



# Why ‘Negative Control’ is a Dead End: A Reply to Mainz and Uhrenfeldt

Lauritz Aastrup Munch<sup>1</sup>

Accepted: 4 March 2021 / Published online: 25 March 2021  
© The Author(s), under exclusive licence to Springer Nature B.V. 2021

## Abstract

Mainz and Uhrenfeldt have recently claimed that a violation of the right to privacy can be defined successfully under reliance on the notion of ‘Negative Control’. In this reply, I show that ‘Negative Control’ is unrelated to privacy right violations. It follows that control theorists have yet to put forth a successful normative account of privacy.

**Keywords** Right to privacy · Negative control · Consent · Control account · Access account

## Introduction

In a recent paper published in this journal, Jakob Mainz and Rasmus Uhrenfeldt (2020) mount a defense of the so-called ‘control account’ of the right to privacy. Taking inspiration from the literatures on the concept of freedom, they persuasively show that the notion of ‘control’ can be disambiguated and that the control account comes out on top if the notion of control is conceptualized as what they term ‘negative’ control. This move, Mainz and Uhrenfeldt submit, enables proponents of the control account to reply successfully to Thomson’s famous objection to their favored account and, importantly, enables the control account to capture cases that intuitively involve violations of privacy but cannot be captured by the rival ‘access’ account. The rivalry between access and control accounts of the right to privacy is a long-standing one in the literature, and Mainz and Uhrenfeldt’s contribution is very welcome as it seeks to offer a novel argument that both fends off a number of

---

Thanks go to two anonymous reviewers from *Res Publica* for helpful comments and suggestions. I also thank Andreas Bengtson for written comments on a previous version of this manuscript as well as Jakob Thrane Mainz for recurrent discussion of the topic of this reply and related questions.

---

✉ Lauritz Aastrup Munch  
laumu@ps.au.dk

<sup>1</sup> Department of Political Science and Government, Aarhus University, Aarhus, Denmark

prominent objections posed against the control account as well as gives us a strong reason to prefer it over access accounts.

In this reply, I aim to show that a loss of ‘negative control’ as Mainz and Uhrenfeldt define the term cannot provide a necessary condition for a violation of the right to privacy. Since a loss of negative control is not necessary for a violation of the right to privacy, the control theorists still owe us a compelling control-based normative account of privacy and an explanation of in what sense privacy violations involve a loss of control. By contrast, I suggest that access accounts appear well-positioned to steer clear of the objection I pose which gives us a new reason to favor access over control accounts. I end the reply by suggesting that privacy right violations might involve what I term ‘normative control’, but that this kind of control is unlikely to vindicate the claims that the control theorists seek to establish.

‘[A counterexample](#)’ section briefly restates Mainz and Uhrenfeldt’s position and provides my main objection. ‘[Wider implications](#)’ section lays out the upshots of my argument and ‘[Conclusion](#)’ section concludes briefly.

## A Counterexample

According to any control account of privacy rights violations, such violations necessarily involve a loss of some sort of ‘control’. This sets such accounts apart from so-called ‘access’ accounts that maintain that what is essential to privacy violations is that they involve some form of ‘access’. Mainz and Uhrenfeldt’s (p. 12) favored version of the control account goes as follows:

**The Control Account:** For any agent A to have her right to privacy violated, there is a necessary and sufficient condition that must be satisfied: agent A has involuntarily lost Negative Control over the access to personal information P about agent A, due to action(s) of agent B, for which B is responsible.

The control account aims to provide the necessary and sufficient condition for a violation of a privacy right. The full definition is dense, but for current purposes we should focus our attention on the notion of ‘negative control’ and how it is invoked in their argument. Mainz and Uhrenfeldt define ‘negative control’ as follows (p. 7):

**Negative Control:** Agent A enjoys Negative Control over access to relevant information P, if, and only if, A is capable of preventing agent B, who attempts to access, from accessing P.

The notion of negative control is supposed to indicate the specific sense in which violations of privacy involve a loss of (some kind of) control (over information). Specifically, Mainz and Uhrenfeldt focus on a case in which some agent (B) attempts to access a piece of information and another agent, A, is *unable* to prevent B from successfully completing his endeavor. In such cases, there is a loss of negative control, the kind of loss that is necessary and sufficient for a violation of privacy according to Mainz and Uhrenfeldt.

One attractive feature of their view is that it seemingly avoids Thomson's (1975) influential counterexample to the control account of privacy violations, which runs as follows:

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

Typically, Thomson's example is taken as an unattractive implication of certain variants of the control account. The reason is that, as Thomson herself states, we would not want to say that somebody's right to privacy has been violated before someone trains the device on somebody's privacy-relevant object. Control accounts that measure out control (only) as a function of other people's ability to access relevant information are vulnerable to this objection, and so the notion of control must be weakened in order not to have this implication.<sup>1</sup> The concept of negative control is supposed to provide this weaker notion of control and is also supposed to demonstrate in just what sense privacy right violations involve a loss of control. This is achieved by introducing a further necessary condition according to which negative control exists or can be lost *only if* some person actually attempts access.

*Pace* Mainz and Uhrenfeldt, I maintain that a loss of negative control is not a necessary condition for a violation of privacy rights.<sup>2</sup> Consider first the following case, meant to illustrate the attractiveness of Mainz and Uhrenfeldt's control account—a case in which privacy is intuitively violated:

**Wiretapping** Smith and Jones are neighbors. Unbeknownst to Jones, Smith wiretaps Jones's telephone, using a fancy device which allows Smith to listen in on Jones's conversations without violating Jones's property rights. As

<sup>1</sup> Mainz and Uhrenfeldt define this 'too demanding' notion of control as 'Republican Control: Agent A enjoys Republican Control if, and only if, agent B does not have the ability to get access to relevant information P about A' (p. 7).

<sup>2</sup> There is a further worry about their notion of 'Negative Control' that I only mention in passing. In order to avoid Thomson's counterexample, Mainz and Uhrenfeldt maintain that negative control is only something an agent, A, possesses when it is true that (1) A is capable of preventing B from accessing some piece of information and (2) *B attempts to access this piece of information*. It is clause ii that distinguishes negative control from republican control. However, the restricted kind of control that is negative control in comparison to republican control is puzzling. It is puzzling, *first*, because it seems to be a kind of control that exists *only when* B attempts to access a piece of information (if control were lost before B attempts to access, perhaps due to B having the ability to access, negative control collapses into republican control). A lacks negative control when B does not attempt to access some piece of information, since a necessary condition (clause ii) for having negative control does not obtain. This implication leaves one wondering why B does not act objectionably *when not attempting access*, since such act-omissions deprive A of negative control (and the instantiated loss of control seems to be part of what makes violations of privacy rights morally objectionable). *Secondly*, and briefly, the fact that negative control only exists when somebody attempts access leaves one wondering just what kind of physical property negative control is and how it differs from republican control in a meaningful way.

it happens, Jones is on vacation for several months, and therefore does not use the telephone in that time period. (p. 13)

Wiretapping is meant to showcase how their control account fares better in comparison to the rival access account of privacy violations. What sets these accounts apart according to Mainz and Uhrenfeldt is that the latter requires that information is *actually accessed*. Mainz and Uhrenfeldt claim that there is not ‘actual access’ to Jones’s personal information, and thus that the access account cannot identify a violation of the right to privacy. This speaks against the access account as it seems intuitively right that there is a violation of privacy in Wiretapping. However, as Mainz and Uhrenfeldt maintain, ‘Jones has lost negative control over the access, since Smith can now listen to Jones’s telephone conversations’ (p. 13). Hence, a control account based on the notion of negative control can identify the sense in which Wiretapping involves a loss of control and explain why Smith’s conduct is morally objectionable.

I now offer a counterexample purporting to show that a loss of negative control is *not necessary* for a violation of the right to privacy. Consider:

**Wiretapping #2.** Smith and Jones are neighbors. Smith wiretaps Jones’s telephone, using a fancy device which allows Smith to listen in on Jones’s conversations without violating Jones’s property rights. Unbeknownst to Smith, Jones has an even fancier device enabling him to both monitor the extent to which he is being subjected to wiretapping and shut down the tapping at the mere push of a button. Jones does *not*, however, deploy his device to prevent Smith’s plan.

In this case, it also seems intuitively right to say that Smith violates Jones’s right to privacy.<sup>3</sup> However, at no point is Smith rendered incapable of *controlling* Jones’s access via wiretapping. Smith just does not act in order to prevent it. If Wiretapping #2 involves a violation of privacy rights, then a loss of negative control is not a necessary condition for a privacy rights violation.

Mainz and Uhrenfeldt might respond by maintaining that Wiretapping #2 does not involve a violation of Jones’s right to privacy. However, I fail to see how this response could be rendered compelling. By analogous reasoning, we normally think

<sup>3</sup> An anonymous reviewer objects that this response presupposes endorsing the view that the *function* of privacy rights is not only securing a kind of control but also, say, protecting against various harms. The reviewer might be right in one sense. I am, for one, sympathetic to the view that the underlying *function* of some right has a bearing on how it should be defined (these are distinct questions). Note, however, that many commentators endorse the view that the *function* of privacy rights is broader than securing a kind of control (see for instance Parent 1983). Hence, for this objection to work, one must show why such widely endorsed views on the *function* of privacy rights are mistaken. I thank the reviewer for raising this objection.

that an assaulter violates an assaultee's rights, even if the assaultee is perfectly able to fend off the assaulter. While it might be prudent of the assaultee (Jones might be likened to an assaultee) to defend himself, a failure to engage in self-defense when one has the ability to successfully do so does not make it the case that the assaulter does not violate the assaultee's rights.<sup>4</sup>

Instead, Mainz and Uhrenfeldt might retort that, since Jones does not push the button to fend off the wiretapping, this reveals that Jones actually wanted to be wiretapped and so Smith violates no rights as he acts in accordance with Jones's will. If there is no violation of privacy in Wiretapping #2, in turn, there is no reason to think that Mainz and Uhrenfeldt fail in providing a necessary condition for a violation of privacy. This response might raise a much broader question about whether consent-based permissions are best understood as a form of communication or as an act of the will, which I cannot pursue presently.<sup>5</sup> However, for current purposes it seems enough to say that it strikes me as unpersuasive to infer from Jones's inaction that he *necessarily* wanted the wiretapping to happen, as we can imagine several reasons why Jones did in fact not act even though he had the ability to do so.<sup>6</sup>

## Wider Implications

Where does this objection leave us? It leaves us with the result that the notion of negative control does not provide a necessary condition for a violation of a privacy right. More generally, my objection shows that the control account might still be in bad standing compared to the access account. The *pro tanto* reason that Mainz and Uhrenfeldt offer for favoring their version of the control account—to wit, that it succeeds in explaining their Wiretapping case and that it avoids Thomson's objection—might very well be outweighed by the fact that it fails to capture other important cases such as Wiretapping #2. On this wider question, Mainz and Uhrenfeldt write that none of the examples or thought experiments provided by the access theorists in the literature so far seem to count decisively in favor of the AA [access account, red.] like Wiretapping counts decisively in favor of the CA [control account, red.]. We cannot think of an example, which stacks the deck of cards in favor of

<sup>4</sup> An anonymous reviewer objects that having the intuition that Wiretapping #2 involves a violation of privacy *presupposes* endorsing the access account of privacy. I do not think this is the case. As the parallel to the self-defense case also illustrates, the intuition pumped in Wiretapping #2 seems to reflect the general fact that we would not want to say that neither wiretapping nor assault (nor any other conduct that typically is taken to violate our rights) is rendered permissible just because the right-holders are capable of preventing such offenses and fail to act to prevent them. Cf. for instance Thomson (1975, p. 300) making a similar point in discussing the permissibility of X-raying people's property: 'Suppose that there was a way in which he could have protected his picture against the action of the [X-ray] device (...) The fact he didn't do this does not make it all right for us to have used the device'. I thank the reviewer for raising this objection.

<sup>5</sup> For a great overview and a compelling argument in favor of the view that consent requires communication, see Bolinger (2019).

<sup>6</sup> Furthermore, we can unproblematically assume that there is no tacit consent present and that Smith does not gain a permission from a successfully inferred or hypothetical consent.

the AA, so we invite the access theorists to provide such an example (p. 14). As argued above, Wiretapping #2 casts doubt on the claim that Mainz and Uhrenfeldt have identified a necessary condition for a violation of privacy with their conception of negative control and thereby puts renewed pressure on the control account of privacy rights. However, is it plausible to think that the rival access account can accommodate cases such as Wiretapping #2? While a full answer to this question is beyond what can be achieved within this reply, the access account *seems* particularly well-suited to make sense of the idea that Wiretapping #2 involves a violation of privacy. The reason is that, although there is no loss of negative control in this case, there certainly is *actual access* to whatever information happens to be present on Jones's telephone line in Wiretapping #2.<sup>7</sup> It seems, then, that access accounts are particularly well-equipped to deal with cases in which the negative control-based control account fails to align with intuitions.

If republican control identifies too strong a form of control, and negative control appears irrelevant, in what sense might it be true that privacy right violations involve 'control'? Here is a possibility: violations of the right to privacy (as with, I suspect, any other waivable right) might involve what we can call *normative control*.<sup>8</sup> Normative control is not control over any property of the natural, physical world (call this 'non-normative control'). Rather, it is a form of control that we have over the normative relations we have to other people. Specifically, the kind of control that is involved in cases such as Wiretapping and Wiretapping #2 might be the fact that Jones has the moral power to decide whether Smith's conduct wrongs him.<sup>9</sup> Note that this kind of control is unaffected by Smith's conduct or abilities. In turn, this normative control simply reflects our commitment to the thought that Smith's conduct wrongs Jones unless Jones beforehand alters the moral landscape by giving Smith permission to tap the wire. While normative control is a type of 'control', normative control is unlikely to vindicate the claims that the control theorists want to make, since the kind of control that the control theorists are after seems to be a form of non-normative control that is present in cases that specifically involve violations of privacy rights. However, normative control is a perfectly general relation that is likely to be present in any rights-based relationship where the right in question is waivable.

<sup>7</sup> I do not want to defend this further result here, but I suspect that it is possible to even interpret the original Wiretapping in a way that shows that there is 'actual access' to information—if nothing else, the piece of information that no phone conversation is currently happening. Hence, suitably interpreted, it seems false to me that there is no 'actual access' in the first place in Wiretapping.

<sup>8</sup> For discussion of normative control, see Owens (2012).

<sup>9</sup> And typically, Jones can exercise this power by, say, communicating consent to wiretapping.

## Conclusion

Mainz and Uhrenfeldt have recently claimed that a violation of the right to privacy can be defined successfully by reliance on the notion of 'negative control'. In this reply, I have shown that negative control is at best contingently related to privacy rights violations, as an involuntary loss of negative control is not a necessary condition for a violation of privacy. It follows that control theorists have yet to put forth a complete and successful normative account of privacy.

## References

- Bolinger, R. J. 2019. Moral risk and communicating consent. *Philosophy and Public Affairs* 47: 179–207.
- 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>.
- Owens, David. 2012. *Shaping the normative landscape*. Oxford: Oxford University Press.
- Parent, W. A. 1983. Privacy, morality, and the law. *Philosophy & Public Affairs* 12(4): 269–288.
- Thomson, J. J. 1975. The right to privacy. *Philosophy and Public Affairs* 4(4): 295–331.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.