Journal of Applied Philosophy, Vol. 35, No. 2, May 2018
doi: 10.1111/japp.12219

Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World

KEVIN MACNISH

ABSTRACT *There is a long-running debate as to whether privacy is a matter of control or access. This has become more important following revelations made by Edward Snowden in 2013 regarding the collection of vast swathes of data from the Internet by signals intelligence agencies such as NSA and GCHQ. The nature of this collection is such that if the control account is correct then there has been a significant invasion of people's privacy. If, though, the access account is correct then there has not been an invasion of privacy on the scale suggested by the control account.*

I argue that the control account of privacy is mistaken. However, the consequences of this are not that the seizing control of personal information is unproblematic. I argue that the control account, while mistaken, seems plausible for two reasons. The first is that a loss of control over my information entails harm to the rights and interests that privacy protects. The second is that a loss of control over my information increases the risk that my information will be accessed and that my privacy will be violated. Seizing control of another's information is therefore harmful, even though it may not entail a violation of privacy. Indeed, seizing control of another's information may be more harmful than actually violating their privacy.

1. Introduction: The Need to Define Privacy

There has been a debate regarding the definition of privacy in philosophical literature since the early 1970s. Among competing definitions are two particularly popular accounts which view privacy respectively as a matter of control or a matter of access. On one side are those who argue that a loss of control over one's information constitutes a loss of privacy. On the opposing side are those who feel that a loss of privacy only occurs when one's information is actually accessed. Within both academic and popular literature the control account appears to have gained the upper hand in this debate.[1]

While these two accounts are the most popular, and strike both myself and others as the most convincing,[2] there are others. These include the right to be let alone, secrecy, personhood, intimacy, and a Wittgensteinian approach of family resemblance.[3] This article does not set out to provide a single definition of privacy but rather contributes to one aspect of the debate, considering just the control and access accounts. I argue that the control account does not capture significant aspects of what is meant by privacy, demonstrating that privacy and control can come apart. Hence control is neither necessary nor sufficient for privacy. By contrast, privacy and access do *not* come apart. As such, I hold that the access account is preferable to the control account.

Does this debate even matter, though? Anita Allen, Daniel Solove and Annabelle Lever have all expressed some scepticism about the need to agree a firm definition of privacy in order to advance privacy concerns in policy and law.[4] However, these views were made prior to the revelations of Edward Snowden in 2013 regarding the collection of Internet and mobile phone information of the population of the UK and the US by their own intelligence agencies, NSA and GCHQ. This information appears to have been collected in bulk, to be searched by analysts for intelligence-worthy data. In response, Tim Berners-Lee and US Senator Rand Paul have each referred to this activity as breaching or invading privacy,[5] while the Court of Justice of the European Union expressed the opinion that the 'safe harbour' agreement permitting the transfer of data from the EU to the US allowed for state access to private information, entailing a compromise of the right to privacy.[6]

In response to these and other criticisms of mass invasions of privacy, then NSA Director Keith Alexander said of two NSA programs that their 'disciplined operation ... protects the privacy and civil liberties of the American people'.[7] Similarly, when Steven Levy interviewed NSA officials in 2013 he concluded that 'looking at the world through [NSA's] eyes, there is no privacy threat in collecting massive amounts of information'.[8]

There is therefore a significant disconnect between those who see the actions of NSA and GCHQ in collecting but not reading people's email and phone records as a massive invasion of privacy and those who do not. On the surface at least, it appears that each side is working with a different definition of privacy. Those who see the collection of this information as privacy-invasive adopt the control approach: in taking control of the information, NSA has invaded people's privacy. Those who do not see the collection of the information as privacy-invasive adopt the access approach: no invasion of privacy occurs unless the information is actually accessed.

The debate regarding the definition of privacy has therefore taken on greater significance in light of the Snowden revelations. If the control account is correct then these revelations demonstrate that there has been a vast invasion of people's privacy. If the access account is correct then, while there has been an invasion of privacy in the cases of data actually accessed by intelligence analysts, this activity is not the vast invasion of privacy suggested by the control account.

As noted, I argue that the control account of privacy is mistaken. However, the consequences of this are not that the seizing control of information is unproblematic. I argue that the control account seems plausible for two reasons. The first recognises that privacy draws some of its value from protecting other rights and interests, particularly the right to security. A loss of control over my information harms these other rights. When a person seizes control of my information, irrespective of whether they access that information, I *feel* vulnerable. At the same time, when I hand over control of my information to another I make an active choice to favour some interest other than privacy (e.g. intimacy, security, or some other interest). The second reason why the control account seems plausible relates to issues of risk. Here, I draw on the work of Hélène Hermansson and Sven Ove Hansson, and a refinement by Jonathan Wolff, to demonstrate that a loss of control entails an increased risk to both my privacy and these other rights. The fact that I no longer control my information entails an increased risk that my information will be accessed by the new controller of that information, which will involve a violation of my privacy. The consequence of this is that, in the absence of knowledge whether my privacy actually *has* been violated, it is prudent for me to act as if it has. Bringing these two reasons together entails that I not only *feel* vulnerable, but that I am vulnerable. This has serious consequences for both the individual and society.

My conclusion is that while a loss of control over one's information does not entail a violation of privacy, it does entail a violation of the rights that privacy protects and therefore feels similar, and that there is an increased risk of my privacy being violated. Furthermore, even though there has not been a violation of privacy in these cases, there is nonetheless harm. Indeed, this harm could be greater than that entailed by an actual violation of privacy.

The value of this approach is that it responds to the problems which arise through the actions of NSA and GCHQ without having to defend a flawed definition of privacy. Through accepting the same definition of privacy as that employed by defenders of these actions it can be demonstrated that those actions are problematic even if they do not involve a violation of privacy.

As a final note regarding the content of privacy, I agree with Adam Moore, George Panichas and Tony Doyle[9] and contrary to Alan Westin and William Parent[10] that privacy need not focus on information. Moore, drawing on Thomson,[11] and Doyle[12] both provide compelling accounts which demonstrate that privacy can be at least an aspect of space (as in, private space) as well as of information. That said, it is information that is most frequently at stake in discussions on privacy and government surveillance. Furthermore, the motivation for this article has been the Snowden revelations discussed above which concern almost purely information. However, the same arguments that I present below regarding privacy of information hold equally well for physical or locational privacy. In short, if you do not access my personal space then I have experienced no loss of privacy in that regard, irrespective of who is controlling that space.

2. Privacy as Control or Access

2.1. Privacy as Control

Leading accounts of privacy currently propose or assume that privacy entails control. If I lose control over my information, these hold, then I have lost (a degree of) privacy. This is held by a number of significant thinkers.[13] Paul Schwartz has referred to the level of support for this control account as 'staggering'.[14] However, it is Julie Inness who has defined and defended this position the most thoroughly. She holds that privacy is 'a variety of freedom, a freedom that functions by granting the individual *control* over the division between the public and the private with respect to certain aspects of her life' [my emphasis].[15]

Inness argues that the control account of privacy accords better with our ordinary language and intuitions than the access account (which she labels the separation account). She points out that the access account takes a morally neutral stance on privacy which does not accord with ordinary usage. Secondly, she argues that the access account is necessarily individualistic. Thirdly, she holds that according to the access account, many apparent violations of privacy are in fact only threatened violations.

In defending the access account I shall respond to each of Inness' challenges to this approach. Before I do, though, I acknowledge that there is an intuitive strength to the control account. If, for instance, you steal my diary then I might well feel violated. We can remove the element of theft if we imagine that I leave my diary on a table in a coffee shop and return to that shop 30 minutes later to retrieve it. When I enter the shop I see a stranger with my diary on her table, a different table from the one at which I was sitting. I therefore know that she, or someone, has moved my diary; but have they read it? I have not been in control of my diary for half an hour, in which time anything might have happened to it. Again, I am likely to feel violated. There are strong feelings which accompany a loss of control such as Inness and others describe. However, I will argue, to associate these feelings with a violation of privacy is a mistake.

2.2. Privacy as Access

In contrast to the control account, the access account holds that information needs to be accessed for there to be an actual violation of privacy. This position is held by Judith Thomson, Ruth Gavison, Sissela Bok, Anita Allen, Hyman Gross, Ernest Van Den Haag, Herman Tavani and James Moor.[16] Thomson argues that a blind spy and a deaf spy who access your information through hearing and reading respectively, 'violate your right to privacy'.[17] Tavani and Moor take the similar view that 'privacy is fundamentally about protection from intrusion and information gathering by others'.[18] Allen's view is that 'anonymity, confidentiality, reserve, and secrecy – not merely having the choice to bring these about – are forms of privacy'.[19]

Despite its relative unpopularity, I believe that the access account is correct. This can be illustrated through returning to the diary example. Imagine that I have returned to the coffee shop after a 30-minute interval to find my diary on a stranger's table. It is unopened. I panic for a moment, but on seeing me the stranger smiles and hands me the book. She explains that she has not opened it, but saw me leave without it and collected it to await my return. She knows how intimate her own diary is, so she respected my privacy and kept it shut, as well as making sure that no one else would be able to read it. I feel an enormous sense of relief, thank her and leave with my dignity intact.

In this case, I do not think that my privacy has been lessened. When I see my diary in another's possession, I fear that my privacy has been violated, and indeed it might have been. However, as long as the diary is not actually opened and read no reduction in privacy has occurred. Note that this is true even though the diary was not under my control for 30 minutes.

By extension, I suggest that if the government collects but does not access my information then there is no privacy violation. Nonetheless, in this case harm has occurred, the nature of which I shall elaborate. Importantly, though, the harm is not a matter of privacy. Losing control in this way is unquestionably problematic, but it is not a privacy issue. However, the harm may be one of greater magnitude than a 'mere' privacy violation.

2.3. Defending Privacy as Access

What of Inness' three arguments against the access account? She claimed that this approach (1) treated privacy as morally neutral, contrary to popular usage; (2) was necessarily individualistic; and (3) treated apparent violations of privacy as only threatened violations. Taking these in turn, I accept that in ordinary language we do treat privacy as valuable. Inness points out that we talk of 'enjoying our privacy,' which suggests value. She argues that cases in which a person has privacy forced upon them, for example through being shipwrecked on a desert island, have to be described by proponents of the access account as cases of 'undesirable privacy'. Yet one struggles to imagine Robinson Crusoe rushing to the first person he has seen in years and thanking him for relieving his privacy.[20]

In making this claim about enforced privacy through the Crusoe example, though, Inness makes the incorrect assumption that privacy involves any and all information about a person. This is clear when she states that, according to the access account, 'as soon as one individual encounters another, no matter the nature of the encounter, privacy is necessary lost'.[21] Yet this is obviously mistaken: privacy does not concern *any* information about me. When Crusoe's rescuer sees that Crusoe has grown a beard, this is not a violation of Crusoe's privacy, just as it is not a violation of my privacy if we meet for the first time and you discover that I wear glasses. This is a straw man version of the access account which does not hold that *all* information is subject to privacy concerns, something which is equally true of control-based accounts. Inness recognises this in her discussion of the latter when she states that, 'control-based definitions of privacy function by giving the individual control over *a certain area* of her own life' [my italics] and again that 'it is the *intimacy* of this information that identifies a loss of privacy'.[22] What is good for the goose is good for the gander, and it seems as if Inness is allowing a limited scope for the content of privacy in the control-based account, but an unlimited scope in the access-based account. This would be acceptable if she gave a reason for this discrepancy, but she does not. As such, she is using a definition of the content of privacy for the access-based approach which she neither could, nor would want to, defend from the perspective of the control-based approach.

Inness continues that privacy is not a morally neutral concept, as held by the access account. She states that 'both our privacy intuitions and linguistic usage support the 'valued' nature of privacy'.[23] The obvious response is to point out that privacy is not a good *simpliciter* as it enables people to 'commit robberies and beat their spouses'.[24] Inness forestalls this objection by stating that it 'conflates the value of privacy with the value of the actions performed under its protection'.[25] However, by seeing privacy as always positively valued it follows that surrendering any privacy, whether understood by the control or access account, is wrong. Yet, as I shall argue, surrendering privacy is a key aspect of intimacy and therefore the loss of privacy may also be valuable.

Inness' second argument against access accounts is that they are necessarily individualistic, as they 'make shared privacy impossible'.[26] She gives examples of inviting a close friend into her house, initiating mutual sexual activity with another, and allowing a trusted friend to read a personal letter. In these cases, she says, she would not thank the other person for lessening her privacy. Rather, she would talk about 'including another within [her] realm of privacy',[27] arguing that in none of these cases is there a loss of privacy but rather a shared intimacy. She goes on to say that,

> . . . this linguistic intuition stems from an underlying intuition about the value of privacy; assuming that lost privacy is inherently undesirable, and that lessening our separation from others is not necessarily undesirable, it follows that

> lessening our separation from others is not always a loss of privacy, as suggested by separation-based accounts of privacy.[28]

I will start with Inness' central claim that access-based accounts 'make shared privacy impossible'. If my wife and I have an intimate conversation that we would not wish to share with another person, this is an example of shared privacy, on either control-based or access-based account. A conversation is not something that I can reasonably have on my own, and so by Inness' definition, according to the access account there can be no private conversations, which is clearly false. Once more, she seems to be arguing against a straw man.

The more fundamental point is whether, in engaging in the given activities, privacy is diminished through the sharing. My intuition here is that it is. James Rachels talks of defining relationships on the basis of degrees of intimacy, defined by the amount of privacy we maintain or surrender.[29] By showing you a personal letter I do lose some privacy, but gain a degree of intimacy through making myself vulnerable. The same is true through consensual sexual activity or inviting you into my house. In each case it would be odd to talk of a privacy loss, as this is not the most important aspect of the event at hand. Rather we celebrate the intimacy gain. In each of the cases Inness lists, the good of privacy is outweighed by the greater good of intimacy.

I want now to return to Inness' claim that there is an underlying intuition about privacy such that the loss of privacy is inherently undesirable. By contrast, she states, lessening our separation from others is not necessarily undesirable. From this, Inness argues, it follows that lessening our separation from others is not always a loss of privacy.

Inness' argument here would only work if privacy were exactly congruent with separation from others. In that case, a loss of privacy would be inconsistent with increased separation from others: you cannot have both together. Either I have privacy (in which case I experience separation from others) or I have community with others (in which case I do not have privacy). These are extreme ends of a continuum and so for most of us it is a matter of more or less, rather than total privacy versus total separation. However, this argument again relies upon Inness' assumption that in the access account privacy entails all information, which I have argued is false. In allowing you to see my face for the first time, I have not lost any privacy (my face is not something that I consider to be private information) but I might in the process become less separated from you. If, for instance, we have only spoken on the phone in the past but now have a video call so that we are able to see each other's faces, we might each feel closer and yet not have experienced any decline in privacy.

The third argument presented by Inness is that access-based accounts of privacy 'create a large class of "threatened privacy violations" that are more accurately described as true privacy violations'.[30] To illustrate this, Inness uses examples of (1) a peeping Tom looking in her bedroom window but whom she evades by hiding under the bed; and (2) a person concerned that a third party is trying to listen a conversation she is having with her friend and so she drags her friend into a closet to avoid being overheard. In both cases, Inness claims, the access account holds that there is no violation of privacy but only a threatened violation, which, she holds, is incorrect. I, on the other hand, argue that these *are* only threatened violations insofar as information is concerned. In the case of (1), the peeping Tom does violate my privacy insofar as he looks into my bedroom, which I likely hold to be a private space. The additional aspect of my being forced to hide is certainly problematic – why should someone else determine what I do, within reason, in my own home – but it is not itself a violation of my privacy. Therefore, in the case of the peeping Tom there is a violation of private *space*. In neither case, though, is the fact that a person has been forced to take action to avoid being heard or seen tantamount to a violation of that person's privacy. Nonetheless, it is worth remembering that just because these cases are 'only' threats to privacy, it does not follow that they are therefore not wrong. Indeed, I shall argue below that it is the increased risk of losing privacy that is one of the considerations that renders a loss of control over information (or space) problematic. In a similar vein, a threat to my privacy also entails an increased risk that my privacy will be lost.

Innes rejects the position that these are only threatened violations because she believes that 'the core of the privacy violation seems to lie in the need to attempt concealment in a zone that is intended to be under the agent's control'.[31] We would not, she says, shout from the closet, 'You are threatening my privacy,' but rather, 'You are invading my privacy.' As with her above arguments, though, one should be careful about placing too much weight on our everyday language which has more than moral exactitude to consider. It is quicker, easier, and has more impact to say that someone is invading your privacy than to say that they are threatening your privacy. In the case of the peeping Tom there *would* be grounds to shout out that he is 'invading my privacy', but, as above, these would be based on the fact that he has gained visual access to a private space. The fact that the person involved has been forced to take action to avoid being seen or heard does not amount to a violation of privacy.

Imagine a scenario similar to (2) which takes place at a crowded party in someone's house. Surrounded by people, I am trying to have a conversation with a friend that I am concerned will be overheard. I may even, as in (2), notice a person standing near to us with no conversation partner and fear that he might listen in to our conversation. In response, I suggest to my friend that we continue the conversation outside or maybe by phone the next day. In this case I would not say that the privacy of my conversation has been violated by being forced to make this decision, although I might say that our private space was violated, or was under threat of violation. Regarding the privacy of our conversation, I would say that this was threatened by the presence of the person standing nearby and others at the party, and so we took steps to ensure that it wouldn't be compromised.

I have gone to some lengths to refute the claims made by Inness against the access-based account of privacy. In many of the cases she describes it does *feel* as if there has been an invasion of privacy, and in many of them she is correct to suggest that we may well *say* that there has been an invasion of privacy. In some cases there may even have been a violation of private space, but in neither case is the fact that people have decided to hide tantamount to a violation of their privacy. Closer examination demonstrates that these feelings are misplaced and that our language can be sloppy, and where there are genuine violations of privacy these are explained by the access account. Thus I suggest that none of Inness' examples or arguments is ultimately convincing. Nonetheless, while language does not always aim at moral exactitude and so we can see why what we say may not always mirror the truth, it is important to dig deeper to examine why it is we might *feel* as if a violation of privacy has occurred when in fact none has.

3. Losing Control

When I lose control of my private information, I lose control over at least some of the rights and interests that privacy protects. For instance, if I live in a society intolerant of homosexuals and lose control over my diary in which I have confessed that I am homosexual then I lose my sense of security in this arena.

While there are unquestionably harms that arise from an invasion of privacy, in addition to the invasion itself, these harms might also arise from other causes. I don't have to have my privacy invaded in order to feel a decreased sense of security. A number of muggings or burglaries on my street might have that effect. In this section I will argue that privacy and control of my information can come apart. Along with Allen, I believe that control is neither necessary nor sufficient for privacy.[2] More than that, though, by drawing on the diary example I will argue that the harms arising from a lack of control of my information may be worse than those arising from an invasion of privacy.

Let us revisit the scenario of me leaving my diary in a coffee shop, and returning to find it in the hands of another person (throughout this example, my focus will be on the information contained within the diary rather than the access to the physical diary itself). Let us also make the case more interesting by suggesting that I am a public figure and there is information in my diary which could have a detrimental effect on my career. I now find my diary in the hands of another customer and despair: has she read it? In the scenario discussed above (Scenario 1), the customer said she had not read the diary and returned it to me unopened. However, this is not the only possible outcome.

One alternative would be for the customer to lie to me. She might have read my diary out of salacious interest, but return it to me without any intention of taking further the information she has discovered. In this case (Scenario 2) there has been an invasion of privacy, not because of me losing control of the diary but because another has read the diary, but the invasion of privacy is the only harm. There will be no further repercussions.

Alternatively, the customer may have read the diary and decided that she could make a lot of money by selling the information she has discovered to the press. She also realises that she could make *even more* money by blackmailing me. In this case I return to the café, see the diary, and feel my life fall apart as she sweetly hands it back to me with a demand for £100,000 to 'keep quiet' (Scenario 3). In this scenario there has again been an invasion of privacy, but there is a further harm of reducing my security, coupled with blackmail and threats for a still greater reduction in security.

There is a further possibility that the customer did not read the diary. Maybe she received a phone call just as she picked the diary up and finished the call as I returned to the shop. Nonetheless, she knows that it is a diary and that I am a public figure. From the look on my face she determines that there must be some salacious information in the diary. She surmises that I might pay to keep this information out of the press and so she pretends to have read the diary and attempts to sting me for £100,000. In this scenario (Scenario 4) I have again not experienced a loss of privacy (the diary remains unread) but I have experienced harm. Indeed, I have experienced the same harms, less the invasion of privacy, which I would have experienced *had* she read the diary and threatened me with blackmail.

Table 1. *Customer finds diary: alternative scenarios*

	Customer Does Not Attempt Blackmail	Customer Attempts Blackmail
Customer leaves the Diary Unread	*Scenario 1* No privacy loss No reduction in security	*Scenario 4* No privacy loss Reduction in security
Customer Reads the Diary	*Scenario 2* Privacy loss No reduction in security	*Scenario 3* Privacy loss Reduction in security

These four different scenarios can be summarised in the following table:

Table 1 demonstrates that whether my privacy is lost depends on the actions of the stranger. The harms that I experience, though, depend in part on my beliefs, irrespective of the facts. This is not to deny that a privacy violation is harmful: it is. However, there are other harms associated with privacy violations besides the loss of privacy. The worst scenario is that in which I experience both a privacy violation and a reduction in security (Scenario 3), and the best that in which there is no violation and no reduction in security (Scenario 1). However, it is important to ask whether it is worse that I suffer a reduction in security but no privacy violation (Scenario 4) or that I suffer a privacy violation and no reduction in security (Scenario 2). Given that I have stipulated the privacy violation alone does not have further consequences, it seems that it is the reduction in security that is the greater harm. Furthermore, while I do not know whether the stranger is lying about reading the diary I will act as if she has.

Table 1 demonstrates that control is not sufficient for privacy. In all four scenarios the customer has control over the diary and yet in two cases (Scenarios 1 and 4) there is no loss of privacy. Furthermore, despite taking control of my information, in Scenario 1 the customer has done nothing wrong. On the contrary, if she has taken the diary in order to protect my privacy then surely she has done the right thing by taking control. The customer having control is therefore not sufficient for there to be a loss of privacy. It is also clear from Table 1 that control is not necessary for privacy, for the simple reason that I have lost control of my information in each of the four scenarios and yet I have retained my privacy in two of the scenarios. Therefore control is neither necessary nor sufficient for privacy.

The phenomenon described by Scenario 4 was exploited by Jeremy Bentham in his Panopticon writings.[33] Here he described a prison with a central tower which had visual, oral, and aural access to every cell. The prisoners cannot see the warder in the tower and so do not know whether they are being watched at any particular moment. As a result, Bentham speculates, they will act as if they are being watched irrespective of the actual fact. This has subsequently been put into practice both in prisons and societies such as the German Democratic Republic (GDR), where the surveillance operations of the Stasi (the secret police) were known as 'Operational Control of Persons'.[34] The implication is that people's actions can be controlled to some degree through instilling in them a belief that their privacy has been compromised, or could be compromised at any time, irrespective of whether it in fact has been or even could be compromised. There are harms resulting from instilling this belief, but these do

not have to include the harm of an actual privacy loss. The *perception* of privacy loss, or possible privacy loss, is sufficient.

The first reason why the control account seems plausible is therefore because the loss of control over one's information involves (or, at least, *may* involve) harm to rights normally protected by privacy. While these rights are normally protected by privacy, they are not *only* protected by privacy. There are other ways in which these rights can be harmed without harming privacy itself. This is demonstrated by Scenario 4, above, in which the customer does not read the diary but attempts to blackmail me nonetheless.

It may be objected that in analogising government surveillance with a diary left in a café, I have drawn a false comparison. After all, it is not as if the governments are tripping over emails left lying around on the Internet. Rather, they appear to have actively pursued the collection of data with the aim of identifying suspicious messages.[35]

It is possible that the café example may be too restrictive here. As an alternative, imagine a scenario in which I am having a private conversation in my house with my wife. A spy may use a laser microphone to hear the conversation through closed windows. This is different to my having left the windows open such that a passer-by inadvertently hears our conversation. In the first case my informational privacy has been violated as the spy had a clear intention of accessing my conversation, whilst in the second my privacy has merely been diminished, on the grounds that the passer-by did not intend to access my information. He did not do anything wrong and could not help but overhear. However, if in the case of the spy I am suspicious of my conversation being recorded and so angle speakers playing music at the window, then there is no violation of my informational privacy. There have been other wrongs committed, not least a deliberate attempt to violate my informational privacy, but in the event I have not had my informational privacy violated.

While there are other wrongs involved in 'collecting' as opposed to 'finding' my diary or my private conversations, such as I have discussed in this section and will develop in the following section, these do not necessarily include a violation or even a loss of informational privacy. My thinking here is similar to that of Jasper Ryberg in his thought experiment of Mrs Aremac,[36] namely that there may be wrongs involved in collecting information, but these are not necessarily privacy wrongs.

4. Privacy and Risk

The second reason why the control account seems plausible relates to the risk that is imposed on the individual who has lost control of her information. A thorough analysis of risk has been carried out in recent years by Hélène Hemansson and Sven Ove Hansson, who point out that there are three parties of significance in any decision involving risk.[37] These are the decision-maker, the beneficiary, and the risk-exposed. Jonathan Wolff has taken this analysis to develop the following table:

Wolff demonstrates the variety of options that exist in deciding whether to undertake a risky venture. Significantly, we may be able to choose who will make the decision in an actual case (e.g. whether the decision is made by a democratic vote or an autocratic decree). If we are not able to choose then the analysis highlights who stands

Table 2. *Risk analysis*[38]

	Party suffering cost	Party enjoying benefit	Party making decision
1	A	A	A
2	A	B	B
3	A	B	A
4	A	A	B
5	A	B	C

to pay the costs associated with particular decisions and where any conflicts of interest might lie.

(1) is the scenario in which an individual gambles with his own stakes. He alone stands to win if all goes well, but he alone also stands to lose if all goes badly. A simple example here might be of a person with no family or other ties of responsibility who gambles his own money in a casino.[39] This person is in a good position to decide whether to undertake the risk, as he will be the one to benefit or lose from that risk.

(2) pictures a scenario in which the decision-maker decides on behalf of others. Here the beneficiary is the same as the cost-payer. This may have benevolent outcomes, such as the case suggested by Wolff of a (non-motorcycle riding) government legislating that all people riding a motorcycle must wear a safety helmet.[40] On the other hand, we may reject such paternalistic practices, as we tend to in medicine, where the 'doctor knows best' model has given way to an emphasis on patient choice and informed consent.

(3) suggests a situation in which the decision-maker has the choice to pay a cost for the beneficiary or not. An illustration here would be the firefighters who helped people escape the World Trade Centre in New York on 9/11 before they themselves were killed in the collapsing buildings. While we see sacrifice as noble, though, the arrangement in (3) is not always desirable. Given that the decision-maker stands only to lose while others stand to benefit, this scenario is likely to make the decision-maker risk averse. Indeed, it is precisely because a rationally self-interested position would incline one to avoid the risk that we celebrate acts of self-sacrifice as noble. Nonetheless, there are other situations in which the decision-maker will not be so noble and will avoid taking the risk altogether, a situation which might be detrimental in contexts such as business or competitive sports. Therefore, there are good reasons to prefer that the person who would pay the cost should not be the person to make the decision. Hence it is preferable that decisions regarding taxation on income and inheritance are not left solely to billionaires.

(4) is often the most ethically problematic. Whereas the decision-maker is risk-averse in (3), she is risk-prone in (4). As Wolff points out, this is arguably the situation that pertained prior to the economic crash of 2007–8 in which bankers were able to take significant risks with money that, ultimately, was not their own.[41] At the same time, risk-taking can be good for bringing about positive changes in society, such as expanding suffrage from a formerly restricted voting base, or the introduction of new inventions, and so being risk-prone is not always problematic.

Finally, (5) describes a situation involving three different parties. Here the decision-maker, beneficiary, and risk-exposed are all different. As such, the decision-maker has to decide as to the best outcome when it is clear that some will lose out while others will benefit. The conflicts of interest faced by the decision-maker in (5) are less obvious than in (3) or (4), but may still be present through lobbying, bribery, or blackmail. A more idealised situation here might involve an independent judge (A) settling a dispute between two people (B and C).

Returning now to the problem of losing control over one's information, we can see why this is problematic. While I am in control of my information, I am in position (1). I am the only one who stands to benefit or lose from any diminution of privacy. Were I a celebrity, together with my spouse we could sell our wedding pictures to a glossy magazine and get a lot of money in return for a loss of privacy regarding the occasion.[42] By the same token, we could choose not to sell those pictures, forfeiting the potential money but retaining a greater degree of privacy.

The problem arises when another person takes control of my information. Call this person the New Controller (NC). Returning to my diary left in the coffee shop, the customer who retrieved the diary is NC. Now someone other than me decides what to do with my diary, and the information contained therein. Imagine I am a celebrity and that this information concerns certain compromising admissions as to my many extra-marital affairs. In this case it seems rational (*ceteris paribus*) for NC to sell the information. All the benefits of such a sale would accrue to her, while the costs (to my reputation, security, dignity, etc.) would fall on my spouse and me, although there would also be painful benefits to my spouse in learning the truth of my philandering ways. In losing control of my information the scenario has moved from position (1) on Table 2 to position (4), or from a position of relative ethical unconcern to that of great ethical worry. As noted above, this means that not only does NC have control over my (formerly-private) information, but also there are incentives for her to act in such a way that she will benefit and I will pay the cost.

Given this situation, I am likely to feel extremely vulnerable. NC is now both able to access my information (i.e. violate my privacy) and, all other things being equal, is likely to use my information for her benefit. Whatever the actual intention of NC, I fear that she will violate my privacy as she has both the means and the incentive. If I do not know whether she has actually accessed my information and I have no means of intervening in her actions, I will, like the citizens of the GDR or inmates of Bentham's Panopticon, act under the assumption that she already has.

If NC is not an individual but the state then the consequences of my worrying that my information has been accessed, or will be accessed if I upset the state, are severe. I may feel chilling effects that deter me from engaging in democratically legitimate but unpopular (to those in power, at least) demonstrations against the government; I may seek to conform to the rest of society a little more closely; and I may decline to speak out against policies with which I disagree. These have consequences both for the individual, whose autonomy is suppressed and whose sense of security challenged, and for society, which will as a result enjoy less free debate and experience more pent-up frustration.

Once more, even though NC has not actually accessed the information she now controls, the consequences are as if she had. As such, the experience is again that of a violation, not necessarily of privacy (although in this case it might be should she choose to access the information), but of those rights and interests that we protect by keeping certain information private.

Finally, it is worth noting that the situation I have described is simplified. The NC may have other reasons that have not been considered for not accessing the information that she possesses. In Scenario 1, for instance, the NC did not read the diary even though she might have stood to gain from doing so. In that case there were competing considerations (her knowledge of how intimate her own diary is, her projected fear should she lose her diary, and her ethical approach to the situation) that outweighed the case in favour of her reading the diary.

To return to the NC as state, there are therefore reasons why the state may not access an individual's information even though it has control of that information. It may be that the state takes a strongly ethical stance on such action, or is limited by laws which strictly regulate which information it is able to access. In the case of secretive state organisations, though, which do not readily demonstrate ethical approaches, are for obvious reasons not subject to public scrutiny, and which do have an interest in accessing information, there are clearly grounds as to why people would be rational to worry about their informational privacy.

5. Privacy and State Intelligence

I have argued that there are two reasons why a loss of control over information may feel like a loss of informational privacy, even though it is not. The first is that a loss of control may involve harms to the rights that privacy protects. Privacy is not inherent to these rights, though. I can have my security harmed without my privacy also being harmed. Experiencing harm to these rights and interests may *feel* like a breach of my privacy even though it is not. The second reason is that the rational action for NC is to violate my privacy. She is in a position where she controls my information and stands to benefit from accessing it. Given this, it is rational for me to worry that she has accessed or will access it and so, once more, I experience harm to the rights and interests that privacy protects.

This returns us to the opening case of the collection of information by NSA and GCHQ. If I am correct that the governments of the UK and US see privacy as a matter of access, and that those protesting the actions of those governments see privacy as a matter of control, then this explains the apparent discrepancy. However, the issue goes further than this. By focusing on privacy as the key problem in the collection of information, a problem which the governments simply do not see, the real issues of harm and wrongdoing (the loss of a sense of security and the increased risk of privacy violation) are missed. If I am correct in defending the access account of privacy, then arguments about privacy are a red herring: focusing on privacy distracts all involved from the real issues of harm to the general populace. Indeed, by focusing the argument on privacy it may be harder to persuade supporters of actions taken by NSA and GCHQ that what they are doing is harmful. They have a response to that argument, namely that they are not violating people's privacy except in specific, justifiable, targeted cases. The arguments presented in this article cannot be dismissed so easily.

Throughout this article I have concentrated on privacy of information, while acknowledging also that privacy is a concept that applies to space. I can have a private

space and you can invade that private space without gaining any new information. Imagine I tell you the exact contents of my bedroom. Shortly thereafter you visit my house and, without my permission, go into my bedroom. You will have gained no new information but you will nonetheless have invaded my private space. Could a similar argument be made in terms of state intelligence agencies having access to my email? NSA and GCHQ do not need to access my email to violate my privacy, according to this argument they would merely need to access my email account, itself a space that should be private to me.

While this argument would work in cases where the state has hacked into a person's email account, hacking is not the issue under discussion in this article. The claim is rather that email is intercepted while in transit and in the control of third parties such as Google or Yahoo. An analogy here would be of me writing a letter and putting it in a borrowed briefcase which I then give to a courier to deliver to a trusted recipient. While in transit between myself and the recipient, and with the permission of the owner of the briefcase and of the courier, the state scans the contents of the briefcase but does not read the letter, and finds out from the courier the addresses between which he is travelling and the times at which he left and will arrive.

While I would refrain from saying that there is *no* invasion of private space here, the issue is less clear-cut than may at first have seemed to be the case.

6. Conclusion

The debate surrounding government surveillance of Internet communications has given a new significance to a long-standing debate as to whether privacy is a matter of access or control. I have argued that it is a matter of access and not control. However, a person losing control of their information is highly problematic. It involves many of the same harms as an actual loss of privacy, to the extent that in losing control of my information I may *feel* as if I have had my privacy violated. This feeling would be understandable, but incorrect. Furthermore, in losing control of my information I would be at the mercy of a new controller who would be risk prone with that information. I would therefore both feel vulnerable and be vulnerable to a violation of my privacy.

Returning to the case of the US and UK (and other) intelligence services collecting quantities of internet traffic relating to the citizens of those states, many have complained that this involves a violation of privacy of those citizens. The intelligence services have responded that this is not the case so long as the information is not accessed. As such, the access account of privacy is held by the intelligence agencies while the control account is that held by their antagonists. In this instance I have argued for the interpretation of privacy offered by the intelligence agencies. However, as I have demonstrated, it does not follow that their activities are thereby harmless. On the contrary, these activities may be more harmful than an actual violation of privacy.

There is one further area of significance which I have not explored in this article and would merit discussion, which is the use of automated systems in the analysis of collected data. I have argued that privacy is a matter of access, and assumed that this access is carried out by a human. However, in the case of collection of data by NSA and GCHQ, according to the Snowden revelations, the swathes of data collected are

investigated by automated systems looking for key words or phrases. If the access of private information by an automated system, as well as by a human, constitutes a violation of privacy then even by the access account there has been a gross violation of privacy involving all data that was searched by automated systems (which is presumably all data collected) as well as that accessed by human analysts.[43]

Kevin Macnish, Inter-Disciplinary Ethics Applied, University of Leeds, 8-12 Fenton Street, Leeds, LS2 9JT, UK. k.n.j.macnish@leeds.ac.uk

NOTES

1 danah boyd, 'Making sense of privacy and publicity' (SCSW, Austin, Texas, 2010), http://www.danah.org/papers/talks/2010/SXSW2010.html; W.A. Parent, 'Privacy, morality and the law', *Philosophy and Public Affairs* 12,4 (1983): 269–88; T.M. Scanlon, 'Thomson on privacy', *Philosophy and Public Affairs* 4,4 (1975): 315–22; Alan F. Westin, *Privacy and Freedom* (New York: Athenaeum, 1967).

2 See, for example, Anita L. Allen, 'Our privacy rights and responsibilities: Replies to critics', *Newsletter of the American Philosophical Association: Philosophy and Law* 13,1 (2013): 19–27; Adam Moore, 'Coercing privacy and moderate paternalism: Allen on unpopular privacy', *Newsletter of the American Philosophical Association: Philosophy and Law* 13,1 (2013): 10–14.

3 Daniel J. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008), pp. 12–13, 40; see also Daniel J. Solove, 'Conceptualizing privacy', *California Law Review* 90,4 (2002): 1087–1155, doi:10.2307/3481326.

4 Allen 2013 op. cit., pp. 21, 22; Annabelle Lever, 'Privacy: Restrictions and decisions', *Newsletter of the American Philosophical Association: Philosophy and Law* 13,1 (2013): 1–7, at p. 2; Annabelle Lever, *A Democratic Conception of Privacy* (Bloomington, IN: AuthorHouse UK, 2013), pp. 73, 81; Annabelle Lever, 'Feminism, democracy and the right to privacy', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2005): http://papers.ssrn.com/abstract=2559971; Solove 2002 op. cit.

5 Tim Bradshaw, 'Tim Berners-Lee is 'deeply concerned' about PRISM', *Financial Times* 7 June (2013): http://blogs.ft.com/tech-blog/2013/06/tim-berners-lee-prism/; Jonathan Topaz, 'Rand Paul: NSA monitoring an "extraordinary invasion of privacy"', *POLITICO* 6 September (2013): http://www.politico.com/blogs/politico-live/2013/06/paul-monitoring-an-extraordinary-invasion-of-privacy-165742.html.

6 Court of Justice of the European Union, Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner*, 94 (Court of Justice of the European Union 2015).

7 Ellen Nakashima, Barton Gellman & Greg Miller, 'New documents reveal parameters of NSA's secret surveillance programs', *The Washington Post* 20 June (2013): https://www.washingtonpost.com/world/national-security/new-documents-reveal-parameters-of-nsas-secret-surveillance-programs/2013/06/20/54248600-d9f7-11e2-a9f2-42ee3912ae0e_story.html?hpid=z2#.

8 Steven Levy, 'I spent two hours talking with the NSA's bigwigs. Here's what has them mad', *WIRED* 13 January (2014): http://www.wired.com/2014/01/nsa-surveillance/.

9 George E. Panichas, 'An intrusion theory of privacy', *Res Publica* 20,2 (2014): 145–61, doi:10.1007/s11158-014-9240-3; Tony Doyle, 'Privacy and perfect voyeurism', *Ethics and Information Technology* 11 (2009): 181–89; Adam Moore, 'Defining privacy', *Journal of Social Philosophy* 39,3 (2008): 411–28; see also Irwin Altman, *Environment and Social Behaviour* (Monterey, CA: Brooks/Cole Publishing Co., 1976).

10 Parent op. cit.; Westin 1967 op. cit.

11 Moore 2008 op. cit., p. 417.

12 Doyle op. cit., p. 182.

13 Altman op. cit.; boyd op. cit.; Ryan Calo, 'Clementi and the nature of privacy harm', *CIS Blog* 6 November (2010}: http://cyberlaw.stanford.edu/blog/2010/11/clementi-and-nature-privacy-harm; Dag Elgesem, 'Privacy, respect for persons, and risk', in C.M. Ess (ed.) *Philosophical Perspectives on Computer-Mediated Communication* (New York: SUNY Press, 1996), p. 51; Charles Fried, 'Privacy', in F.D. Schoeman (ed.) *Philosophical Dimensions of Privacy*, 1st edn. (Cambridge: Cambridge University Press, 1984), p. 209; Stephen T. Margulis, 'Conceptions of privacy: Current status and next steps', *Journal of Social Issues* 33,3 (1977): 5–21, doi:10.1111/j.1540-4560.1977.tb01879.x; Arthur Raphael Miller, *The Assault on Privacy:*

Computers, Data Banks, and Dossiers (Ann Arbor, MI: University of Michigan Press, 1971), p. 25; Moore 2013 op. cit.; Moore 2008 op. cit.; Daniel O. Nathan, 'Just looking: Voyeurism and the grounds of privacy', *Public Affairs Quarterly* 4,4 (1990): 365–86; Parent op. cit.; Scanlon op. cit.; Alan F. Westin, 'Social and political dimensions of privacy', *Journal of Social Issues* 59,2 (2003): 431–53, at p. 431, doi:10.1111/1540-4560.00072; Westin 1967 op. cit., p. 7.

14 Paul M. Schwartz, 'Internet privacy and the state', *Connecticut Law Review* 32 (2000): 815–59, at p. 820.

15 Julie Innes, *Privacy, Intimacy, and Isolation* (Oxford: Oxford University Press, 1992), p. 42.

16 Anita L. Allen, *Uneasy Access: Privacy for Women in a Free Society* (Totowa, NJ: Rowman & Littlefield, 1988); Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation*, New edn. (New York: Vintage Books, 1998); R. Gavison, 'Privacy and the limits of the law', in F.D. Schoeman (ed.) *Philosophical Dimensions of Privacy* (Cambridge: Cambridge University Press, 1984), pp. 346–402; Hyman Gross, 'The concept of privacy', *New York University Law Review* 42 (1967): 34–54, at p. 34; H.T. Tavani & J.H. Moor, 'Privacy protection, control of information, and privacy-enhancing technologies', *Computers and Society* 31,1 (2001): 6–11; Judith Jarvis Thomson, 'The right to privacy', *Philosophy and Public Affairs* 4,4 (1975): 295–314; Ernest Van Den Haag, 'On privacy', *Nomos* 13 (1971): 147–53.

17 Thomson op. cit., p. 307.

18 Tavani & Moor op. cit., p. 6.

19 Anita L. Allen, 'Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm', *Connecticut Law Review* 32 (2000): 861–75, at p. 861.

20 Julie C. Inness, *Privacy, Intimacy, and Isolation*, New edn. (New York: Oxford University Press, 1996), p. 44.

21 Ibid., pp. 43–44.

22 Ibid., pp. 47, 58.

23 Ibid., p. 44.

24 Tavani & Moor op. cit., p. 8; see also Westin 1967 op. cit.; Altman op. cit.; and Valerian J. Derlega & Alan L. Chaikin, 'Privacy and self-disclosure in social relationships', *Journal of Social Issues* 33,3 (1977): 102–15, doi:10.1111/j.1540-4560.1977.tb01885.x.

25 Inness op. cit., p. 45.

26 Ibid., p. 46.

27 Ibid.

28 Ibid.

29 James Rachels, 'Why privacy is important', *Philosophy and Public Affairs* 4,4 (1975): 323–33, at p. 331.

30 Inness op. cit., p. 46.

31 Ibid., p. 47.

32 Allen 2000 op. cit., pp. 867–8.

33 Jeremy Bentham, *The Panopticon Writings* (London: Verso Books, 1995).

34 Anna Funder, *Stasiland: Stories from Behind the Berlin Wall*, New edn. (London: Granta Books, 2004), p. 198.

35 I am grateful to Annabelle Lever for raising this issue.

36 Jesper Ryberg, 'Privacy rights, crime prevention, CCTV, and the life of Mrs Aremac', *Res Publica* 13,2 (2007): 127–43.

37 Hélène Hermansson & Sven Ove Hansson, 'A three-party model tool for ethical risk analysis', *Risk Management* 9, 3 (July 2007): 129–44, at p. 130.

39 Granted, there is still a cost-payer in this case if we consider opportunity cost and the person who might have benefitted from person A's charity, but this is to complicate the picture unnecessarily. We might also need to stipulate that person A is not addicted to gambling and so not suffering additional harms that would arise from the act of gambling.

40 Wolff op. cit.

41 Ibid.

42 I accept that others might also benefit from the pleasure they gain in seeing the photographs, but I would suggest that this pales into insignificance next to the seven-figure sums given to the celebrity couple.

38 Jonathan Wolff, 'Five types of risky situation', *Law, Innovation and Technology* 2,2 (2010): 151–63, doi:10.5235/175799610794046177.

43 I am grateful to Rob Lawlor, Helen Morley, Carl Fox, Annabelle Lever, Roger Crisp and an anonymous reviewer for comments which have significantly strengthened the arguments and illustrations in this article.