Three Control Views on Privacy

Leonhard Menges

This is the accepted manuscript version of an article forthcoming in *Social Theory and Practice* (https://pdcnet.org/soctheory).

Abstract

This paper discusses the idea that the concept of privacy should be understood in terms of control. Three different attempts to spell out this idea will be critically discussed. The conclusion will be that the so-called Source Control View on privacy is the most promising version of the idea that privacy is to be understood in terms of control.

Keywords: privacy; control; choice; negative control; sourcehood

1. Introduction

This paper discusses the idea that the concept of privacy should be understood in terms of control. This idea has been spelled out in different ways (Section 2). But which one is the

most adequate? This is the guiding question of the paper.

I will argue for three main theses. First, the standard version of the control view—which says that privacy consists in having a choice between different options—can be defended against the most prominent objections (Section 3). Second, this standard version of the control view is, nonetheless, false, but it is so for reasons other than its opponents typically claim (Section 4). Third, the most adequate attempt to spell out the idea that privacy is to be analyzed in terms of control is the Source Control View (that I have recently developed, see Menges 2020b; 2020a).

Some clarifications are in order. One is that I will only be concerned with informational privacy and not with locational, decisional, or other kinds of privacy. Informational privacy is the kind of privacy we have in mind when we worry whether, for example, the data mining of Google, Facebook, the NSA, and so on affect our privacy. Second, very similar questions about privacy are sometimes discussed under two different headings. Some privacy scholars discuss the question of how to understand the *concept* of privacy (e.g. Parent 1983a; Macnish 2018; Lundgren 2020). Others discuss the *right* to privacy and the question of what we have a right to when we have a right to privacy (e.g., Thomson 1975; Rickless 2007; Davis 2009; Marmor 2015). This paper follows the first group. The arguments in this paper can also be framed as arguments for and against certain views on the right to privacy and I plan to spell this out in future work. The official theses in this paper, however, are only concerned with the concept of privacy.

The third remark is, probably, the most important. Even though I believe that a clear account of the concept of privacy can throw new light on certain legal, ethical, and political problems, that will not be the aim of this paper. It focuses solely on conceptual issues. That

is, the goals of this paper are deliberately moderate. To see this, consider what a *complete* control account of privacy is sometimes expected to do.

Anita Allen (1999) argues that a control view is confronted with three independent challenges: first, it needs to show that this view is *conceptually adequate*, that is, it should fit with at least an important part of our everyday understanding and usage of "privacy". This is the challenge I will be concerned with in this paper. Second, the control view should be defended against the objection that it has *practical limits* because there are serious "concerns about whether people can actually control personal data" (Allen 1999: 869). Third, Allen objects that the control view has *moral limits* because "in so many policy contexts it is wrong to insist on individual control over personal data" (Allen 1999: 871).

Assume for a moment that a control account of privacy can meet these challenges. A defender of this account then still needs to show, fourth, that it is *theoretically fruitful*. That is, most authors who discuss privacy are not only interested in abstract philosophical questions. They want to make sense of ethically, socially, and politically pressing real-world issues, for example in the context of new information technology. Most prominently, Helen Nissenbaum has argued that the idea that privacy is control fails on this. She contends that control views do not "provide sufficiently finely tuned responses to many challenges to privacy posed by these [socio-technical] systems and practices" (Nissenbaum 2009: 103; relevant socio-technical systems involve CCTV security cameras or the Internet).

A complete control account should deal with these challenges. But, as I said, this paper has more moderate aims. It only focuses on conceptual questions and leaves the other issues untouched. The hope is, of course, to thereby provide clear conceptual grounds that

will help meeting the other desiderata in future work.[1] But this is not the aim of *this* paper.

With this in place let me begin with a more detailed presentation of the control view on privacy.

2. Three Versions of the Control View on Privacy

The idea that privacy is to be analyzed in terms of control is very popular and sometimes presented as the standard view on privacy, especially by its critics (see, e.g., Allen 1999: 863; Rickless 2007: 779; Barocas and Nissenbaum 2014: 45; Macnish 2018: 419). To be more precise, I will call the basic idea

> *The Control View*: An agent has privacy just in case the agent has some kind of control over personal data.

The Control View has an initial plausibility because in many cases privacy and control behave in sync: when control is diminished, then privacy is, intuitively, also diminished, and the other way around. To illustrate, consider the following case:

> *Housemate*: While you are writing in your diary that you fell in love with S, your housemate peeps over your shoulder and learns about your feelings.

[1] Thus, I don't agree with those who argue that a purely conceptual approach to privacy is pointless (see Moore 2008: 416; van den Hoven 2008: 303).

Intuitively, your housemate diminishes both your control over personal data and your privacy. The Control View says that this is not a coincidence. According to this view, your housemate's diminishing your control over personal data constitutes diminishing your privacy.

Many have taken this to be an initially plausible and elegant account of privacy and have tried to spell out the details. In what follows I will focus on the question of how to spell out the notion of control at the heart of the Control View.

2.1 The Standard View: Control as Choice

The standard version of the Control View contends or suggests that having the relevant kind of control should be understood as having a choice between different options. Proponents of this view believe that having privacy is essentially a matter of having a choice about whether or not something happens.

Charles Fried, for example, argues that "[t]he person who enjoys privacy is able to grant or deny access to others" (Fried 1968: 210). Thus, he contends that privacy involves a choice over whether or not something happens, namely that others have access. Similarly, Richard B. Parker argues that "because husband and wife choose to constantly sense one another, husband and wife will be much more intimate. This choice is an exercise of privacy" (Parker 1974: 286). Another example is Julie Inness. She argues that privacy is a form of control and specifies her understanding of the relevant kind of control. She says that we have the relevant kind of control "in situation *X* when there exists a reasonable

probability that we could regulate the outcome of the situation without recourse to emergency maneuvers" (Inness 1992: 51). In this context, the notion of regulation is important. Inness takes privacy to involve the ability to regulate outcomes, which can, plausibly, be characterized as having some kind of choice over whether or not the outcome occurs.

Those who focus on the right to or the value of privacy also argue or suggest that privacy and the right to it are primarily concerned with protecting choice between different options. James Rachels, for example, explains the value of privacy in the following way:

> The explanation is that, even in the most common and unremarkable circumstances, we regulate our behavior according to the kinds of relationships we have with the people around us. If we cannot control who has access to us, sometimes including and sometimes excluding various people, then we cannot control the patterns of behavior we need to adopt (this is one reason why privacy is an aspect of liberty) or the kinds of relations with other people that we will have (Rachels 1975: 331).

Rachels suggests that the importance of privacy at least partly consists in giving us choice over "sometimes including, sometimes excluding various people". Admittedly, it does not follow from this that Rachels is committed to saying that having privacy itself is having a choice between options. However, this would be an interpretation that comes quite close to what he actually says. We find similar remarks in more recent work on the value of or the right to privacy, for example in Beate Rössler (2004: chap. 5.1) and Andrei Marmor (2015: 11)

The point of this brief survey is to show that many of those who accept the Control View also accept the more specific idea that having privacy essentially involves having a choice between options. I will call this version of the Control View the

> *Control as Choice View*: An agent has privacy just in case the agent has some kind of control over personal data. This control (partly) consists in the agent's having a choice with regard to whether or not some event occurs.

Applied to the Housemate case, this view says that your housemate diminishes your privacy by taking away certain options to choose from. Most clearly, your housemate takes away the option to keep your feelings secret and, thereby, diminishes the choice that constitutes your privacy, according to the Control as Choice View.

2.2 Two Recent Alternatives: Negative Control and Source Control

While the Control as Choice View is typically taken to be the standard account, very recently two alternatives have entered the scene.

Jakob Mainz and Rasmus Uhrenfeldt (2020) explicitly focus on the right to, not the concept of, privacy. They suggest that control theorists of the right to privacy should understand this right as the right to what they call negative control, a notion inspired by Isaiah Berlin's (1958) distinction between positive and negative liberty. Mainz and Uhrenfeld define negative control in the following way: "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" (Mainz and Uhrenfeldt 2020: 7). Proponents of the control account of the concept of privacy can adopt this idea. They can say that A has privacy with regard to personal information P just in case A is capable of preventing any agent B, who attempts to access, from accessing P. Let me call this Mainz-and-Uhrfeldt-inspired account the

> *Negative Control View*: An agent has privacy just in case the agent has some kind of control over personal data. This control consists in the agent's being able to prevent others from accessing the data if they attempt to do so.

This account says that your housemate diminishes your privacy by diminishing your ability to prevent others from accessing information about your feelings. First, your housemate accesses the data and, second, it becomes much harder for you to keep third parties from learning about this information because your housemate can tell them about it.

I have presented a second alternative to the Control as Choice View (Menges 2020b; 2020a). While Mainz and Uhrenfeldt adopt a notion of control from political philosophy, my view is inspired by debates about acting out of free will and responsibility for actions. In this debate, many of those who contend that humans can be responsible and act out of free will even if our universe is deterministic argue that agents can have a certain kind of control over what they do even if they cannot effectively choose between different options. So-called Frankfurt cases provide the most famous examples. In these cases it is inevitable that an agent A will perform a certain action X. This is so because another agent B has set things up in such a way that should A be inclined to not do X, B will make it the case that A

does X. However, A shows no inclination at all to not do X, B does not intervene, and A does X for their own reasons (for overviews see Sartorio 2016; Robb 2020). The key point of Frankfurt cases is to trigger the intuition that A is responsible for X and does X out of free will even if A could not effectively choose between doing X and not doing X. If one assumes that an agent is only responsible for an action if they had a certain kind of control over performing it (a highly plausible assumption), then we are committed to saying that A had a kind of control even though A had no choice.

One prominent way to spell out this kind of control is in terms of being the right kind of source of the action. That is, the action must be grounded, in the right way, in the agent and not in someone or something else. For example, the action must be grounded in certain desires and second-order desires, cares, beliefs, or certain traits of the agent (for an overview see McKenna and Coates 2020). Details aside, the general idea is that agents have the relevant kind of control over their actions just in case, if the agents act at all, then they are the right kind of source of this action.

The key idea is that the kind of control that is at the heart of the Control View on privacy should be understood as source control. Let me call the resulting account the

> *Source Control View*: An agent has privacy just in case the agent has some kind of control over personal data. This control consists in "the agent's being such that if the [data flow], then the agent is the right kind of source of this [data] flow" (Menges 2020a, 20).

On this view, your housemate diminishes your privacy by letting information about your

feelings flow even though you were not the right kind of source of this flow. The data flow circumvented your desires, beliefs, cares and so on, which, according to the Source Control View, constitutes diminishing your privacy.[2]

To sum up, there are at least three different attempts to spell out the notion of control at the heart of the Control View on privacy. One spells out control in terms of having a choice between options, the other in terms of being able to prevent others from accessing data, and the third in terms of sourcehood of information flow. The question is: which one is best?

3. The Standard Challenges

[2] An anonymous referee asks the difficult question "what is data flow?" I adopt the notion from Nissenbaum, who speaks about "information flow" and characterizes it by using other metaphors: for her, information flow is "movement, or transfer of information from one party to another or others" (Nissenbaum 2004: 122) or "distribution, dissemination, transmission" of information from one party to another (Nissenbaum 2009: 145). This sounds as if information flows only, on Nissenbaum's view, if there is a party that, in fact, receives the information. On my view, by contrast, no receiver is needed. Data flow as soon as there is a source (e.g., an agent) and the data "move" away from the source (like a trickle that comes from a source of water). For this to happen, no receiver and no conscious agency is needed. Importantly, however, the Source Control View does *not* say that having privacy is simply being the source of a data flow. The view says that having privacy is being *the right kind* of source of the data flow, if the data flow. And it is an open question how to spell out "the right kind" (see Menges 2020a: sec. 4.1).

Opponents of the Control View have long argued that it is extensionally inadequate. In this section I will present the two standard arguments to this conclusion (Section 3.1) and I will argue that the Control as Choice and the Source Control View can be defended against both objections (Sections 3.2 and 3.3). The Negative Control View has a serious problem, however (Section 3.2).

3.1 Too Broad and Too Narrow

In the literature on privacy, the standard procedure to test the extensional adequacy of an account of privacy involves two steps. First, one imagines a situation in which it is intuitively plausible that an agent has privacy with regard to a certain piece of information. Applying the conceptual account under consideration to this situation should, and typically does, imply that, according to this view, the person has privacy. Second, one imagines an event that changes the situation in a way that (a) intuitively does not diminish the person's privacy or (b) intuitively diminishes the person's privacy. Then, we apply the account of the concept of privacy again. If the event is of type (a) such that, intuitively, it does not diminish the person's privacy but the account implies that it does, then this speaks against the account: the case shows that the account under consideration is too broad or, in other words, that it implies false positives. If the event is of type (b) and, intuitively, diminishes the person's privacy, but the account under consideration implies that it does not, then this also speaks against the account: it shows that the account is too narrow or implies false negatives.

Here are two widely discussed examples of this procedure. Consider, first, a

> *Threatened Loss Case*: First, imagine that I have a fight with my partner and nobody knows about it but us. Second, our neighbor A "invents a fantastic X-ray device that enables him to look right through walls. A then focuses the device on my home [where I am having the fight with my partner] but refuses to use it" (Parent 1983b: 344).

While some may be put off by such a bizarre case, there are important real-life scenarios that are similar in relevant ways. For example, the Snowden revelations suggest that the collection of Internet and mobile phone data by the NSA and GCHQ was—in relevant respects—like my neighbor's focusing the fantastic device on my home. Like the neighbor, members of the intelligence agencies could easily access data about Internet users but, in most cases, refused to do it (see Macnish 2018: sec. 1). Prisons offer another real-life Threatened Loss Case. Prisoners in solitary confinement are, sometimes for a long time, completely alone and nobody accesses personal information about them. In some prisons, however, officials can access information about the prisoners by entering the cells at any time or by using cameras, just like my neighbor in the case above (see Allen 1999: 868).

In order to keep things simple, I will focus on the Threatened Loss Case involving the fantastic X-ray device. But it is important to keep in mind that there are socially important analogous cases.

Opponents of the Control View start with the intuitive idea that, before setting up the device, my partner and I have privacy with regard to the information that we are having a fight. The relevant event is, then, my neighbor's setting up the fantastic device. This event

is of type (a) because, the objection goes, merely setting up the device without using it does not, intuitively, diminish our privacy. According to the objection, the Control View implies that setting up the X-ray device diminishes our privacy because it diminishes our control over whether or not my neighbor can learn about the fight. Opponents of this view conclude that the Control View is extensionally inadequate because it is too broad (Parent 1983b: 344; see also Allen 1999: 868; Rickless 2007: 783; Davis 2009: 457; Moore 2010: 21 N. 35; for a related but different case see Macnish 2018: 420; Lundgren 2020: 169).

Another famous test of the extensional adequacy of the Control View is based on

> *Voluntary Divulgence Cases*: First, imagine that I have a serious problem with trying to publishing papers in prestigious journals, which makes me suffer from self-doubt. I have recently begun to drink a bottle of liquor a day, and nobody knows anything about any of this. Second, imagine that, in a sober moment, I voluntarily divulge this personal information about myself to complete strangers.

That Voluntary Divulgence Cases are not only philosophers' fantasies should be obvious to everyone who has used social networks or consumed commercial TV in the last few decades.

The starting point is, again, the intuition that I have privacy with regard to the relevant personal information when nobody knows about it. My voluntarily divulging it is, then, taken to be an event of type (b) because opponents of the Control View say that it is intuitive that my conduct diminishes my privacy. The objection continues that the Control View implies that my voluntarily divulging the information does not diminish my privacy

because I have full control over my doing it. According to this view, the objection says, I exercise the kind of control that constitutes my privacy, but I do not diminish it. As some opponents of the Control View find this implausible, they conclude that this view is too narrow and, therefore, extensionally inadequate (see, e.g., Gavison 1980: 427; Allen 1988: 26; 1999: 867; Parent 1983a: 273; Lundgren 2020: 171).

Threatened Loss and Voluntary Divulgence Cases provide the most famous challenges to the extensional adequacy of Control Views. The first is meant to suggest that Control Views are too broad, the second that they they are too narrow.

3.2 Three Replies to Threatened Loss Cases

The core of this sub-section will be a defense of the Control as Choice View against the objection from Threatened Loss Cases. Moreover, I will argue that the Negative Control View has serious problems with these cases.

Take the Control as Choice View and recall that Inness (see 1992: 51) characterizes the kind of control that she takes to be essential for privacy as there being a reasonable probability that one can regulate the outcome of the situation without recourse to emergency maneuvers. Her illustration of an emergency maneuver is someone's hiding under the bed from a Peeping Tom. She suggests that the control that constitutes privacy is only lost when the measures one takes to protect one's personal realm "are required to be emergency measures or access is actually gained" (Inness 1992: 51).

Interestingly, Inness' view has not been taken into account in the recent debates about the concept of privacy (see Macnish 2018; Lundgren 2020). One possible reason for this is

that the claim that one's privacy is only diminished when access is gained or one is required to adopt emergency measures is underdeveloped and quite *ad hoc*. In what follows, I will propose an understanding of emergency measures that helps the Control as Choice View deal with the objection from Threatened Loss Cases and that avoids the *ad hoc* part of Inness' reply (thanks to an anonymous referee for pressing me on this).

Think about emergency maneuvers that have nothing to do with privacy. Imagine, first, that kidnappers incarcerate you. Fortunately for you, your cell has a big window to the street that you can open. Intuitively, the kidnappers have diminished your control over where you can go. They do this by putting you in a situation in which you have only two bad options, namely staying incarcerated or adopting an "emergency maneuver", namely climbing out of the window. As a second example, imagine that robbers coerce you by telling you: "Your money or your life!". And imagine that they mean it in earnest: if you let them kill you, they won't take your money and, for example, will leave it to your family. Thus, you still have a choice between getting killed or losing (family) money. Nonetheless, the robbers radically diminish your control over what you do. They do this by putting you in a situation in which you have two bad options, namely getting killed or adopting the "emergency maneuver" of giving them your money.

Let us take a step back. According to a standard account of autonomy, one way to diminish a person's autonomy is to restrict the options that are available to the person (Raz 1988: 373–377; for an overview see Christman 2020). This is what the kidnappers and robbers do in the two cases. They diminish your autonomy by putting you in situations in which either something bad will happen to you or you do something that is still bad, but less so.

My proposal is that Inness' reference to "emergency maneuvers" can be replaced by or understood in terms of autonomy-diminishing option restriction. That is, when Inness talks about emergency maneuvers one can think of whatever courses of action are left to us after others have restricted our options in an autonomy-diminishing way. This provides the resources for an account of privacy that I will call the

> *Inness-style Control as Choice View*: An agent has privacy just in case the agent has some kind of control over personal data. This control (partly) consists in the agent's having a choice between different options and it being reasonably probable that the agent's choice determines which option is realized. Others diminish this choice by restricting the agent's options about what happens with their personal data in an autonomy-diminishing way.

I do not contend that this is the view Inness argues for—I'm not interested in exegetical questions here. Rather, this should be read as an Inness-inspired attempt to spell out some details of the Control as Choice View. Moreover, this view is quite attractive. Note, for example, that the reference to autonomy fits nicely with standard Control as Choice Views because proponents of it often defend the value of privacy by arguing that it protects personal autonomy (e.g., Inness 1992: chap. 7; Rössler 2004: chap. 3; for a critical discussion see Mokrosinska 2018). Moreover, this version of the Control as Choice View avoids Inness' *ad hoc* contention that an agent's privacy is only diminished when others access data or the agent has to do something.

Of course, the account is not complete. One natural question to ask is: when, exactly,

does a restriction of option diminish an agent's autonomy? To illustrate, imagine that Peter asks Jane out for dinner. "Jane declares that she is only willing to eat Japanese food and Peter is desperate enough for her company that he complies with this demand" (Miller 2010: 113). Would Jane, thereby, diminish Peter's autonomy? A full account of autonomy should provide an answer, but developing one would go far beyond the scope of this paper. However, the discussion so far shows where defenders of the Inness-style Control as Choice View can look when they try to fill this gap. They should consult the best accounts of diminishing autonomy by restricting options in other debates. One example is the discussion in migration ethics about whether border control undermines the autonomy of migrants by restricting their options (see Abizadeh 2008; 2010; Miller 2010).

Let us, finally, see how the Inness-style Control as Choice View deals with the Threatened Loss Case: my partner and I are having an argument and the X-ray device is focused on our home, but the neighbor refuses to turn it on. At this moment our neighbor is not restricting our options with regard to what happens with our personal data. All options are still available to us. That is, no autonomy-diminishing option restriction takes place. To put it in the terms used by Inness: we do not need to take emergency measures to protect the information that we are having a fight—indeed, we do not need to take any measure because the neighbors refuse to turn on the device. Thus, there is still a reasonable probability that our choice determines the outcome. For example, we can choose whether or not our neighbors learn about the fight because we can tell them about it or not. That is, we still have the kind of control that, on the Inness-style Control as Choice View, constitutes our having privacy. This version of the Control as Choice View does not, therefore, imply a false positive when applied to the Threatened Loss Case.

Importantly, I have not argued that the Inness-style view is correct. Indeed, I will argue below (Section 4) that it is false. But we can learn something important from this defense of the Control as Choice View: Threatened Loss Cases are often presented as posing problems for the Control as Choice View *as such*. That is, opponents of this view take these cases to make clear that it is not true that privacy should be understood in terms of having a choice between options. The Inness-style reply shows, however, that the case does not pose problems for the Control as Choice View as such but only for specific versions of it. This is so because there is an Inness-inspired notion of control as choice over options that does not imply that control is lost in Threatened Loss Cases.

Let me now turn to the Source Control View. As it has been explicitly designed in order to deal with Threatened Loss Cases, it is no surprise that it has the intuitively plausible implication (see Menges 2020b). The Source Control View says that the privacy-constituting kind of control is the agent's being such that if personal data flow, then the agent is the right kind of source of this flow. As the information about our having a fight does not flow to the neighbor before they turn on the device, this control is not diminished in the Threatened Loss Case. Thus, the Source Control View implies that no privacy is diminished.

The Negative Control View has more problems with the objection at issue. Mainz and Uhrenfeldt content that in "order for Negative Control to be lost, someone must attempt to get access, and in [Threatened Loss Cases], the neighbor does not attempt to get access" (Mainz and Uhrenfeldt 2020: 14). Then, no privacy is lost in the Threatened Loss Case and the Negative Control View would have the correct implication. However, there is reason to doubt that this reply works. Recall that Mainz and Uhrenfeldt define A's negative control

over access to personal data P in terms of A's being "capable of preventing agent B, who attempts to access, from accessing P" (Mainz and Uhrenfeldt 2020: 7). The problem is that this definition does not fit with the contention that "in order for Negative Control to be lost, someone must attempt to get access" (Mainz and Uhrenfeldt 2020: 14). And it is the latter claim that does all the work in the reply to Threatened Loss Cases. Let me elaborate.

The definition says that negative control consists in one's being *capable* of preventing others from accessing if they try to access. But this capability can be diminished without someone's trying to access. As an analogy, take people who are paralyzed because someone put k-o-drops in their drinks. Intuitively, they are not capable of preventing others from, say, touching them. They do not have the ability to prevent others from touching them, independently of whether others try. That is, they lack negative control over whether others touch them even if others do not attempt to touch them. Thus it is false to say in this case that in order for negative control to be lost, someone must attempt to touch them.

The same holds for negative control over personal data. Imagine that someone puts a fantastically effective truth drug in my drink without my knowledge and against my will. Intuitively, I am not capable of preventing others from accessing personal data, such that I do not have negative control over them. This is so even if nobody asks me a question or tries to access personal data in other ways. Thus if one accepts the definition of negative control presented by Mainz and Uhrenfeldt, then it is false to say that "in order for Negative Control to be lost, someone must attempt to get access". However, the reply of the Negative Control View to the objection from Threatened Loss Cases relies on the assumption that others' attempting to access personal data is necessary for losing negative control. Therefore, the reply fails.

As an intermediate conclusion, a version of the standard Control as Choice and the Source Control View can be defended against the objection from Threatened Loss Cases. The Negative Control View, however, does not meet this challenge. Thus, we are left with two versions of the Control View.

3.3 A Three-Step Reply to Voluntary Divulgence Cases

Recall the Voluntary Divulgence Case: I exercise control over the information that I have severe personal problems by telling a complete stranger about them. The objection says that the Control View implies, implausibly, that I, thereby, retain my privacy. In what follows I will present a three-step reply on behalf of all versions of the Control View that is inspired by a remark by Inness (1992: 46). I have spelled out the details of step 1 and 2 in (Menges 2020a: sec. 3). Thus, step 3 is the most important part of this reply.

First, proponents of Control Views should argue that they have no problem making sense of the idea that some Voluntary Divulgence Cases involve diminishing privacy. Agents who have only diminished control over personal information because of drugs, mental health issues, ignorance, or something similar diminish their privacy by voluntarily divulging information. These factors undermine the control that constitutes privacy, according to Control Views. Therefore, exercising this control does not retain privacy.

Second, proponents of the Control View should contend that agents who have *full* control over their information do not diminish their privacy by revealing personal facts about them. Let me illustrate. In 2006 Tarana Burke used the phrase "Me Too" on the website "Myspace" in order to share the message with survivors of sexual assault that they

are not alone. She, thereby, revealed that she was sexually assaulted (see Garcia 2017; Biography.com Editors 2018). Let us imagine that she had full control over what she did. Did she diminish her privacy by exercising this control? I find it most plausible to say that she did not. We could say that she shared private information with the public. But this does not necessarily involve giving up privacy because we can share private information with a good friend without giving up privacy.

Here is another case: in 2014 Thomas Hitzelsberger was the first high-profile soccer player to reveal that he is gay. "I'm coming out about my homosexuality because I want to move the discussion about homosexuality among professional sportspeople forwards," he said (BBC 2014). Again, let us imagine that he had full control over what he did. It is not obvious that Hitzelsberger diminished his privacy. Alternatively, one can say that he invited the public into his private realm in order to open a debate. This does not need to involve losing privacy. More generally, proponents of the Control View should contend that exercising full control over personal information by revealing it does not diminish their privacy.

Some may find this hard to accept. The worry is that it seems very plausible that my exercising full control by voluntarily divulging personal information somehow *does* affect my privacy. And, the worry continues, the reply I have just presented cannot make sense of this. The third step is meant to tackle this objection. The basic idea is that proponents of the Control View should argue that agents who reveal personal information by exercising full control *now* can, thereby, threaten their *future* privacy. In this way, the view makes sense of the intuition that privacy is somehow affected in many Voluntary Divulgence Cases, namely: the agent's future privacy is threatened.

The basic insight is that those who exercise control over personal information now by making it public can and often do, thereby, diminish their future control over what happens with the information. Imagine that I have full control when I tell the strangers about my personal problems in the original Voluntary Divulgence Case. Later, the strangers can post about it on social networks or tell my head of department about it. Thus, my telling the strangers about personal information now makes it much easier for others to later restrict my options about what happens to my personal data. The Inness-style Control as Choice View, therefore, implies that my future privacy is threatened in this case. Similarly, after having told the strangers about my problems, it is much more likely that the information flows without my being the right source of the flow: they can, in principle, do with the information whatever they want. Thus the Source Control View also implies that my future privacy is threatened.

This line of thinking shows that both versions of the Control View can make sense of the idea that privacy is somehow affected in some Voluntary Divulgence Cases. Proponents of these views should argue that exercising full control by telling strangers about personal information can and often does threaten our future privacy with regard to the information.[3]

---

[3] Note that Inness and others (1992: 52; Matheson 2007: 255; Moore 2008: 415) propose a similar line of thinking, but seem to come to a different conclusion. They contend that the Control as Choice View can make sense of the idea that *current* privacy is *given up* in Voluntary Divulgence Cases. But this presupposes that my exercising a certain kind of control now diminishes this very control in this very moment. I'm puzzled by this presupposition and none of the defenders of Control as Choice Views has, as far as I know, spelled out the details of this reply to Voluntary Divulgence Cases, especially with regard to the temporal aspect. My proposal is to distinguish between the control that I have right now, when divulging information, and the control that I have afterwards. With this distinction on the table, it seems

Thus, all Control Views can be defended against the objection from Voluntary Divulgence Cases. First, if the agents' control is diminished because of factors such as mental health issues, then the views have no problem saying that privacy is diminished by exercising this control. Second, it is far from clear that exercising full control by divulging personal data to strangers diminishes one's privacy. Third, voluntarily divulging personal information often sincerely threatens our future privacy. Importantly, the last step makes sense of our uneasiness about some of these cases.

Let me briefly sum up the discussion of the Control View so far. The Negative Control View has severe problems with one standard challenge. Therefore, I put it aside. The Control as Choice and the Source Control View, however, have no problems with the standard challenges. Thus, we still do not know which of them is conceptually more adequate.

4. The Objection from Impeded Information Flow

Even though the Control as Choice View can be defended against standard objections, I believe that it is extensionally inadequate. I will now show why.

Consider what I will call the case of

Impeded Information Flow: You write an email to your friends in a country far away

most plausible to say that my exercising control now by divulging information threatens my future control over the information.

> telling them that you fell in love with S. Unbeknownst to you, your housemate hacks your email service provider (not your computer) such that every email that is sent using this service provider is encrypted in a way that neither your friends nor any other recipient can decipher. Thus you do not succeed in telling your friends about your romantic feelings by sending them emails.

Again, some may be put off by such an artificial case. But there are similar situations in the real world. After many people responded to the official declaration that Alexander Lukashenko won the 2020 election in Belarus with protests in the streets, there was an internet blackout in most of Belarus. Many protesters and observers believe that the Internet was voluntarily cut off such that this was a "rare example in modern Europe of government voluntarily knocking its entire country offline to stifle dissent" (Auseyushkin and Roth 2020; see also Makhovsky and Balmforth 2020). A voluntary state-wide internet blackout can be thought of as a case of Impeded Information Flow. Those who cut off the internet are, in certain respects, like your housemate encrypting your emails: they make sure that you cannot reveal information by using a certain technology without hacking your personal devices. Of course, they also make sure that you can't *access* information, but this point is not relevant in this context. In what follows, I will again focus on the more artificial case because the more salient issues about free speech or the right to protest may distract us from privacy. But let us keep in mind that there are similar socially important real-world cases.

The starting point is that, before your housemate hacks your email service provider, your privacy is intact. The Control as Choice View also suggests that, other things being

equal, this is so. Then, your housemate's hacking the service provider is an event of type (a) because, intuitively, it does not diminish your privacy. Your housemate makes you be *less* open than you would otherwise be and than you want to be by hacking your email service provider. Your housemate *impedes* your ability to reveal certain aspects of yourself. Such conduct certainly diminishes your freedom and autonomy. But, intuitively, it does not diminish your privacy.

No proponent of the Control as Choice View has, as far as I know, explicitly endorsed the claim that impeding information flows can diminish a person's privacy. And I doubt that they had this in mind. But I will now argue that they are committed to this claim and that this speaks against the Control as Choice View.

Take, first, Fried's analysis of privacy, according to which, "[t]he person who enjoys privacy is able to grant or deny access to others" (Fried 1968: 210). In the case at hand, your ability to grant access to your friends is not completely lost because you can still, for example, call them. However, you wanted to grant access by sending emails, you can typically do this, and you reasonably expect that it will work. Your housemate's hacking the service provider makes it the case that you cannot grant access in this way such that your ability to grant access is diminished. We can also imagine a version of the case in which the only way for you to tell your friend that you fell in love with S is via email. We can imagine, for example, that you don't have telephones, the postal service is on strike, and so on. Then, you can't grant access to this personal information such that Fried's view implies that your privacy is lost. This is implausible.

Consider, second, Inness' view, according to which privacy necessarily involves "a reasonable probability that we could regulate the outcome of the situation without recourse

to emergency maneuvers" (Inness 1992: 51). In the case of Impeded Information Flow, you cannot regulate the outcome of the situation in the way you want to regulate it and in the way you can reasonably expect it to work. The outcome of writing and sending the emails is very different from what you wanted and expected it to be. In the version of the case in which all alternative communication forms are ruled out, you cannot regulate the outcome at all. Thus, this view also implies that privacy is diminished in these cases. This speaks against the view.[4]

The Inness-style Control as Choice View that I presented above also implies that privacy is lost in this case. This is because your housemate diminishes your choice by restricting your options about what happens with your personal data in an autonomy-diminishing way: their hacking the email service provider makes it the case that you can't choose the option to tell your friends about your feelings by sending them emails.

Finally, take Rachels' (1975) account. Again, Rachels does not explicitly contend that privacy should be thought of in terms of choice. But he suggests that a key function of privacy is to protect our ability to regulate our social relationships by enabling us to include or exclude certain others. In the case at hand, you cannot regulate your personal relationships by including others in the way you want to and in they way you can reasonably expect to work. If we assume (and it should be clear that this is an assumption) that Rachels understands having privacy in terms of being able to regulate relationships in

---

[4] One reading of Inness avoids the conclusion that privacy is lost in Cases of Impeded Information Flow. On this interpretation, privacy is only lost when access is actually gained if one does not adopt emergency measures (see Inness 1992: 51). However, as I said above, this is the most *ad hoc* part of Inness' overall view. And I see no resources within her account to make sense of this assumption.

this way, it would follow that, on this view, privacy would be diminished. This would be implausible.

We could go on and test each version of the Control as Choice View with this case. Fortunately, however, this is not necessary because there is good reason to think that the case of Impeded Information Flow poses a problem for the Control as Choice View as such.[5]

---

[5] Is this objection new? In the literature I found three cases that have some similarities with the case of Impeded Information Flow. The first is one developed by Daniel Farber as a problem for Inness' account of the right to privacy (see Farber 1993: 514–15; see also Solove 2008: 28). I leave it aside because Farber's case focuses on legal issues that are not of primary importance for the aims of this paper. Second, Steve Matthews (2008: 141) discusses a case in which a person is temporarily dumb and, therefore, cannot reveal personal information about themselves. As I said in the Introduction, I hope that all arguments presented here can also be used in order to defend or reject accounts of the *right* to privacy, even if this is not my primary aim. The dumbness case is not useful in this respect because no account of the right to privacy suggests that a right is infringed here. The case of Impeded Information Flow, by contrast, also poses a problem for Control as Choice Views on the right to privacy. Third, Mainz and Uhrenfeldt have developed a case that looks similar to the case of Impeded Information Flow: "Too Much Info #1: Suppose that Smith and Jones are coworkers. 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" (Mainz and Uhrenfeldt 2020: 8). This case poses a problem for views that understand a person's privacy as having a choice between another person's not having access to information and the person's *actually accessing* information. In Too Much Info #1, the second option is taken away because Jones makes sure that he does not access the information. However, Control as Choice Views don't need to say that this is the relevant pair of options. They could say, for example, that privacy essentially involves the choice between not letting personal information flow and letting personal information flow. We can let personal information flow without its

The Control as Choice View says that a person's privacy essentially involves her having a choice between at least two options. In Impeded Information Flow, you cannot choose whether or not the information that you are in love with S flows to your friends in the way you want it to flow and in the way you can reasonably expect to work. This is because your housemate diminishes your choices by taking away the option to let the information flow by using your email service provider. Thus, if the Control as Choice View is true, then your housemate diminishes your privacy. However, your housemate does not diminish your privacy. Therefore, the Control as Choice View implies a false positive and is extensionally inadequate.

In contrast to the standard cases that are used to challenge the extensional adequacy of the Control as Choice View, the case of Impeded Information Flow points to the very core of this view, namely that privacy essentially involves having a choice between options. Accepting this view commits one to saying that it is possible to diminish privacy by taking away each option: first, one can diminish people's control by taking away the option to not let information flow and, thereby, by making them reveal more than they otherwise would. Second, one can diminish control by taking away the option to let information flow and,

---

being the case that someone else accesses the information (see footnote 2 above). This is what happens in Too Much Info #1: Smith lets the information flow without Jones' accessing the information. A version of the Control as Choice View that understands privacy as having a choice between letting and not letting information flow would, therefore, imply that no privacy has been diminished in Too Much Info #1. In cases of Impeded Information Flow, by contrast, the couple's choice is diminished because the option to let information flow is taken away. Therefore, this case poses a different and more general problem to Control as Choice Views than Too Much Info #1. Thanks to Jakob Mainz and Stefan Riedener for pressing me on this.

thereby, by impeding their revealing certain information. If one assumes that having privacy necessarily involves having this kind of control, then one is committed to saying that impeding their revealing certain information diminishes their privacy. However, our everyday understanding of privacy is such that it can only be diminished in the first way. Thus, these cases suggest that the core feature of the Control as Choice View—not just a specific attempt to spell out choice—is implausible.

The Source Control View has, in contrast to the Control as Choice View, no problem dealing with the Case of Impeded Information Flow. Your housemate acts such that the information that you fell in love with S does not flow to others at all. The Source Control View says that privacy is only diminished when information flows. Thus, no privacy is diminished in this case, according to the Source Control View.

To sum up, the Control as Choice View is extensionally inadequate. Even though the Threatened Loss and the Voluntary Divulgence cases fail to show that this is so, the case of Impeded Information Flow is successful in this respect.

5. Conclusion

In the literature, there are at least three different attempts to spell out the notion of control at the heart of the claim that the concept of privacy should be analyzed in terms of control. This paper aimed at providing a systematic evaluation of them. One main thesis of the paper is that while the classic Control as Choice View can be defended against the most

famous challenges, it has significant problems with an objection that has not received the attention it deserves. Another main thesis is that the recent Negative Control View fails to meet one of the standard challenges. Thus, the only version of the claim that the concept of privacy should be understood in terms of control that can deal with all the cases discussed here is the Source Control View. For those who find the idea plausible that privacy is control, this is good reason to opt for the Source Control View and to scrutinize if it can deal with the other desiderata I have presented in Section 1.

Author Information

Leonhard Menges

leonhard.menges@sbg.ac.at

University of Salzburg

Department of Philosophy (KGW)

Acknowledgment

I am grateful to Jakob Mainz, Stefan Riedener, and two anonymous referees for helpful written comments on more recent versions of the paper. The paper has a long history. An earlier version has been commented on by three other(?) referees for this journal and very early versions have been presented in Osnabrück, Essen, and Düsseldorf (all 2016), in

Berlin (2017) and in Graz (2018). Thanks to the referees and audiences for comments. An even earlier version was discussed by Hannah Altehenger and Simon Gaus in 2016 in Lübeck. Thanks to both of them. Thanks to Claire Davis for proofreading almost all these versions.

References

Abizadeh, Arash. 2008. "Democratic Theory and Border Coercion: No Right to Unilaterally Control Your Own Borders." *Political Theory* 36 (1): 37–65.

———. 2010. "Democratic Legitimacy and State Coercion: A Reply to David Miller." *Political Theory* 38 (1): 121–130.

Allen, Anita L. 1988. Uneasy Access: Privacy for Women in a Free Society. Totawa, NJölev: Rowman & Littlefield.

———. 1999. "Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm." *Connecticut Law Review* 32: 861–875.

Auseyushkin, Yan, and Andrew Roth. 2020. "Will Knocking Belarus Offline Save President from Protests?" *The Guardian*, August 11, 2020, sec. World news. https://www.theguardian.com/world/2020/aug/11/belarus-president-cuts-off-internet-amid-widespread-protests.

Barocas, Solon, and Helen Nissenbaum. 2014. "Big Data's End Run around Anonymity and Consent," in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, ed. Julia Lane, Stefan Bender, Victoria Stodden, and Helen Nissenbaum, 44–75. New York: Cambridge University Press.

BBC. 2014. "Thomas Hitzlsperger: Former Aston Villa Player Reveals He Is Gay." BBC Sport. January 8, 2014. https://www.bbc.co.uk/sport/football/25628806.

Berlin, Isaiah. 1958. "Two Concepts of Liberty," in *Liberty*, ed. Henry Hardy, 166–217. New York: Oxford University Press 2002.

Biography.com Editors. 2018. "Tarana Burke Biography." The Biography.Com Website. 2018. https://www.biography.com/activist/tarana-burke.

Christman, John. 2020. "Autonomy in Moral and Political Philosophy," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Fall 2020. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/.

Davis, Steven. 2009. "Is There a Right to Privacy?" *Pacific Philosophical Quarterly* 90 (4): 450–475.

Farber, Daniel A. 1993. “Book Review: Privacy, Intimacy, and Isolation by Julie C. Inness.” *Constitutional Commentary* 510 (10): 510–519.

Fried, Charles. 1968. “Privacy [A Moral Analysis],” in *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand David Schoeman, 203–223. Cambridge: Cambridge University Press, 1984.

Garcia, Sandra E. 2017. “The Woman Who Created #MeToo Long Before Hashtags.” *The New York Times*, October 20, 2017, sec. U.S. https://www.nytimes.com/2017/10/20/us/me-too-movement-tarana-burke.html.

Gavison, Ruth. 1980. “Privacy and the Limits of Law.” *The Yale Law Journal* 89 (3): 421–471.

Hoven, Jeroen van den. 2008. “Information Technology, Privacy, and the Protection of Personal Data,” in *Information Technology and Moral Philosophy*, ed. Jeroen van den Hoven and John Weckert, 301–21. Cambridge, UK: Cambridge University Press.

Inness, Julie. 1992. Privacy, Intimacy, and Isolation. New York: Oxford University Press.

Lundgren, Björn. 2020. “A Dilemma for Privacy as Control.” *The Journal of Ethics* 24 (2): 165–175. https://doi.org/10.1007/s10892-019-09316-z.

Macnish, Kevin. 2018. “Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World.” *Journal of Applied Philosophy* 35 (2): 417–432. https://doi.org/10.1111/japp.12219.

Mainz, Jakob Thrane, and Rasmus Uhrenfeldt. 2020. “Too Much Info: Data Surveillance and Reasons to Favor the Control Account of the Right to Privacy.” *Res Publica*. https://doi.org/10.1007/s11158-020-09473-1.

Makhovsky, Andrei, and Tom Balmforth. 2020. “Internet Blackout in Belarus Leaves Protesters in the Dark.” *Reuters*, August 11, 2020. https://www.reuters.com/article/us-belarus-election-internet-idUSKCN2571Q4.

Marmor, Andrei. 2015. “What Is the Right to Privacy?” *Philosophy & Public Affairs* 43 (1): 3–26.

Matheson, David. 2007. “Unknowableness and Informational Privacy.” *Journal of Philosophical Research* 32: 251–267.

Matthews, Steve. 2008. “Privacy, Separation, and Control.” *The Monist* 91 (1): 130–150. https://doi.org/10.5840/monist200891116.

McKenna, Michael, and D. Justin Coates. 2020. “Compatibilism,” in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Spring 2020. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/spr2020/entries/compatibilism/.

Menges, Leonhard. 2020a. “A Defense of Privacy as Control.” *The Journal of Ethics*. https://doi.org/10.1007/s10892-020-09351-1.

———. 2020b. “Did the NSA and GCHQ Diminish Our Privacy? What the Control Account Should Say.” *Moral Philosophy and Politics* 7 (1): 29–48. https://doi.org/10.1515/mopp-2019-0063.

Miller, David. 2010. “Why Immigration Controls Are Not Coercive: A Reply to Arash Abizadeh.” *Political Theory* 38 (1): 111–120.

Mokrosinska, Dorota. 2018. “Privacy and Autonomy: On Some Misconceptions Concerning the Political Dimensions of Privacy.” *Law and Philosophy* 37 (2): 117–

143. https://doi.org/10.1007/s10982-017-9307-3.
Moore, Adam. 2008. “Defining Privacy.” *Journal of Social Philosophy* 39 (3): 411–428.
———. 2010. Privacy Rights: Moral and Legal Foundations. University Park: The Pennsylvania State University Press.
Nissenbaum, Helen. 2004. “Privacy as Contextual Integrity.” *Washington Law Review* 79 (1): 119–158.
———. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press.
Parent, W. A. 1983a. “Privacy, Morality, and the Law.” *Philosophy and Public Affairs* 12 (4): 269–288.
———. 1983b. “Recent Work on the Concept of Privacy.” *American Philosophical Quarterly* 20 (4): 341–355.
Parker, Richard B. 1974. “A Definition of Privacy.” *Rutgers Law Review* 27 (2): 275–97.
Rachels, James. 1975. “Why Privacy Is Important.” *Philosophy & Public Affairs* 4 (4): 323–333.
Raz, Joseph. 1988. The Morality of Freedom. New York: Oxford University Press.
Rickless, Samuel C. 2007. “The Right to Privacy Unveiled.” *San Diego Law Review* 44 (1): 773–799.
Robb, David. 2020. “Moral Responsibility and the Principle of Alternative Possibilities,” in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Fall 2020. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/fall2020/entries/alternative-possibilities/.
Rössler, Beate. 2004. The Value of Privacy. Cambridge, UK: Polity Press.
Sartorio, Carolina. 2016. “Frankfurt-Style Examples,” in *The Routledge Companion to Free Will*, ed. Kevin Timpe, Meghan Griffith, and Neil Levy, 179–190. New York: Routledge.
Solove, Daniel J. 2008. Understanding Privacy. Harvard University Press.
Thomson, Judith Jarvis. 1975. “The Right to Privacy.” *Philosophy & Public Affairs* 4 (4): 295–314.