary to A's preferences results in a loss of A's source control over P, actual access to information P about A results in a loss of source control of P. Thus, the distinction between the views collapses.

On the actual access front, I claim that no actual access is achieved such that A does not lose source control, or B actually accesses information P about A when A loses source control of P. A loses source control of P when P flows in a way that is not grounded on A's intention or desire. Since actual access occurs when B accesses information that A intends to keep private, I conclude that the loss of source control leads to actual access. Moreover, it is impossible for A to lose source control of P while B has not accessed P. B not accessing P means that P has not yet flowed. If no one has actual access to the information, A can still remain the right source control of information. If the information does not flow, that is, no actual access occurs, only leeway control is lost, and A remains the right source control of information. Thus, when A is not the right source of control over their information P, having actual access to P diminishes A's privacy. I conclude that actual access does not diminish privacy if the access relates to A in the appropriate way. Thus, the distinction between the views collapses.

The preceding discussions show that the source control and actual access accounts of privacy are extensionally equivalent but different in their underlying rationales. In other words, these are two formulas that lead to the same result: a loss of privacy. The implications for such a difference in underlying rationales can be discussed in relation to the normative aspect of privacy, when privacy matters morally. Given that the main goal of this paper is to focus on the descriptive aspect of privacy, I briefly explain its implications. As both accounts of privacy are extensionally equivalent, I view them as two perspectives that reach the same peak of a mountain, and I see the value of privacy as a cluster that encompasses the values represented in both accounts. Privacy is itself a cluster of values that intersects with the cluster of values that comprise control accounts, such as autonomy and individual liberty (see, e.g. Roessler [7]), and also with the cluster of values comprising access accounts, such as secrecy and anonymity (see, e.g. Gavison [5]). By perceiving privacy as a cluster of values, we can take a pluralistic approach that encompasses all the values in the cluster to understand the normative aspect of privacy. This means that we take into account all different values of privacy to form a more comprehensive and inclusive understanding of its normative aspect.

8 Conclusion

This paper offered new insight into the debate about the nature of privacy. There is persistent disagreement in the literature on privacy's proper meaning and definition. However, the two definitions that are prominently discussed in the literature are 'control' and 'access'. Control [4] and limited access [20] accounts of privacy have recently been developed by identifying the kind of control that is relevant

to determining whether a person has privacy with regard to certain information and by incorporating a semantic account into the limited access account of privacy. Source control [10, 11] and actual access [12, 13] accounts of privacy are these most recent versions. Because they are the most in-depth version of the classic accounts of control and access, they were chosen as the focus of this paper. However, the debate over which account provides the proper definition of privacy, which is presented in the traditional control and access views, persists in the most recent versions, as well. In this paper, I demonstrated that the revised versions of the source control and actual access of privacy are extensionally equivalent. First, I discussed these views are extensionally equivalent when applied to various test cases. They only differ regarding the explanation of why privacy is diminished. Second, from a theoretical perspective, the relationship between source control and actual access views is equality, meaning that the extensions of these views are equivalent, while the differences between these two can metaphorically be explained by referring to different sides of the same mountain.

Acknowledgements I wish to extend my special thanks to Dr. Kevin Macnish, Dr. Adam Henschke, and Dr. Björn Lundgren for their helpful advice and comments that helped improve the quality of my paper.

Author contributions HA: is the single contributor of this paper.

Funding Haleh Asgarinia is supported by the Ph.D. fellowship from the 'PROTECT- Protecting Personal Data Amidst Big Data Innovation' project, funded by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 813497.

Data availability Not applicable.

Code availability Not applicable. The paper in part or in full has not been submitted or published anywhere. The paper will not be submitted elsewhere until the editorial process is completed.

Declarations

Conflict of interest The author has no competing interests to declare.

Ethics approval Not applicable.

Consent to participate Not applicable.

Consent for publication Not appliable.

References

1. Parfit, D.: On What Matters: One. Oxford University Press, Oxford (2011)
2. Warren, S.D., Brandeis, L.D.: The right to privacy. Harv. Law Rev. **4**(5), 193–220 (1890). https://doi.org/10.2307/1321160
3. Solove, D. J.: "Understanding Privacy," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 1127888. Available: https://papers.ssrn.com/abstract=1127888
4. Inness, C.: 1996 Privacy, Intimacy, and Isolation. Oxford University Press, New York (1996)
5. Gavison, R.: Privacy and the limits of law. Yale Law J. **89**(3), 421–471 (1980). https://doi.org/10.2307/795891
6. Reiman, J.H.: Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. St. Clara Comput. High-Technol. Law J. **11**, 27 (1995)
7. Roessler, B.: "The Value of Privacy | Wiley," *Wiley.com*. https://www-wiley-com.ezproxy2.utwente.nl/en-us/The+Value+of+Privacy-p-9780745631103 (2005)
8. Westin, A. F.: "Privacy And Freedom." 6 (1967)
9. Henschke, A.: Ethics in an Age of Surveillance: Personal Information and Virtual Identities. Cambridge University Press, Cambridge (2017)
10. Menges, L.: A defense of privacy as control. J. Ethics **25**(3), 385–402 (2020). https://doi.org/10.1007/s10892-020-09351-1
11. Menges, L.: Did the NSA and GCHQ diminish our privacy? What the control account should say. Moral Philos Polit. **7**(1), 29–48 (2020). https://doi.org/10.1515/mopp-2019-0063
12. Macnish, K.: Government surveillance and why defining privacy matters in a post-snowden world. J. Appl. Philos. **35**(2), 417–432 (2018). https://doi.org/10.1111/japp.12219
13. Macnish, K.: Mass surveillance: a private affair? Moral Philos Polit. **7**(1), 9–27 (2020). https://doi.org/10.1515/mopp-2019-0025
14. Finn, R.L., Wright, D., Finn, R., Wright, D., Friedewald, M., Isi, F.: Seven Types of Privacy. In: European data protection: coming of age, pp. 3–32. Springer, Netherlands. Dordrecht (2013)
15. Powers, M.: A cognitive access definition of privacy. Law Philos. **15**(4), 369–386 (1996). https://doi.org/10.2307/3505032
16. Frankfurt, H.G.: Alternate possibilities and moral responsibility. J. Philos. **66**(23), 829–839 (1969). https://doi.org/10.2307/2023833
17. M. McKenna and D. J. Coates, "Compatibilism." Available: https://plato-stanford-edu.ezproxy2.utwente.nl/archives/spr2020/entries/compatibilism/
18. Mainz, J.T., Uhrenfeldt, R.: Too much info: data surveillance and reasons to favor the control account of the right to privacy. Res. Publica. **27**(2), 287–302 (2021). https://doi.org/10.1007/s11158-020-09473-1
19. Rumbold, B., Wilson, J.: Privacy rights and public information. J. Polit. Philos. **27**(1), 3–25 (2019). https://doi.org/10.1111/jopp.12158
20. Gavison, R.: Privacy and the limits of law. In: Schoeman, F.D. (ed.) Philosophical dimensions of privacy 1st, pp. 346–402. Cambridge University Press, Cambridge (1984)