Res Publica (2021) 27:669–674
https://doi.org/10.1007/s11158-020-09495-9

COMMENT

# Confusion and the Role of Intuitions in the Debate on the Conception of the Right to Privacy

**Björn Lundgren**[1,2,3]

Accepted: 28 December 2020 / Published online: 4 March 2021


## Abstract

Recently, Jakob Thraine Mainz and Rasmus Uhrenfeldt defended a control-based conception of a moral right to privacy (Mainz and Uhrenfeldt, *Res Publica*, 2020)—focusing on conceptualizing necessary and jointly sufficient conditions for a privacy right violation. This reply comments on a number of mistakes they make, which have long reverberated through the debate on the conceptions of privacy and the right to privacy and therefore deserve to be corrected. Moreover, the reply provides a sketch of a general response for defending the limited access conception of the right to privacy against control-based intuitions.

**Keywords** Privacy · Right to privacy · Control · Limited access

## Introduction

Recently, Jakob Thraine Mainz and Rasmus Uhrenfeldt defended a control-based conception of a moral right to privacy (Mainz and Uhrenfeldt 2020)—focusing on conceptualizing necessary and jointly sufficient conditions for a privacy right violation. In this reply, I will start by briefly commenting on a number of mistakes they make, which have long reverberated through the debate on the conceptions of privacy and the right to privacy and therefore deserve to be corrected. Next, I will turn to a more important issue: I will address some problems with the main argument of Mainz and Uhrenfeldt. In responding to their argument, which makes use of some common control-based intuitions, I will provide a sketch of a general response for

✉ Björn Lundgren
bjorn.lundgren@umu.se; bjorn.lundgren@iffs.se; bjorn.lundgren@philosophy.su.se

[1] Department of Historical, Philosophical and Religious Studies, Umeå University, Umeå, Sweden

[2] Institute for Futures Studies, Stockholm, Sweden

[3] Department of Philosophy, Stockholm University, Stockholm, Sweden

defending the limited access conception of the right to privacy (i.e., what Mainz and Uhrenfeldt call 'the access account', or 'AA') against control-based intuitions.

## Common Mistakes

There are at least three common mistakes that the arguments in Mainz and Uhrenfeldt suffer from. Although many of these are fairly simple, their common occurrence in the literature makes it worthwhile quickly commenting on them.

First, the arguments in Mainz and Uhrenfeldt include a mild version of a conceptual conflation between the concepts privacy and the right to privacy, mistakenly presuming that their main opponent (Macnish 2018) is talking about *the right to privacy*, although he is talking about privacy (see Lundgren 2020a, p. 169).

While Mainz and Uhrenfelt recognize the possibility of a straw man, the motivation of the illicit presumption is only motivate in a footnote, saying:

> If Macnish did not intend this to be a discussion of privacy *rights*, he should have made that more explicit, and probably abstained from using the word 'violation'. (2020, p. 11, fn. 20)[1]

This is symptomatic of a growing problem in the literature in which it is common to use 'privacy' when one means 'the right to privacy'. Such an example was considered already by Parent (1983, p. 273, fn. 11) and as I note in Lundgren (2020a, p. 166, fn. 2) it is extremely common and likely an effect of the legal discussion on privacy, which is—for good reason—focused on the right to privacy.

It is problematic that we find ourselves in a situation where those using terms correctly are required to be more explicit in stating that they mean something other than what they say (even if it should be recognized that Macnish should have said what he meant by 'privacy violations').

Second, Mainz and Uhrenfeldt make use of a false dichotomy from Moore (2008), between normative and descriptive conceptions of privacy. As Mainz and Uhrenfeldt note, Moore suggests that 'A descriptive account […] describes *a state* or *condition* of privacy while normative accounts refer to moral obligations and rights' (Mainz and Uhrenfeldt 2020, p. 2; cf. Moore 2008, pp. 212–213).

The dichotomy is false since we should either hold that normative conceptions of privacy can define privacy (not the right to privacy), without concern of obligations or right—for example, simply as a value or a good. Alternatively, we should hold that beyond descriptive and normative conceptions of privacy, there could also be axiological conceptions of privacy, which concern the value of privacy.

Moreover, Mainz and Uhrenfeldt further reduce the normative account to an account that supplies necessary and jointly sufficient conditions for '*violations* of the moral *right* to privacy' (2020, p. 2). Although normative requirements for privacy are often discussed under a right-based normative theory, there is no reason

[1] The paper is currently only available online and lacks pagination. Hence, I have introduced a page count, starting from 1.

why we cannot think of privacy obligations on the basis of, for example, consequentialist theories.

Third, Mainz and Uhrenfeldt miss the fact that privacy is the object of the right to privacy, which implies that there has to be an appropriate consistency between how we conceptualize the former and the latter (see Lundgren 2020a). Thus, Mainz and Uhrenfeldt ignore the need to defend their (control-based) conception of privacy against a large set of counter-examples available in the literature.

Of course, Mainz and Uhrenfeldt are not technically analyzing the concept of the right to privacy, but necessary and jointly sufficient conditions for when a right to privacy is violated. Nevertheless, their analysis has conceptual implications for the concept of a right to privacy. Thus, whether the analysis of *privacy right violations* in Mainz and Uhrenfeldt holds cannot be reduced to whether it, for example, manages to avoid any counter-arguments against that conception as such. It also depends on whether an appropriate analysis of *privacy*—relative to the (implied) analysis of *the right to privacy*—can avoid any relevant counter-arguments. The problem of Mainz and Uhrenfeldt is a general problem in the literature for most proponents of a specific analysis of the right to privacy; that is, that potential problems for the associated analysis of privacy are not taken into consideration.

Setting those issues aside I will now turn to the analysis of privacy right violations in Mainz and Uhrenfeldt.

## Examining Mainz and Uhrenfeldt's Conception and Analysis of Privacy Right Violations

In defending a final control-based conception of privacy right violations ('**CA**4'), Mainz and Uhrenfeldt test that conception against an example called 'Wiretapping' (the example is structurally similar to some examples of Thomson 1975). In Wiretapping, Smith wiretaps Jones's telephone. However, because Jones is away (i.e., not using his phone), Smith does not access Jones's private information. Nevertheless, Mainz and Uhrenfeldt argue that Smith violates Jones's right to privacy because Smith's wiretapping causes Jones to lose *negative control* over his private information.[2] Moreover, on their reading of the limited access view, Smith does *not* violate Jones's right to privacy, because he does not actually access Jones's private information. (*N.B.*, Mainz and Uhrenfeldt focus on *informational privacy*; I will follow this limitation even if none of my arguments depend on restricting the discussion to concern only information.)

This test is problematic for at least two reasons. First, the argument depends on us accepting a control-based intuition. Indeed, this is something that proponents of the limited access conception of the right to privacy might—and often do—deny (even if Mainz and Uhrenfeldt strangely have included a control-based condition in the

[2] Mainz and Uhrenfeldt define *negative control* as follows: '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.' (p. 7).

limited access conception).[3] That is, the argument does nothing to convince someone who does not share their control-based intuitions that they are correct. Thus, a proponent of the limited access conception can just deny the example because they normally deny those kinds of intuitions. Indeed, the debate is partly about which intuitions are correct. Supplying a standard example that speaks in favor of control-based intuitions does nothing to move those that do not already share those intuitions. (*N.B.*, this does not imply that there cannot be something *else* wrong about Smith's action of wiretapping Jones's phone.)

However, it is arguably a general problem in the debate on the conceptions of privacy and conceptions of the right to privacy that proponents on each side do not take the other side's intuitions into account. That is, we might think that a proponent of a limited access conception of the right to privacy should take the intuition of Mainz and Uhrenfeldt seriously. Indeed, this seems to be the presumption (although the paper provides no reason for why that is the case; instead it argues that these intuitions are stronger than those in favor of the limited access conception, but that is circular, given that the argument depends on accepting the strength of the intuitions under discussion). Yet in such a situation a proponent of the limited access conception can easily agree with the intuition that Smith has violated Jones's privacy, but deny that the limited access conception cannot explain this. In fact, as I will argue it is Mainz and Uhrenfeldt's control-based conception of the right to privacy (**CA**4) that cannot manage to deal with variants of Wiretapping.

There are different possible routes to explain that Smith violated Jones's right to privacy in Wiretapping. I will limit the discussion to defending what I think is a new solution (see Lundgren *forthcoming*): A proponent of the limited access conception can hold that the right to privacy protects against *substantial risks of access*, not merely *actual access*. That is, while *actual* access to someone's private information might be a necessary criterion for when someone's *privacy* is diminished, it is not clear that we should hold that *actual* access is a necessary criterion for when the *right to privacy* is violated. Formulated this way, the right to privacy protects actions that *substantially risk diminishing privacy*. Although it should be recognized that such a view has—as far as I know—never been defended in print, that is the response I would suggest *if* one takes seriously the intuition that the right to privacy is violated (which we have not been given any reason to do). Moreover, the view

[3] In the paper's final definition of the limited access view—called 'the access account'—it is defined as follows: '**AA**4: For any agent A to have her right to privacy violated there are two each necessary and jointly sufficient conditions that must be satisfied: (1) Agent A has involuntarily lost Negative Control over the access to personal information P about A, *due to the action(s) of agent B, of which B is responsible,* and (2) agent B (or someone else) actually accesses P.' (Mainz and Uhrenfeldt 2020, pp. 12–13).

This is a misunderstanding of the of limited access view. It is not necessary that there is a loss of control (strangely they even quote Macnish saying that control is a neither necessary nor a sufficient condition for privacy—although Macnish talks of privacy, not the right to privacy, Mainz and Uhrenfeldt rely on Macnish to define a limited access conception of privacy right violations). That is, an agent B can violate A's privacy by accessing A's P, even if B (or anyone else) is not in a position to control other's access to P. Although we might deny that access is impossible without also affecting negative control, but if so, the first condition is redundant. (Henceforth, I will set it aside for the purpose of keeping the reply brief.)

could be defended on the basis of a more general idea that people have *a pro tanto* right not to be exposed to risks (see, e.g., Hansson 2003).[4]

More importantly, Mainz and Uhrenfeldt arguably implicitly endorse the idea I presented above. Consider the following argument against the limited access conception:

> Even if the wiretap had randomly malfunctioned unbeknownst to Smith, so Smith did not get access to the information that Jones did not use the telephone, Smith would clearly still have violated Jones's right to privacy. (2020, p. 13)

However, even if we agree that Smith violated Jones's right to privacy, it is questionable if that is true according to Mainz and Uhrenfeldt's definition of a privacy violation. Imagine a case in which Smith is prevented from accessing Jones's phone not because of a malfunctioning device, but because Jones has a machine to prevent wiretapping. In this case, Jones retains *negative control* of his private information. However, we may still want to claim—as in Mainz and Uhrenfeldt—that Smith has violated Jones's right to privacy. While such a view is consistent and defendable, it is not compatible with the analysis of privacy violations in Mainz and Uhrenfeldt because Jones still has negative control (i.e., there is no violation according to **CA**4). Alternatively, if we want to maintain that Smith violates Jones's right to privacy in the above examples, we could say that the *attempted access* is a privacy right violation because it put the access to Jones's private information at serious risk.

To sum up: In a situation such that B is attempting to violate A's right to privacy, it seems reasonable to think that B can violate A's right to privacy, even if B fails to affect A's privacy (i.e., access A's private information). That is, we might think that the right to privacy does not only protect against *actually* diminishing someone's privacy, but also against attempts to diminish someone's privacy (i.e., attempted access to their private information). Alternatively, if we deny the intuition that Smith violated Joe's right to privacy, we could say that Smith attempted, but failed, to violate Jones's right to privacy. That is not to say that Smith has done nothing wrong, since we might think that attempted privacy violations are wrong (just as we think that attempted murder is wrong) and that it is closely related to the right to privacy (just as the right to life morally protects us both against murder and attempted murder).

This issue arguably requires further discussion, but the point here is that Mainz and Uhrenfeldt's Wiretapping case does not present a *pro tanto* reason to favor the control-based conception of the right to privacy. This is because we can either deny their intuitions that Jones's right to privacy was violated, or we can accept the intuition. If we deny the intuition, then the argument does not move the debate, but if we accept the intuition, then it seems that their analysis of privacy right violations fails.

[4] Hansson actually calls the right *prima facie*, following a common usage of the term in moral philosophy due to W. D. Ross. However, *prima facie* is an epistemic condition and what Hansson describes is a right that can be overridden under various conditions (i.e., 'Exposure of a person to a risk is acceptable if and only if this exposure is part of an equitable social system of risk-taking that works to her advantage'; Hansson 2003, p. 305). Thus, it is more appropriate to refer to it as a *pro tanto* right. I have made this argument previously (see Lundgren 2020b, p. 229, fn. 39; cf. also Kagan 1989).

**Acknowledgements** I want to thank Kevin Macnish for comments prior to submission.

**Funding** Open Access funding provided by Umea University. This work was partially supported by the *Wallenberg AI, Autonomous Systems and Software Program—Humanities and Society* (WASP-HS) funded by the *Marianne and Marcus Wallenberg Foundation* and the *Marcus and Amalia Wallenberg Foundation* (grant number: MMW 2018.0116). Open Access funding provided by *Umeå University.*



## References

Hansson, S.O. 2003. Ethical Criteria of Risk Acceptance. *Erkenntnis* 59 (3): 291–309. https://doi.org/10.1023/a:1026005915919.

Kagan, S. 1989. *The Limits of Morality*. Oxford: Clarendon Press.

Lundgren, B. 2020a. A Dilemma for Privacy as Control. *Journal of Ethics* 24: 165–175. https://doi.org/10.1007/s10892-019-09316-z.

Lundgren, B. 2020b. Against AI-improved Personal Memory. In *Aging Between Participation and Simulation: Ethical Dimensions of Socially Assistive Technologies in Elderly Care*, ed. J. Haltaufderheide, J. Hovemann and J. Vollmann, 223–234. https://doi.org/10.1515/9783110677485-014.

Lundgren, B. *Forthcoming*. How we can make sense of *control*-based intuitions for *limited access*-conceptions of the right to privacy. *Journal of Ethics and Social Philosophy.*

Macnish, K. 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, J.T., and R. 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.

Moore, A.D. 2008. Defining Privacy. *Journal of Social Philosophy* 39 (3): 411–428. https://doi.org/10.1111/j.1467-9833.2008.00433.x.

Parent, W.A. 1983. Privacy, Morality, and the Law. *Philosophy & Public Affairs* 12 (4): 269–288. https://www.jstor.org/stable/2265374.

Thomson, J.J. 1975. The Right to Privacy. *Philosophy & Public Affairs* 4 (4): 295–314. https://www.jstor.org/stable/2265075.