The Journal of Political Philosophy: Volume 27, Number 1, 2019, pp. 3–

Privacy Rights and Public Information*

Benedict Rumbold
Philosophy, University College, London

and

James Wilson
Philosophy, University College, London

OUR subject is the nature and limits of individuals' rights to privacy over information that they have made public.[1] Consider the following case. The UK and Republic of Ireland charity Samaritans provides a long-established and well-respected suicide-prevention telephone helpline. In 2014, Samaritans launched a web app called Radar, which aimed to detect signs of emotional distress or suicidal thoughts in Twitter posts. The idea was that you, as a Twitter user, could sign up to Samaritans Radar and the service would monitor the public tweets of all the people you were following on Twitter. Radar would then alert you if it detected a tweet, or pattern of tweets, in any of the people you were following that indicated that the person 'could be going through a tough time'.[2] Importantly, Radar did not inform those whose tweets were being monitored, nor was consent sought from them.

Should we be concerned with these kinds of practices? Do they violate individuals' right to privacy? One, influential, tradition within the philosophy of privacy thinks not. As explained, Radar works by analysing tweets individuals have made public and, according to this tradition, informational privacy is by its nature limited to private information. First, one has no right to privacy over information that was never private to begin with. Second, insofar as any individual makes once-private information public, they waive their right to privacy with respect to both *that* information and anything one may infer from it.

Thomson offers what may be regarded as a canonical statement of this position. To illustrate her view, she provides the following series of examples. Say

*We would like to thank i-sense EPSRC IRC in Early Warning Sensing Systems for Infectious Diseases (Grant reference number EP/K031953/1, <http://www.i-sense.org.uk>), Professor Rachel McKendry, and the *Journal of Political Philosophy*'s two anonymous reviewers.

[1]By 'making public' here, we mean disclosing a piece of once-private information to a person or persons who are not bound by agreement to hold said information in confidence.

[2]The relevant materials are archived at Samaritans Website (2016), <http://www.samaritans.org/news/samaritans-launches-twitter-app-help-identify-vulnerable-people?>.

doi: 10.1111/jopp.12158

you possess some picture. In one case, you want someone else to look at this picture and therefore (1) invite her to look at it, or (2) get her to look at it whether she wants to or not. In another case, you do not mind who looks at the picture and therefore (3) let it be looked at. Again still, despite not wanting anyone to look at the picture, you (4) leave it somewhere where another person would have to go to some trouble to avoid looking at it, or (5) leave it somewhere where nobody could reasonably be expected to know it belonged to anybody.[3] In Thomson's view—and that of numerous others—despite having a right that others do not look at one's picture, a right to keep it *private*, in all these cases one has *waived* that right; in cases (1), (2), and (3) intentionally, in cases (4) and (5) unintentionally.[4] And, 'given a man has waived his right to a thing, we violate no right of his if we do not accord it to him'.[5]

Although Thomson does not explicitly discuss this, the same logic would seem to cover anything anyone might infer from looking at the picture. Say, for example, that the picture is a photograph of you at high school. By looking at the picture, someone might be able to tell (with varying degrees of accuracy) the school you attended, how happy you were at the time, perhaps something about the kind of social groups you used to keep company with, and so on. If one has waived one's right to privacy about the picture itself, it looks as though one has waived one's right to privacy about these pieces of information as well. Correspondingly, no one violates any right of yours by inferring them from the information you have made public, whether or not you intended to publicize *those* pieces of information when you publicized the original picture.

On Thomson's view, then, an individual's right to privacy begins and ends with that information they hold in private. And this seems to have been the view adopted by Samaritans. Indeed, in the 'Frequently Asked Questions' prepared for the launch of the app, Samaritans explained that 'All the data used in the app is public, so user privacy is not an issue. Samaritans Radar analyses the Tweets of the people you follow, which are public Tweets. It does not look at private Tweets.'[6] It is fair to say, however, that others felt differently. Within a couple of days of its going live, a change.org petition was created by members of the public, alleging that 'Samaritans Radar breaches people's privacy by collecting, processing and sharing sensitive information about their emotional and mental health status.'[7] Samaritans were caught off guard by the scale of the anger, and

[3]Judith Jarvis Thomson, 'The right to privacy', *Philosophy and Public Affairs*, 4 (1975), 295–314, at pp. 301–2.

[4]Ibid.

[5]Ibid.

[6]Samaritans Website (2016), <http://www.samaritans.org/sites/default/files/kcfinder/branches/branch-96/files/FAQs%20for%20Radar%20-%20EXTERNAL%281%29.pdf>. Accessed 28 Mar. 2017.

[7]Change.org Website (2016), < https://www.change.org/p/twitter-inc-shut-down-samaritans-radar>. Accessed 28 Mar. 2017.

Radar was suspended, before being taken offline permanently only nine days after it launched.

Whether or not Twitter users' rights to privacy were violated in this particular case, we think that it is important to have an account of the right to privacy that at least makes it intelligible that such uses of information *could* violate privacy—that there can be cases in which an individual's right to privacy could be violated by the appropriation and dissemination of information either that they themselves have made public or that has been inferred from information they have made public.

The idea that we might be under continued obligations to protect an individual's right to privacy, even when they are acting within a public domain is not new. One writer who has perhaps done more than any other to illuminate this field is Helen Nissenbaum.[8] Among various other innovations, Nissenbaum makes two interventions critical to the present debate. First, Nissenbaum eschews orthodox views that start by drawing a strong distinction between private and public spheres—wherein the 'private' indicates the realm of familial and other personal or intimate relations and 'public' the civic realm or realm of community outside of this personal one—before assigning special protection only to activities in the former domain. Rather, as Nissenbaum shows, it is not the case that 'outside of this special realm no norms of privacy apply', or that personal information is somehow 'up for grabs'.[9] Even in public, norms governing what Nissenbaum calls the 'appropriate flow of personal information' can still render certain activities violations of individuals' right to privacy.[10] Secondly, Nissenbaum draws our attention to the extent to which the norms governing the appropriate flow of personal information are shaped by their social context, being a function of (1) the types of information in question; (2) the respective roles of the subject, the sender (who may be the subject), and the recipient of this information; and (3) the principles under which the information is sent or transmitted from the sender to the recipient.[11] Thus, on Nissenbaum's view, the right to privacy is properly understood as a right to 'contextual integrity' and what *this* amounts to 'varies from context to context'.[12]

Nissenbaum's work provides a powerful set of tools with which to analyse the normative structure of new problems in the philosophy of privacy. However, while Nissenbaum alerts us to the possibility that the right to privacy may cover activities in a greater range of domains than we previously assumed, one set of cases she overlooks, perhaps, are those in which duty-bearers overlook their

[8]See Helen Nissenbaum, 'Protecting privacy in an information age: the problem of privacy in public', *Law and Philosophy*, 17 (1998), 559–96; Helen Nissenbaum, 'Privacy as contextual integrity', *Washington Law Review*, 79 (2004), 101–39; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford University Press, 2009).

[9]Nissenbaum, 'Protecting privacy in an information age', p. 581.

[10]Nissenbaum, *Privacy in Context*, p. 127.

[11]Ibid.

[12]Ibid.

duties to right-holders, not because they fail to recognize the presence of certain norms of contextual integrity, but because they mistakenly believe that such norms are no longer in force. In the case of Radar, then, we would argue that the mistake Samaritans made was not that they wrongly assumed that there *were* no norms of contextual integrity with respect to people's activity on Twitter; rather it was that, based on a misreading of the normative significance of certain actions by Twitter users, they wrongfully concluded that such norms were no longer in operation.

In our view, then, in order to make better sense of what is going on in these sorts of cases, we need to shift our attention away from questions about *where* individuals may exercise their right to privacy, and instead look to how right-holders *manage* their rights within such domains—in particular, by what actions individuals 'hold' their rights and by what actions they 'waive' them. This, in turn, leads to a further discussion about what inferences duty-bearers may legitimately draw about their continued obligations to right-holders from how those right-holders behave. In this sense, then, our primary interlocutor in what follows is Thomson, rather than Nissenbaum. Following Thomson, we do not contest the idea that individuals can waive their right to privacy and often do so when making a piece of once-private information public. However, we do contest the idea, intimated by Thomson, that one can waive one's right to privacy *unintentionally*. From this, it follows that there is a class of public information—namely, once-private information that individuals have made public unintentionally—which remains under the protection of an individual's right to privacy, even when it has passed into the public domain. As we shall see, this class includes any information the right-holder was unaware could be inferred from information they have made public and which they would not otherwise have wanted to be in the public domain.

In what follows, we detail this argument in greater depth, drawing out its various implications and responding to various counter-arguments. We begin, in Section I, by outlining what we take as the *content* of the right to privacy, that is, what we take the right to privacy to be a right *to*.[13] Here we primarily draw on an account of the right to privacy recently offered by Marmor; although, as we also emphasize, our argument does not necessarily depend on subscription to that particular conception of the right to privacy (nor certain other debates about privacy and its moral import). In Section II, we then give a broad account of the obligations engendered by individuals' right to privacy, the actions by which a rights-holder may absolve us of them or 'waive' such rights, and the kinds of information that we may thereby take them to cover. In Section III, we explore the issue of information obtained through analysis and inference. In Section IV, we then consider the extent of our obligations when the ethical status of public

[13]Cf. Leonard W. Sumner, *The Moral Foundations of Rights* (Oxford: Clarendon Press, 1987), p. 11.

information is unclear. In Section V, we discuss a few complications and ambiguities of our position, centring on what can be considered a 'reasonable expectation'. In Section VI, we consider the implications of our theory for the ethics of Big Data, before concluding in Section VII.

I. THE CONTENT OF THE RIGHT TO PRIVACY

The philosophical literature provides a plethora of competing conceptions of the content and purpose of the right to privacy, from the notion of privacy as control over information (as espoused by Fried, Parent, and Prosser)[14] to privacy as control over access (defended by Allen, Gavison, and Moore).[15] Nothing about the thesis we shall lay out here requires us to decide between these or other conceptions. Since what interests us here is a question about (1) what kinds of action by an agent may be said to waive their right to privacy, and (2) the kinds of information that a rights-holder should be understood as holding their right to privacy over, both questions may be addressed independent of many of the current views about what constitutes an individual's right to privacy.[16]

However, that being said, for ease of explication it will be helpful to explore the points we want to make in the context of a more specific account of the right to privacy, even if the implications of our argument are broader.[17] For the purposes of exposition, then, in what follows we adopt a recent account set out by Marmor. On Marmor's account, an individual's right to privacy is best understood as being grounded in their interest in having a reasonable measure of control over the ways in which they can present themselves and what is theirs to

[14]Charles Fried, *An Anatomy of Values* (Cambridge, MA: Harvard University Press, 1970); William A. Parent, 'Privacy, morality, and the law', *Philosophy and Public Affairs,* 12 (1983), 269–88; William Prosser, 'Privacy', *California Law Review,* 48 (1960), 383–423.

[15]Anita Allen, *Uneasy Access: Privacy for Women in a Free Society* (Totowa, NJ: Rowman & Littlefield, 1988); Ruth Gavison, 'Privacy and the limits of law', *Yale Law Journal*, 89 (1980), 421–71; Adam D. Moore, 'Privacy: its meaning and value', *American Philosophical Quarterly,* 40 (2003), 215–27.

[16]As well as being logically independent of most positions on what constitutes the content of an individual's right to privacy, we also take the argument presented in what follows to be independent of a host of further questions about privacy's basic nature, including the question of why privacy might be considered morally valuable to begin with, and the debate as to whether there is something fundamentally distinctive and coherent about the various claims that have been called privacy interests (what DeCew calls the 'coherentist' thesis), or whether, like Thomson, one believes that what are called privacy concerns are analysable or reducible to claims of other sorts, such as infliction of emotional distress or property interests (what DeCew calls the 'reductionist' thesis); Judith W. DeCew, 'Privacy', *Stanford Encyclopedia of Philosophy* (Spring 2015), ed. Edward N. Zalta, <http://plato.stanford.edu/archives/spr2015/entries/privacy>.

[17]Writing our account in light of a putative characterization of the right to privacy can also be seen to serve an additional function. All being well, if our account succeeds in further clarifying what information one may be said to hold a right over and by what means one may be said to waive such a right, without also violating the tenets of some putative conception of the right to privacy x, then such an argument also shows that such an account is true of at least one conception of the right to privacy: namely, x. Another way to view the argument presented in this article, then, is an attempt to further develop Marmor's account in those directions—although, as set out, we take it to have a broader applicability than that.

others.[18] There are a few features of this conception that are worth bearing in mind in what follows.

First, as Marmor himself emphasizes, the notion of privacy he endorses follows two intuitions originally articulated by Thomson: that 'a violation of a right to privacy is not simply about what is known but mostly about the ways in which some information is obtained'; and that 'when we focus on what is wrong about the way in which some fact came to be known, we can normally explain it as a violation of one's proprietary rights: somebody used something that is yours without your permission'.[19] However, rather than following Thomson's view that privacy may thereby be reduced to certain other, more basic, rights (notably proprietary rights), Marmor argues that there is something coherent and distinctive about privacy rights: specifically, they safeguard our interest 'in having a reasonable measure of control over ways in which we present ourselves to others and the ability to present different aspects of ourselves, and what is ours, to different people'.[20]

As Marmor is happy to admit, the qualifier that we only have a right to a 'reasonable' measure of control over the way we present ourselves to others is 'a rough and vague criterion'.[21] However, it reflects two limitations to our right to privacy: first, that no one *can* have 'absolute control' over the ways in which they are perceived by others; and secondly, that no one *ought* to have too much control over the way they present themselves to others. What is necessary, though, is *some* control. The appropriate measure of control required in any situation, then, becomes a question of what is reasonable to protect those interests safeguarded by the right itself. Such a threshold is vague in that it admits of reasonable disagreement as to the extent of that limit, yet what it loses in precision it gains in flexibility: what constitutes a 'reasonable measure of control' in one situation may be different from another.

II. THE OBLIGATIONS ENGENDERED BY AN INDIVIDUAL'S RIGHT TO PRIVACY AND THE ACTIONS BY WHICH A RIGHTS-HOLDER MAY ABSOLVE US OF THEM

As discussed, the principal aim of this article is to elucidate some of the fundamental characteristics of the right to privacy. However, the main argumentative work done in the article is in our explication of the duties engendered by the right to privacy and by what actions right-holders absolve duty-bearers of such obligations, which is to say, to 'waive' them.[22]

[18]Andrei Marmor, 'What is the right to privacy?', *Philosophy and Public Affairs*, 43 (2015), 3–26.
[19]Ibid., p. 6.
[20]Ibid.
[21]Ibid., p. 26.
[22]Here we follow Tasioulas's view of rights as the source of certain duties, each right endowing the right-holder with a justifiable claim on another's action; John Tasioulas, 'Taking rights out of human rights', *Ethics*, 120 (2010), 647–78; cf. H. L. A. Hart, 'Are there any natural rights?', *Philosophical Review*, 64 (1955), 175–91.

What are the duties, then, engendered by an individual's right to privacy? To date there has been surprisingly little discussion about this issue in the literature.[23] However, to the extent that the question has been considered at all, writers have tended to characterize the duties generated by the right to privacy in terms of an obligation on the part of duty-bearers to refrain from doing something harmful or restrictive to right-bearers with respect to the domain covered by the right in question. Thus, when we understand an individual's right to privacy in Marmor's terms, as a right to have a reasonable measure of control over the ways we present ourselves to others, we might correspondingly think that, by holding such a right, right-bearers make a justifiable claim on us *not* to impede, circumvent, or otherwise supersede *their* efforts in presenting whichever 'self' they wish to whomever they wish at any given moment.[24]

Needless to say, this prescription might be seen to cover a whole host of possible actions. However, one important class of these—certainly one which scholars working in privacy have been most concerned with—is the appropriation and public exposure of information that rights-holders had sought to keep private. On this line of thought, then, there is some set of information that a person holds 'in private'—which is to say, confidential to that person and anyone they have brought into their confidence—and one of the duties engendered by an individual's right to privacy is to refrain from any action which attempts to gain access to such information without their consent and/or make such information known to others.[25] The classic example here is the picture kept locked away in a safe, with the owner's right to privacy giving us good reason to refrain from gaining access to the safe to look at the picture and/or showing the picture to others.

However, the question now arises, does an individual's right to privacy give them a justifiable claim over our actions with regard to any other kinds of information? As noted in the introduction to this article, for many the simple answer here is no. That is, insofar as an individual does not hold a piece of information in private, they have no claim on us as to what we do with it. First, consider information that was never private to begin with. The colour of the sky, for example, might be considered as one piece of eternally public information. According to this account, individuals have no justifiable claim over our action with regards to this kind of information because such information was never held by them in the requisite sense. Such information belongs to everyone and no one (picking up, perhaps, on the intuition that there is something 'proprietary' about privacy when it applies). Next, consider information that, though once private,

[23]One notable exception here is Neil C. Manson and Onora O'Neill, *Rethinking Informed Consent in Bioethics* (Cambridge: Cambridge University Press, 2007), esp. ch. 5.

[24]An interesting question here is whether this duty includes a duty not to challenge any false claims an individual makes about themself. Do we fail in our obligations as duty-bearers, for example, when we call someone out on a lie? However, insofar as these questions draw us into more thorny questions of individuals' rights to do wrong, we take such matters to be largely outside the scope of this article.

[25]Thomas Nagel, 'Concealment and exposure', *Philosophy and Public Affairs,* 27 (1998), 3–30.

now finds itself in the public domain by way of some action of the right-holder. Here, the argument goes, rights-holders have no justifiable claim over our action with regard to such information because, although they *did* have such a claim, by virtue of making such information public they have *waived* that claim—that is, they have absolved us of any obligations that we were previously under with respect to their right to privacy about *that* piece of information. Thus, whether a piece of now-public information is public by virtue of its always having been public, or whether it is public by virtue of some action of the right-holder, individuals have no legitimate claim over our actions. In turn, we might reasonably conclude that there are only two kinds of information—private information and public information—and one's right to privacy (and the duties it engenders) covers only that information currently held in private.

In our view, however, there is good reason to think the situation is more complicated than this. In particular, one salient fact seemingly missed by this account is the question of how a piece of once-private, now-public information came to be in the public sphere in the first place and, in particular, whether it was the result of an intentional action by the rights-holder or an unintentional one. For her own part, Thomson notes this possible consideration when detailing the five cases referred to at the beginning of this article, yet she also takes it to be irrelevant. Thus, for Thomson, regardless of whether such information was made public intentionally (as in cases (1), (2), and (3)), or unintentionally (as in cases (4) and (5)), one has 'waived' whatever privacy rights one had over such information.

Yet the idea that cases (1)–(5) are morally equivalent seems wrong. In particular, it seems odd to claim that one could waive a right unintentionally. Rather, if one is to waive a right, one would seem to need actually to waive it—the very notion of 'waiving' implying an intentional action on the part of the relevant agent with regard to their right.

One thing Thomson might mean here—which seems right—is the idea that one could, through a series of unintentional actions, render certain obligations engendered by a right *defunct*, which is to say, impossible for any relevant duty-bearers to fulfil. It appears to be something like this idea that Thomson wants to get at in case (4), where the visitor appears to be precluded from fulfilling their duty *not* to look at the picture because they have no option *but* to look.[26] Yet there is a gap between unintentionally rendering defunct certain obligations engendered by a right and waiving that right. In particular, where waiving one's right to something might be seen to absolve duty-bearers of all their obligations engendered by that right (or, if specified, some explicitly demarcated set of obligations), from the fact that, by one's action, one renders some set of

[26]We note that in Thomson's original formulation of the example it is not that the visitor has no option *but* to look, but rather that they would 'have to go to some trouble to avoid looking at it'. We note the vagaries around what constitutes being able *not* to look and the idea of a certain set of obligations being effectively defunct in Section V.

obligations engendered by one's right *defunct*, it does not seem to follow that one renders all such obligations defunct, but rather only those that it is now impossible to fulfil. Returning to (4), then, simply because I have unintentionally created a situation where you cannot help but see the picture, thereby making it impossible for you to fulfil your duty to refrain from appropriating that information, it does not mean you are therefore absolved of all your duties engendered by my right to privacy—say, your duty not to disseminate its contents to others—for, of course, nothing about my actions, intentional or otherwise, has made fulfilling *those* duties impossible.

In some cases, this also seems true of one's duty not to appropriate some bit of information. For example, imagine your neighbours are having a highly personal, but also very loud, argument that you cannot help but overhear. Given the context, you know that your neighbours have absolutely no intention of broadcasting their discussion, perhaps being unaware how loudly they are talking, or that their windows are open, or that you are at home. What, then, are your obligations towards them? For Thomson, of course, there are none (at least, no obligations that could be understood in terms of their right to privacy).[27] However, we might think that, even if they are talking loudly, so loudly that it is impossible not to hear that they are having an argument, it would still be wrong of you to pay too close attention to precisely *what* they are saying. If you are to respect their privacy, you still have an obligation to refrain from attempting to appropriate the content of their discussion, to adopt a kind of wilful deafness to a conversation that, as far as they are aware and as far as they intend, remains private.

What all this suggests, of course, is that there may be some pieces of once-private information that have found their way into the public domain, but in respect to which a rights-holder has not waived their right nor, indeed, necessarily rendered defunct all our obligations engendered by that right. And, from here, it also becomes clear that, contra Thomson, the mere fact that a piece of information is *within* the public domain does not therefore imply that one is under no obligations with respect to it, for it may be that the relevant rights-holder never waived their right over that information.

One likely concern one might have with this view is that it makes the ethical situation with regard to once-private, now-public information much more complicated than accounts such as Thomson's would suggest. This is correct, in ways we will shortly go on to detail. However, we would argue that it also elucidates situations which we might otherwise consider somewhat murky. Take the case of a wrongly addressed email. One receives a salacious email that

[27]Thomson discusses a very similar case: 'Suppose that my husband and I are having a fight, shouting at each other as loud as we can; and suppose that we have not thought to close the windows, so that we can easily be heard from the street outside. It seems to me that anyone who stops to listen violates no right of ours; stopping to listen is at worst bad, Not Nice, not done by the best people'; Thomson, 'The right to privacy', p. 296.

was clearly intended for another party. Should one read it? Would it violate the sender's right to privacy to read it, or to send it on to others? Interestingly, whenever this case is discussed, commentators often suggest that one's obligations are 'unclear', that 'our intuitions pull us in different ways', and that there is 'extensive disagreement' about where one's duty lies. However, we would argue that the situation is clear: of course one should not read it,[28] let alone disseminate it to others.[29] Certainly, the mere fact that someone has failed to keep private what they hoped to keep private does not give one carte blanche with regard to any information they have inadvertently disclosed.[30]

Indeed, as well as clarifying our obligations in these kinds of cases, the foregoing analysis also provides something of an error theory as to how we came to think such cases were troubling in the first place. That is, we might think that our confusion about what we ought to do in these kinds of cases can be traced directly to, on the one hand, a philosophical model that tells us that we *have* no obligations with regards to public information, and, on the other, a set of intuitions that claim the exact opposite—just because the sender sent the email accidentally does not mean that you are thereby absolved of your duty to respect their right to privacy.

III. DUTIES REGARDING INFORMATION OBTAINED THROUGH ANALYSIS AND INFERENCE

Let us take stock. One way in which one might read the previous section is as setting out a new model of how individuals manage their rights within a relevant domain. Within this model, individuals are taken to hold certain rights, from which it follows that there is a continued obligation on the part of duty-bearers to respect and fulfil those rights. Right-holders may also, through *intentional* action, *waive* their rights, which is to say, absolve relevant duty-bearers of their duties

[28]Plainly, this is not to say that we would never read it (simple curiosity being a powerful urge to resist). But even if nine times out of ten we would read the email, that would not show that there is nothing wrong about reading it.

[29]There is an interesting question about the relative stringency of our different obligations here. Is our obligation not to send the email on to others (dissemination) more stringent than our obligation not to read it (appropriation)? The way we phrase the sentence above suggests that it is. However, this might not necessarily always be the case. One can imagine cases, for example, where our appropriating a piece of information another wanted to keep private would be worse than disseminating it. (Here we might think, for example, of a piece of information a loved one wanted to keep from us, yet which they would not care if anyone else knew—say, the fact that they were adopted.) The question of whether the right to privacy engenders obligations of differing strengths and, if so, whether these are codifiable or context-dependent, is a fascinating area for future discussion but one which, unfortunately, there is not the space to enter into here.

[30]The same point holds for rights generally, and is not confined merely to the right to privacy. Suppose I am going away on holiday, and entrust the key to my house to a neighbour so that he can water the flowers in my back garden. The garden also contains a swimming pool—and the key gives access to this space. So giving the neighbour access to the garden for the purposes of watering also gives him easy opportunity to use my swimming pool. But if he did so in a way that went against my intentions, that would nonetheless count as a violation of my property right. Thanks to a referee for forcing us to be clearer on this point.

with regard to those rights. They may also, through *intentional* or *unintentional* action, render their rights *defunct*, which is to say, make it impossible for relevant duty-bearers to fulfil their duties with regard to those rights. What they may not do is *unintentionally waive* their rights, which is to say, accidentally absolve duty-bearers of their rights. As we have seen, this model may be applied straightforwardly to how individuals manage their right to privacy: in different situations and through different actions individuals may hold, waive, or render their rights to privacy defunct.

Let us now consider information gained through analysis and inference. As stressed by Manson and O'Neill, one complicating factor around the ethics of privacy is that information used in thought, communication, and action does not fall into discrete types. Rather, it may be considered 'inferentially fertile':

> Knowing that your neighbour smokes heavily—which may be public knowledge and readily accessible—allows you to make quite robust inferences about her probable future health. Sometimes we can infer what is taken to be personal information on the basis of information that is taken to be non-personal, indeed public.[31]

This inferential fertility raises a further question about the duties engendered by the right to privacy: namely, what are our obligations with regards to information that a person may wish to keep private (X), but which we are able to infer from information they have made public (Y)?

Thomson's response to this is, again, uncompromising. That is, since any information X one is able to infer from public information ultimately originates in information that P has put in the public domain (whether intentionally or not), appropriating or transmitting such information does not violate any right of P's, even if that information is identical to information P wished to keep private. Again, just because P may not have known that by divulging Y she was therefore also divulging X, *that* does not mean that our uncovering X through analysis of Y violates her right to privacy, for by putting Y in the public domain, P has waived her right to privacy over it and anything that may be inferred from it, irrespective of whether that act of publicity was intentional.

On our model, however, we see that the inferential fertility of information adds another layer of complexity to the picture. That is, if we assume that there is a certain class of information that, though possible to infer from information P has intentionally made public, is nonetheless information that they did not intend to make public, we appear to create a new class of information and a new set of duties around it. Previously, then, we had:

1) Private information (or information held 'in private');
2) Information that has always been public;

[31]Manson and O'Neill, *Rethinking Informed Consent in Bioethics*, p. 104.

3) Once-private information an individual has intentionally made public; and,
4) Once-private information an individual has unintentionally made public.

In the prior section, we argued that the right to privacy covered (1) and (4), did not cover (2), and had been waived with respect to (3). However, the inferential fertility of information suggests a new set of categories related to (3) and (4).

5) Information inferred from once-private information that an individual has intentionally made public *and which itself counts as a piece of information that the individual intended to make public;*
6) Information inferred from once-private information that an individual has intentionally made public *but which does not count as a piece of information that the individual intended to make public*; and,
7) Information inferred from once-private information that an individual only made public unintentionally.

Our view, then, is that right to privacy continues to track the extent to which an individual *intended* to make a piece of information public. Thus the right to privacy continues to be waived in the case of (5) and continues to cover (7). However, it also covers (6), which is to say, information inferred from information that an individual has intentionally made public, but which does *not* count as a piece of information they intended to make public. This puts the idea obscurely, but it can be rendered in a fairly simple example. Imagine Annabel. Annabel is a famous actress. She also suffers from a rare and very hard to diagnose genetic disorder, a piece of information about herself she wishes to keep private. One day, Annabel agrees to take part in a new medical initiative. The primary purpose of the initiative is to promote the donation of genetic code for research purposes. As a participant in the initiative, Annabel agrees to donate her DNA to medical science and, to allay the public's worries about genetic research, even agrees to post it on the internet, together with a note advertising the fact that it is hers. Unbeknownst to Annabel, however, by posting this information on the internet, Annabel also makes it possible for those trained in genetic medicine to deduce that she suffers from her rare genetic disorder. Brian is one such researcher and, having studied Annabel's DNA, decides to go to the papers to publicize that fact.

In this case, Thomson, and those who follow her, would argue that there is nothing wrong with Brian's actions, at least with regard to Annabel's rights. By posting her genetic code on the internet, Annabel has waived her right to privacy over both that information and anything that may be inferred from it, even if, when she originally posted her genetic code, she did not intend to disclose the fact she suffers from a rare genetic disorder. By contrast, we argue that, despite the fact that Annabel intended to publicize the contents of her DNA, by virtue of the fact that she did not intend thereby to publicize the fact

she suffered from a rare genetic disorder, Brian's actions still count as a violation of her right to privacy.[32]

This argument, we feel, tracks our normal judgements about Brian's actions. That is, we seem to feel that by publicizing Annabel's condition, Brian does something wrong and, in particular, that he wrongs Annabel. However, it is also clear that at this point our model faces certain difficulties. For example, imagine that, rather than posting her DNA on the internet, during a party Annabel happens to bump into Sherlock Holmes. As the world knows, Holmes is a master of both observation and deduction and, during their conversation, he is able to deduce by mentally interrogating a series of stories Annabel tells him that she suffers from the rare genetic condition that she has tried so desperately to keep private. What kind of duties might Holmes be under at this point? On our model, it is not just that Holmes is under a duty to refrain from publicizing Annabel's condition but, perhaps more surprisingly, that he infringes (possibly even violates) Annabel's right to privacy insofar as he makes any effort to deduce the nature of Annabel's condition in the first place (to 'appropriate' it from information Annabel makes public).

This example is clearly somewhat fanciful; however, it seems to map a whole host of comparable scenarios involving big data analytics, as we explore in Section VI. Moreover, although none of us, perhaps, possesses the same keen eye as Sherlock Holmes, nor is as accurate in the inferences we draw from our observations, we are also constantly in the process of making inferences based on the information before us, inferences which may lead us to deduce certain pieces of information others had hoped to keep private, but which they have unwittingly divulged through various public utterances and actions. Picking up on a colleague's change in dress and demeanour, you rightly conclude that they are in a new relationship. Reflecting on various cues given over a recent family meal, you deduce that your sister has lost her job. Tasting a friend's coq au vin one evening, you correctly surmise that they did not spend their summer training to be a cordon bleu chef as they claimed and that they must have been doing something else entirely. Are we really saying that all such examples infringe an individual's right to privacy?

The worry here, then, is not that any of these examples *refute* our model, but rather that, put together, they seem to suggest it is *too expensive* in the sense that

[32]One instinctive reaction to this is to claim that Annabel is just daft. How could she not have realized that by posting her genetic code online she would also thereby be making it clear to anyone with the requisite skills and knowledge that she was suffering from a rare genetic disorder? 'Genetic' is in the name! Following this, we might even be inclined to think that whatever right to privacy Annabel had, she has surely forfeited such a right by virtue of her stupidity—that she 'gets what she deserves'. However, irrespective of questions of desert, and although we might chastise Annabel for her naivety in this situation, it is far from clear that, simply by virtue of that naivety, we should also think she has somehow forfeited her right to privacy. After all, one does not forfeit one's right to private property simply by absent-mindedly leaving one's car keys in one's car. Failing to act in a way that ensures, as far as possible, that the car will not be stolen does not somehow mean that the car is no longer *ours*, or that we cannot make reasonable demands on others by virtue of our rights over it.

it renders too many actions ethically unacceptable. In responding to this concern, it is worth separating out two different kinds of cases: first, cases in which we, as duty-bearers, *know* that a piece of once-private information *is* private *and* that the relevant right-bearer has only made it public unintentionally; and secondly, cases in which we do not know either whether a piece of once-private information is private *or* whether the right-bearer has made it public intentionally or unintentionally. In the rest of this section, we respond to the first set of cases. We deal with the second in the next.

In those cases, then, where we, as duty-bearers, know that a piece of once-private information *is* private *and* that the relevant right-bearer has only made it public unintentionally, we find ourselves ready to bite the bullet. That is, insofar as P has been attempting to keep a given piece of information private and we, as duty-bearers, know this, we believe that it would infringe her right to privacy were we to appropriate it by inferring it from information she has made public (intentionally or not). She has a right, as Marmor would put it, to have a reasonable measure of control over which 'self' she presents at any given moment to any given audience. By interrogating, then, your sister's public behaviour and disseminating any inferences you draw ('she has lost her job'), you infringe your sister's right to privacy (assuming, that is, that such information is covered by those rights).[33]

However, if this seems a radical claim, a few things may be said in mitigation. First, by virtue of natural psychology, it looks as though there are going to be countless cases in which we cannot help but infer something about someone based on the information before us. In the case of our friend's claim to have spent the summer training to be a cordon bleu chef, then, we might think that it is simply not possible for us to refrain from drawing an inference about the truth of that claim having tasted their coq au vin. To taste the dish is to know. Thus, following the analysis offered in Section II, we might similarly think that, in this case, our friend has unintentionally rendered our duty *not* to appropriate that information defunct. It is the equivalent of it being impossible 'not to look'.

Secondly, in asserting that individuals' rights to privacy can cover information that may be inferred from information they have (intentionally or unintentionally) made public, we are not saying that duty-bearers are under a

[33]A wonderful example of this duty not to pry is given in Jane Jacobs's *The Death and Life of Great American Cities* (New York: Modern Library, 1993), p. 78. Here, in a discussion of the importance of privacy in cities, Jacobs gives the example of Joe Cornacchia, a local delicatessen owner who looks after the house keys of local people while they are away: 'In our family, for example, when a friend wants to use our place while we are away for a week end or everyone happens to be out during the day, or a visitor for whom we do not wish to wait up is spending the night, we tell such a friend that he can pick up the key at the delicatessen across the street. Joe Cornacchia, who keeps the delicatessen, usually has a dozen or so keys at a time for handing out like this . . . Now why do I, and many others, select Joe as a logical custodian for keys? Because we trust him, first to be a responsible custodian, but equally important because we know that he combines a feeling of good will with a feeling of no personal responsibility about our private affairs. Joe considers it no concern of his whom we choose to permit in our places and why.'

corresponding duty to refrain from making *judgements* about individuals based on their public utterances and behaviour. It may be, for example, that individuals wish to present themselves not only as people with a certain history, but as persons of a certain character—morally upstanding, perhaps, or wise, or modest, or athletic. However, whether or not someone *is* a person of a certain character, whether they are moral or wise or athletic, is not, strictly speaking, a piece of private information. It is not something that they hold and which they may choose to divulge to certain people and not others. Rather, it is something we, the moral community, decide about *them*. As such, although the right to privacy might cover information about an individual's actions and history we can infer from their public utterances and behaviour, it does not cover the judgements we may make on the basis of those utterances and behaviour.

Finally, it is important to note that, in saying that certain actions 'infringe P's right to privacy', we are not claiming that such actions necessarily *violate* P's right to privacy, which is to say, that they are always overall wrong, all things considered. Rather, in our view, even though φ-ing may infringe P's right to privacy, it might still be overall justified, given the other moral considerations at play. For some, of course, this will make little sense. For example, for those who are committed to an especially stringent conception of rights, who take rights to routinely 'trump' other moral considerations, insofar as φ-ing infringes P's right, it is necessarily always (or nearly always) all-things-considered wrong, for it is just part of what it means for P to have a right to φ that it cannot be overridden by alternative moral considerations (or can only be so overridden in a small minority of cases). If, then, telling others that your sister has lost her job infringes her right to privacy, it is always (or almost always), all-things-considered morally unacceptable, even if it is done with her best interests at heart.

Our own view takes rights to be much less stringent than this. That is, we would argue that there are a range of situations in which an individual's right to privacy may be permissibly overridden in the face of alternative moral considerations. Thus, if one believes that it is in one's sister's interests that the family know she has lost her job, perhaps so they might be able to support her better, then, on our view, it may well be morally acceptable to share this information with that group, even though it infringes her right to privacy. Similarly, we might think that a detective is justified in uncovering certain aspects of a suspect's private life in the course of their investigations, even if it infringes their right to privacy, and so on and so forth.

In this way, the present model of the right to privacy might be considered to be partly dependent on a conception of rights that takes them to be less stringent than is commonly supposed; or, at least, is far more attractive as a theory insofar as one also subscribes to a less stringent conception of rights. Yet this should not be taken as a strict logical entailment. Rather, one may subscribe both to an absolutist conception of rights and the model of the right to privacy described here; it is simply that insofar as one does, one is forced to accept that far more

agents are engaged in far more unethical behaviour than if one were to marry it with a less stringent conception.

IV. OUR OBLIGATIONS WHERE THE ETHICAL STATUS OF THE INFORMATION IS UNCLEAR

Thus far we have argued that the right to privacy covers not only private information, but also once-private information that a right-holder has unintentionally made public, the latter class including any information they were unaware could be inferred from information they *have* intentionally made public, and would not have otherwise released. We believe that this description of the scope of the right to privacy is the right one, following necessarily from a set of intuitive judgements about when someone can be said to have waived their right. Yet there are undoubtedly drawbacks to this model. First, it complicates the ethical permissibility of using public information insofar as it suggests that some uses of public information are ethically unacceptable. Whether one takes rights to be more or less stringent as moral considerations, it also suggests that a lot of behaviour we might once have thought acceptable is, in reality, unacceptable. Perhaps most pressingly, however, it also creates a certain ambiguity about the nature of our obligations when the ethical status of the information is unclear. What are we to do when we do not know whether a person has made a piece of information public intentionally or unintentionally, or, indeed, whether it is a piece of private information at all?

One problem here is that insofar as one thinks that the appropriation or dissemination of once-private information *may* infringe one's right to privacy, one might also think that we ought to refrain from the appropriation or use of *any* public information where we are unsure whether that information has been made public intentionally. To follow such a principle would ensure that we will always protect individuals' privacy-related interests. However, it also has the unhappy consequence of effectively prohibiting all intentional (that is, non-instinctive) analyses of once-private information. Not only might we think this comes at huge social cost, we might also think it runs afoul of common-sense morality. That is, it just does not seem to track our normal thinking about public information that we should *never* appropriate or disseminate it on the slim risk it may once have been private and has only been publicized unintentionally, even where we have no good reason to believe that this is the case.

Does, then, our model of the right to privacy lead us down an ethical dead end? Not necessarily. The point where this reading goes wrong, it seems, is in its assumption that the fact that the appropriation or dissemination of once-private information *may* infringe one's right to privacy necessarily engenders an obligation to refrain from the appropriation or use of *any* public information where we are unsure whether that information has been made public intentionally or not. Rather, we might think that the duties engendered by the

right to privacy stop short of requiring duty-bearers to do *that*.[34] In Marmor's model of the right to privacy, this limit is captured in his reference to the idea that rights-holders only have a justifiable claim to a 'reasonable measure of control' over the ways in which they present themselves, and what is theirs, to different people.[35] Similarly, we might think that individuals' right to privacy does not engender an obligation on the part of duty-bearers to refrain from the appropriation and dissemination of *any* now-public information that *may* have been publicized by a right-holder unintentionally. Rather, we might think that it only requires them to refrain from the appropriation and disclosure of information that *they have reason to think was once private, and which the relevant right-holder would have wanted to keep private*. In this way, then, whether or not Q's actions infringe or even violate P's privacy rights depends in part on what Q could reasonably have expected P's concerns were with regard to once-private information that now finds itself in the public domain.

As with Marmor's qualification of how much control we may rightfully demand with respect to how we present ourselves to others, there is something a little 'rough and vague' about the use of reasonableness here. However, we feel it again tracks our normal judgement about the relevant class of cases. In the case of Annabel, then, we might reasonably expect that Annabel would not have wanted the fact that she suffers from her rare genetic disorder to be widely publicized, even when she has posted her DNA profile online (simply by virtue of the fact that people do not generally like their medical histories being made public). In forwarding such information on to the media, then, Brian fails to abide by his moral duty—he had good reason to think that that piece of information *was* private and that Annabel would have wanted to keep it private. At the same time, however, we can easily imagine a host of further information capable of being inferred from Annabel's DNA profile that we would not normally expect her to want to keep private (for example, the colour of her eyes and the likely colour of her children's eyes, the fact that she has 23 pairs of chromosomes, and so on). Accordingly, Brian cannot be said to be failing in his duties with regards to Annabel's right to privacy if he publicizes *that*.

From this, though, we can also recognize that there will be some cases in which a conscientious agent, taking the utmost care to respect an individual's right to privacy, will still get it wrong about what that individual intended or did not intend when they made a certain piece of information public. In some, fairly benign, cases (at least with respect to the interests of the subject of the disclosures), she will refrain from publicizing information that the individual did not actually intend to keep private. In other, more troubling, cases, she will

[34]One way to cash this out would be to say that it is not by virtue of *any* aspect of X's well-being that Y may be held to be under some duty to them, but rather only those aspects of X's well-being that provide a *sufficient reason* for holding Y to be under such duties. Cf. Joseph Raz, 'The nature of rights', *Mind*, 93 (1984), 194–214.

[35]Marmor, 'What is the right to privacy?', p. 6.

publicize information that the individual *had* hoped to keep private. However, as above, although the latter sorts of cases are cause for regret in the harm they do to P, we do not believe that they violate P's rights. For P cannot really be said to have a right to privacy over information that is currently public (or has been inferred from information that is currently public), and which no one could have any reason to think they wished to keep private—even if they only made such information public unintentionally. In this final analysis, then, we tend to agree with Thomson, that an individual has no right to privacy over a private picture when they 'leave it somewhere such that nobody could be reasonably be expected to know it belonged to anybody' (Thomson's fifth case). However, where Thomson sees this as true by virtue of the fact that in such a case an individual has unintentionally 'waived' their rights to privacy, we see it as true by virtue of the inherent limits in the duties engendered by the right to privacy itself.

V. COMPLICATIONS AND CLARIFICATIONS

The model presented in this article gives rise to a number of questions and possible counterarguments. For example, much of our argument rests on the assumption that agents' actions fall fairly neatly into one of two camps: the intentional and non-intentional. However, while seemingly true of many cases of action, it is not clearly true of all action. What, for example, of information that the right-holder does not know if they would like publicized, or cases in which they have no real feelings either way? What if their feelings on the matter are mixed, making their subsequent actions ambiguous? Say, for example, one leaves a diary detailing one's suicidal thoughts out where a loved one can find it, half by accident but also, perhaps, half hoping that they will find it and realize how deeply unhappy one is. Should we consider such a disclosure intentional or not? In these kinds of situations we might think that there is a degree of indeterminacy about the extent to which a right-holder's action was intentional or not, leading in turn to an ambiguity as to what our duties are in respect to their rights.

Another area of indeterminacy relates to the question of when one's obligations around a particular piece of information become defunct. Take the example of the picture on the table (Thomson's fourth case). In Thomson's original formulation of this example, the idea here was not that it was *impossible* for the visitor *not* to look, but rather that 'they would have to go to some trouble to avoid looking at it'. Now, for ease of explication, in Section II we rendered this as being effectively impossible *not* to look, in order to make clear the idea that in certain situations, certain duties engendered by P's right to privacy may be rendered defunct. However, one might argue that in almost all cases we have some sort of choice *not* to look at a picture, even if it means walking around with one's eyes closed or refusing to pay attention to anything that one sees. As Thomson's depiction of the scenario makes clear, in most situations the point is that one would simply have to go to some trouble to avoid looking. We might

therefore conclude that one's obligations with regard to an individual's right to privacy become defunct not necessarily (or not only) when it is *impossible* for us to fulfil them, but also when fulfilling them would require such a burdensome set of manoeuvres on our part as to be somewhat unreasonable. Again, though, if this is the case, then it suggests a degree of ambiguity as to when the circumstances are such that fulfilling one's obligations with regard to P's right to privacy are sufficiently burdensome as to render them effectively defunct and when they are merely a burden that we are duty-bound to bear.

Another respect in which the current model may be questioned is in our apparent assumption that all the duties engendered by an individual's right to privacy are somehow on a par, which is to say, that it would be 'just as wrong' to appropriate a piece of information as it would be to share it with another, or that it would be 'as wrong' to share a piece of information under conditions of confidence as it would be to make that piece of information *truly* public—say, by posting it on the internet or shouting it from the rooftops. Clearly this seems false (and, indeed, we would argue that it is not actually an assumption of our account). Yet, if it is false, it suggests that the various duties engendered by a right such as the right to privacy may be of different normative standing to one another and to other moral considerations. In turn, this would appear to imply that, if rights *can* be overridden by alternative moral considerations, it may be that certain moral considerations are sufficient to override *some* duties engendered by the right to privacy but not others. The thought here, then, would be that 'catching a murderer' could conceivably justify a detective appropriating certain details of a suspect's life and the sharing of that information with certain other members of the police force, but not in appropriating *any* information about the suspect's life, nor in sharing *any* information with *any* other members of the police force or the public at large.

All these sets of issues look rich seams for further enquiry. However, without wanting to downplay them or others, given the confines of space we would like instead to make a few brief points on the idea of a 'reasonable expectation'.

One concern we may have with the present conception is that it can seem to suggest that the acceptability of the expectation (and hence the extent to which a duty-bearer's behaviour to P violates the right to privacy) is dependent on how far it accords with the cultural norms prevalent in their society. That is, Q could not be said to have violated P's right to privacy if she publicized once-private information that, given the social norms prevailing within her society, she had no good reason to think P would have ever intended to keep private.

In one sense, of course, the fact that the current model is socially relative in this respect might be seen as one of the features in its favour: since it is flexible in a way similar to Marmor's account, it is able to account for why the publicity of certain information may constitute a violation of privacy in certain societies but not others. Thus, Q's dissemination of a photo of P, a married woman, sitting in her garden with her hair down, might be read as a serious violation of her right to

privacy were it to be disseminated in a population of Orthodox Jews but not necessarily in other cultures. Yet this feature of the current model also carries certain problems, most notably insofar as it appears to discriminate against minorities. Returning to the example of Q disseminating a photo of P with her hair down, then, we may note that not only do cultural expectations about the privacy of hair differ widely, but so too does awareness of this variation. Say, for example, that as an Orthodox Jew, P considers Q's photograph of her to be both highly personal and private. But as, say, a British citizen living in a close-knit rural village in England, going by the social norms prevalent in her society, Q could not be reasonably expected to think that P would have wanted such a photograph to be kept private.[36] Yet this is exactly the opposite conclusion to the one we would draw were Q an Israeli citizen living in the Lower Galilee. In the former case, then, despite P's interests remaining the same and Q's actions being effectively identical, P has no justifiable complaint against Q, whereas in the latter case she does.

However, rather than suggesting a flaw in the present model, what this example alerts us to is perhaps the simple fact that what constitutes a reasonable expectation—and hence the limits of what an individual may justifiably demand of others with regard to their privacy—cannot be defined simply by the *most prevalent* norms within a given society. Rather, we might think that to constitute a reasonable expectation of what P intended to publicize, one would also need to consider the likelihood of P being a member of minority group and the norms held by such groups. Another guiding light here might be to consider how the act of publicity fits with the wider actions of the right-holder themself. That is, is there anything about P's wider actions that would give us a clue as to her intentions with regard to this act of publicity? Even this, though, is really just another way of saying that establishing whether or not P might have intended to make X public (and thus what constitutes a reasonable expectation about her wishes in this regard) might be as much about understanding the context in which the act of publicity takes place as the content of the piece of information in question.

VI. IMPLICATIONS FOR THE ETHICS OF BIG DATA

As a rule, we have tried to approach the questions raised in this article as generally as possible, which is to say, at a relatively high level of abstraction. However, before concluding, we would like to dwell for a moment on the implications of our model for our thinking about the ethics of Big Data.

To date, much of the debate around Big Data has focused on the ethical acceptability of linking and analysing large datasets of *private*, personal

[36]Unless, that is, they were aware that P was an Orthodox Jew and were familiar with Jewish customs around modesty, but we will assume for the purposes of this example that Q is entirely unaware of such facts.

information, often for some sort of public benefit.[37] Insofar as such practices seek to make use, without appropriate consent, of information that individuals (wrongly) believe private, we have generally taken the ethics around such practices to be fairly clear cut: namely, all such analyses are infringements of an individual's right to privacy.[38] However, a large field of modern data analytics also looks to interrogate personal information that individuals have made *public*. For example, analyses are routinely run on individuals' Twitter accounts and Facebook posts, both of which may be deemed (depending on the settings associated with the relevant accounts) 'public' information. As with analyses of private information posted on the web, such interrogations can lead to some fairly startling findings. Statistical models have been written to predict, with a high degree of probability, users' socio-economic status, voting patterns, even sexuality. Indeed, one recent research project—to which the authors are attached in an advisory capacity—attempts to predict whether or not Twitter users are suffering from seasonal flu through their use of certain key words in their tweets (the thought being that such information will allow for more effective public health interventions).[39]

Following the theory laid out above, one problem with Thomson's approach to privacy, in our view, is that it can make the ethics of these practices rather hard to discern. Like the case of the wrongly addressed email, on the one hand Thomson's model seems to make all use of such public information fair game. On the other hand, however, we seem to have a strong intuition that individuals cannot be considered to have waived all their rights to privacy just by virtue of having posted certain bits of information on the internet, especially when they may be entirely unaware of just how much information analysts are able to uncover by interrogating such information. Consider the case of 'Creepy', a computer program created to highlight the amount of information about our whereabouts we may be unintentionally broadcasting by uploading images containing geolocation tags:

> You can enter a Twitter or Flickr username into the software's interface, or use the in-built search utility to find users of interest. When you hit the 'Geolocate Target' button, Creepy goes off and uses the service's APIs [application program interface] to download every photo or tweet they've ever published, analysing each for that critical piece of information: the user's location at the time.

[37]Solon Barocas and Helen Nissenbaum, 'Big Data's end run around anonymity and consent', *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, ed. Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum (Cambridge: Cambridge University Press, 2014), pp. 44–75; Mireille Hildebrandt, 'Defining profiling: a new type of knowledge?', *Profiling the European Citizen: Cross-disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer Netherlands, 2008), pp. 17–45.

[38]Obviously, this is not to say that they are always unjustified, all things considered, or that there may not be other ways of ensuring such data is usable, e.g., anonymizing or pseudonymizing.

[39]Benedict Rumbold, Clare Wenham, and James Wilson, 'Self-tests for influenza: an empirical ethics investigation', *BMC Medical Ethics*, 18 (2017), 33.

> While Twitter's geolocation setting is optional, images shared on the service via sites like Twitpic and Yfrog are often taken on a smartphone—which, unbeknownst to the user, records the location information in the EXIF [Exchangeable image file format] data of the image. Creepy finds these photos, downloads them, and extracts the location data.
>
> When the software finishes its run, it presents you with a map visualising every location that it found—and that's when the hairs on the back of your neck go up. While the location of an individual tweet might not reveal much, visualising a user's history on a map reveals clusters around their home, their workplace, and the areas they hang out. Everything a stalker could need, in other words.[40]

As the author of this piece implies, it seems fairly intuitive to think that if we were to use a programme like Creepy to map P's movements, we would wrong P and, in particular, wrong her by violating her right to privacy. Yet this seems something that Thomson's model cannot allow.

One of the benefits of the theory presented in this article, then, is that it helps clarify the scope of individuals' rights in this regard: against the standard model, individuals' right to privacy is properly understood as covering not only private information, but once-private information a right-holder has unintentionally made public (the latter class including any information they were unaware could be inferred from information they *have* intentionally made public, and would not have otherwise released). From an analyst's point of view—one who is unsure of the ethical acceptability of a specific analysis of public information—this clarification is important for two reasons. On the one hand, it elucidates an important obligation owed by the data-analyst to the data-subject: refrain from the appropriation or disclosure of any information you think the right-holder would have wanted to keep private *even if it is already within the public domain*. On the other hand, it also reveals that not all analyses of once-private information are necessarily ethically impermissible: subject to meeting certain other conditions, analyses of data may still be morally permissible, provided they do not appropriate or disclose any information there is good reason to think the data-subject would have wanted to keep private.

In this way, then, the analysis of Twitter data to establish, say, whether or not users are suffering from flu may be considered ethically permissible, because it looks unlikely that such analysis will result in the appropriation or disclosure of any information that those users wished to keep private: we do not normally treat whether or not one is suffering from flu as a highly personal matter; suffering from such a disease carries no social stigma; and we know by virtue of the fact that users are tweeting *about* having cold-like symptoms (the data the analysis interrogates) that they are relatively relaxed about making such information known on a public forum. By contrast, cases such as Samaritans Radar, where the

[40]ITProPortal Website (2011), 'Creepy app signals an end to privacy', <http://www.itproportal.com/2011/03/30/creepy-app-warns-end-privacy/>.

analysis is used to detect suicidal thoughts, would be a violation of privacy, as most people *would* treat suffering from suicidal thoughts as a private matter. Even if, then, one *could* identify whether a Twitter user was suffering from severe depression from their tweets, there is good reason to think one *should not*, and certainly one should not disseminate such information.

One question this analysis remains silent on, perhaps, is the matter of identifiability, anonymization, and aggregation. That is, it might be argued that if the data is aggregated in large numbers and no effort is made to identify individual users—then such analysis would not violate any individual's right to privacy, regardless of whether it is 'appropriated' information that they would have preferred to keep private. However, while this looks a rich topic for future discussion, there is insufficient space to consider it in depth here.[41]

VII. CONCLUSION

Does appropriation, dissemination, or analysis of publicly available information violate one's right to privacy? In this article we have argued: maybe. That is, if such activities threaten information that an individual intended to keep private, then it may violate their right to privacy, even if it is already in the public domain. We have argued against one hugely influential model of the right to privacy which asserts that when one puts any information in the public domain—whether intentionally or not—one waives one's right to privacy, both over it and over anything that may be inferred from it. Rather, on our conception, one can only waive one's right to privacy by actually waiving it. This revision undoubtedly complicates our understanding of the ethical acceptability of certain practices, yet it also clarifies them, paying heed to intuitions that the traditional model finds difficult to embrace. And while it raises several new questions with regard to the philosophy of privacy, it also presents a powerful new rule for those looking to interrogate the growing mass of publicly available information: namely, do not appropriate or disclose any information that you have reason to think the right-holder wished to keep private.

[41]For some interesting analysis in this area, see Barocas and Nissenbaum's analysis of the 'tyranny of the minority' in 'Big Data's end run around anonymity and consent'.