Surveillance without 'Baddies'

Liability and Consent in Non-Antagonistic Surveillance Ethics

Lippert-Rasmussen, Kasper; Vrist Rønn, Kira

Published in:
The Ethics of Surveillance in Times of Emergency

DOI:
10.1093/oso/9780192864918.003.0007

Publication date:
2023

Document version:
Final published version

6

Surveillance without 'Baddies'

Liability and Consent in Non-Antagonistic Surveillance Ethics

Kasper Lippert-Rasmussen and Kira Vrist Rønn

According to one influential definition, surveillance is 'any systematic and routine attention to personal details, whether specific or aggregate, for a defined purpose' (Lyon 2014: 2). Most theorists assume that surveillance, so defined, is morally problematic when it is non-consensual, e.g., because of how it violates privacy rights. For present purposes, we shall simply assume that non-consensual surveillance is morally problematic. However, whether this is the case—and if so, why—is a huge question in itself.[1]

The majority of scholars exploring the ethics of surveillance primarily address the issue in antagonistic contexts—roughly, contexts in which a wrongful aggressor intends to harm or wrong an innocent victim, and a rightful defender surveils the aggressor to prevent the harm or wrong. Examples of such contexts include counter-terrorism and crime prevention/crime detection (Kleinig 2009; Lyon 2014; Macnish 2014, 2015; Marx 1998). Accordingly, many scholars have drawn on distinctions from the ethics of war and self-defence in order to develop a framework for surveillance ethics (Bellaby 2012; Kleinig 2009; Macnish 2014, 2015; Nathan 2017; Rønn and Lippert-Rasmussen 2020).[2] Such frameworks naturally focus on considerations regarding the *liability* of the surveilled and how it affects the moral permissibility of surveillance.

[1] First, theorists distinguish between *bodily privacy* and *informational privacy* (Solove 2008; Tavani 2008). Second, surveillance scholars distinguish between informational privacy violations as being a question of either *loss of control* of private information or someone *accessing* this information for a defined purpose (Macnish 2018). Third, scholarship specifies different forms of 'bads' and 'wrongs' related to surveillance, e.g., the loss of freedom and the (potential) abuse of power that is facilitated by collecting and storing citizens' (personal) information (in democratic societies) (Stahl 2016). For present purposes, we need not go into the complications raised by these three distinctions, since whichever aspect of privacy or harm one focuses on, pandemic-related surveillance may infringe such aspects of privacy, and give rise to relevant kinds of harm. However, not all uses of Covid-19 tracking apps violate privacy rights (however construed) (see section: 'Why Consent Might Matter').

[2] Some scholars are sceptical about transferring the distinctions from the ethical theories on self-defence and just war to surveillance (see, e.g. Diderichsen and Rønn 2017; Lever 2016; Stoddart 2014). It is beyond the scope of this chapter to address this scepticism.

Kasper Lippert-Rasmussen and Kira Vrist Rønn, *Surveillance without 'Baddies': Liability and Consent in Non-Antagonistic Surveillance Ethics* In: *The Ethics of Surveillance in Times of Emergency.* Edited by: Kevin Macnish and Adam Henschke, Oxford University Press. © Oxford University Press 2023. DOI: 10.1093/oso/9780192864918.003.0007

The Coronavirus pandemic, which presents a potentially lethal threat to the affected individuals, motivates broadening the focus of the ethics of surveillance to non-antagonistic contexts. The reason for this is that one way of reducing the spread of Covid-19 is through the use of various surveillance methods. In this chapter, we will focus on the use of Covid-19 tracking apps or, more generally, infection tracking apps. While Covid-19 is the first occasion on which such surveillance devices have received significant attention, other pandemics or more run-of-the-mill infections, e.g., the common flu, raise essentially the same issues as the Covid-19 pandemic, though the stakes might typically be lower or unfortunately, in some future pandemics, higher. Such apps are intended to warn people against close contact with infected individuals, facilitate identification of anyone who has been in contact with somebody infected, and ensure appropriate testing and self-isolation (Stanley and Granick 2020). Many different versions of such apps exist, and the risks related to these innovations vary depending on the specific design concerned.[3]

In infection-related surveillance contexts, there is no human *aggressor* and, therefore, no antagonistic relationship between *the surveillant* and *the surveilled*. Accordingly, many might find it unclear that anyone is liable to any form of intervention that, in the absence of actions for which they are responsible, would constitute a wrongful intervention against them. Accordingly, in the next section, we address the question of whether and in what form liability plays a role in surveillance ethics in the context of pandemics. Can persons who are not responsible for catching an infectious disease, and who do not intend to harm or wrong others by transmitting it, be liable to surveillance because they pose a threat? If so, are they innocent or culpable threats? We argue that infection-bearers—and, for that matter, people who think that they might be bearers of an infection, but in fact are not—can very easily become liable threats by failing to minimize the risk they pose to others. In failing to do so, they become culpable threats and, therefore, liable to certain forms of intervention that would otherwise wrong them. We refer to these as *negligent, liable threats*. We focus on liability to surveillance through infection-tracking apps. However, tracking apps in themselves might do little to mitigate epidemics. People need to act on the information obtained by such devices, e.g., by taking a test and by self-isolating if the test is positive. If they do not take such steps voluntarily, in our view they might become

[3] In general, a core distinction between the types of infection-tracking apps is whether they store all collected information on citizens' movements and infection status in a central register or in decentralized locations, only accessible to individual phone users. The centralized version enables the authorities to follow closely both the development in infection rates and the attitude and behaviour of citizens (Stanley and Granick 2020). It also enables a type and range of surveillance that is unfamiliar in democratic societies and creates a significant vulnerability, namely the risk of hacking of such registers and misuse at the hands of the authorities (Stahl 2016). Many liberal democracies have opted for the decentralized version. In this chapter, we focus our attention on the use of tracking apps in liberal societies, where the risk of information being misused is relatively low.

liable to involuntary testing or quarantine. We believe liability extend to such measures as well in case they are not taken voluntarily.

Our argument in the third section raises the question of the moral significance of consent in relation to infection-related surveillance. In this context, however, a dilemma might easily arise. On the one hand, the developers and health authorities in many countries emphasize that *consent* on the part of the users of Covid-19 related apps is a crucial concern. On the other hand, widespread use of the app—and, of course, appropriate precautionary measure typically being taken in response to the information being provided through the apps—is necessary to achieve the desired effect (according to Oxford researchers, around 80 per cent of the population should download the app) (Vaughan 2020), yet such levels of usage are unlikely to be achieved if consent is required.

The third section argues that the alleged trade-off between the effectiveness of surveillance-based means of fighting infections—or, more generally, non-antagonistic surveillance contexts—on the one hand, and accommodating concern for people's consent on the other, is much less of a dilemma than it might otherwise have been. This assumes that many, if not most, who do not use infection tracing apps are culpable threats. As such, these people are not wronged by surveillance measures being imposed upon them, regardless of whether they consent to these measures.[4]

The third section might give the impression that we think that, morally speaking, there is no reason to favour voluntary infection surveillance measures over non- or involuntary surveillance measures, or that consent to surveillance is morally irrelevant. The penultimate section cautions against this impression in two ways. First, it argues that offering the surveilled the option to consent can make a difference to what it is possible to do to the surveilled without wronging them. Second, even setting aside considerations about wronging, offering citizens the option to consent might have inherent moral value. In relation to discussions of the morality of paternalism, it is generally thought that paternalistic policies are disrespectful because they send the message that the state deems citizens incapable of doing what is best for themselves, or at least unlikely to do so. We argue that if that is the case, then the state similarly treats citizens disrespectfully by not offering them the option of consenting to infection related surveillance, and by sending the message that they are incapable of making the morally right choice, or

[4] Jeff McMahan (2009: 159) defines culpable threats as 'people who pose a threat of wrongful harm to others and have neither justification, permission, nor excuse'. Also, according to McMahan's (2009: 10) account, people are liable to attack, or other unwanted interventions, when the circumstances dictate that they have forfeited their rights not to be subjected to this treatment. One can be liable without culpability, e.g., if one innocently poses a threat of wrongful harm to others, as in McMahan's (2009: 165) example of the conscientious driver whose car unpredictably veers out of control and towards a pedestrian.

at least unlikely to do so. This might not amount to wronging citizens, but it might still be morally unjustified.

The final section briefly concludes by summing up our main claims regarding the moral justifiability of infection tracking apps in general, and Covid-19 tracking apps specifically.

Liability of (Potential) Infection Bearers

As already noted, many discussions of the ethics of surveillance draw on the ethics of war and self-defence. The paradigmatic case that such ethical theories address is one in which an aggressor (a state or an individual) wrongfully attacks a defender (another state or individual). Most agree that in such cases, the defender is morally permitted to do things to the aggressor that, in the absence of the aggression, would have wronged the aggressor, notably using lethal force to thwart the attack. One central explanation of why this is morally permissible is that the aggressor poses an unjust threat, and thus has become liable to defensive force (Clark 2000; Uniacke 2011). The aggressor has unjustly made it the case that, unavoidably, someone or other will suffer harm, and justice requires that this harm befalls the aggressor who made it unavoidable, rather than someone else. This means that the aggressor's rights, e.g., to life, are not violated when the aggressor is killed in proportionate self-defence and has no moral complaint against the defender's use of lethal force against them. Alternatively, if the defender could save their life by attacking an innocent bystander, this would not be permissible. An innocent bystander does not pose any threat to the defender and is therefore not liable to the use of any force (McMahan 1994; 2009). Hence, liability is crucial to the principle of discrimination, i.e., that lethal (or at least severely harmful) force can only be used against aggressors/combatants, and not against bystanders/civilians.[5]

If we move from the context of war and physical aggression to surveillance in counter-terrorism or crime prevention/crime detection, i.e., what we have referred to as antagonistic settings, it seems natural to assume that liability plays a similarly crucial role (Nathan 2017; Macnish 2015). Following McMahan, we assume that a person is liable to defensive harm if, and only if, he or she morally responsible for posing an objectively unjustified threat. Something resembling the principle of discrimination naturally applies to surveillance, too. In other words, there is a crucial difference between how, say, people who are (reasonably suspected of

[5] Liability is also central to the principle of proportionality. Theories of just war and self-defence generally assume that the use of force must be proportional. This means that the balance between the inflicted harms and the severity of the infringements in question, on the one hand, and the anticipated benefits, on the other, must be sufficiently favourable for the use of force to be justified.

being) terrorists or organized criminals might be surveilled, and how ordinary citizens might be surveilled, since, arguably, only the former are liable to surveillance (Nathan 2017; Rønn and Lippert-Rasmussen 2020; Stahl 2016). Similarly, liability also plays a crucial role in determining whether surveillance is proportionate (Kleinig 2009; Macnish 2014, 2015, 2018; Marx 1998; Nathan 2017, Rønn and Lippert-Rasmussen 2020). As with theories of just war and self-defence, it is the norm to distinguish between narrow proportionality (cases in which surveillance is directed intentionally at liable threats) and wide proportionality (cases in which surveillance is intentionally or unintentionally directed towards non-liable threats), and then focus on the former (McMahan 2009; Rønn and Lippert-Rasmussen 2020). Hence, liability is also central to surveillance ethics (cp. Diderichsen and Rønn 2017).

Turning now to surveillance in the context of infections and surveillance, some might find the idea that liability plays a significant role strange. The reason for this is not that, offhand, liability appears never applicable to this context. If I deliberately infect myself with, say, Covid-19 and seek to transmit the disease to as many vulnerable people as possible by deliberately coughing on them, it is natural to say that I am liable to surveillance (and even to harsher measures such as quarantine). However, the point is that generally speaking, hardly anyone would appear to be liable for Covid-19-related reasons. Unlike in our previous example, people are not, on the whole, morally responsible for becoming bearers of the disease—quite the contrary—and people do not generally seek to transmit the disease to others. Hence, in practice, it might seem that the distinction between liable and non-liable is largely irrelevant to Covid-19-related surveillance, as virtually everyone is non-liable.

However, this initial view is problematic. There are at least three ways to reach that conclusion. First, there is the straightforward observation that many people are in fact responsible for acting in ways which impose, and they are aware impose, a significant risk on others of transmitting the disease to them, e.g., by attending large gatherings or by refusing to wear masks and then interacting with others. Such behaviour plausibly gives rise to liability to modest interventions to prevent people from transmitting the relevant disease.[6]

Second, consider Robert Nozick's classic discussion of *innocent threats*. He imagines a person who is unexpectedly caught by a gust of wind and hurled down a well. At the bottom of the well is another person, who will be crushed to death when the falling person lands. The falling person, however, will survive unharmed. According to Nozick and many others, the person at the bottom of the well could

[6] There is a moral difference between liable to lethal force and liability to surveillance through infection apps in that, intuitively, more is required for liability to the former than to the latter much less harmful intervention.

shoot the innocent threat without violating the falling person's rights if doing so would somehow save their own life (Nozick 1974: 34).[7] One view here is that in this case, the innocent threat is liable to defensive harm, since the person at the bottom of the well has a right not to be killed. This right is infringed by the falling person, whose falling body is causally responsible for the threat to the person in the well (Thomson 1991). This is so even if the falling person is in no way morally responsible for his falling body posing a deadly threat to the person at the bottom of the well.

Many will find it highly implausible that facts for which individuals bear no moral responsibility can render them liable to deadly defensive force (Clark 2000). Still, if we accept this view—and some will argue that we must in order to be able to explain why it is morally permissible for the person at the bottom of the well to defend themselves—then a similar view applies in the case of infection-related surveillance. A person who is innocently unaware that she might infect others because she is innocently unaware of both the fact that she has Covid-19 and the fact that, relative to what she knows, she might infect others with Covid-19, is an innocent threat to others in much the same way as Nozick's person who is picked up by the wind and thrown into a well (Lippert-Rasmussen 2020). If we agree that we do, in fact, all pose innocent threats to others, since we could all potentially be infected with Covid-19, are we then allowed to infringe on, e.g., others' rights to privacy or other freedoms as self-defence against a morally innocent, but liable, threat? For instance, would it be possible to forcibly install tracking apps on smartphones without wrongfully violating the users' rights?[8] If we accept the analogy of the falling person in Nozick's example, the answer would be yes. Hence, we might reframe the analogy in the context of Covid-19, and claim that we all have a right not to be infected by others, and therefore it is permissible to infringe another person's (and our own) rights, e.g., the right to privacy, as an act of self-defence against the innocent but rights-violating threat that we all pose.

Some may find this line of reasoning problematic. For example, McMahan argues against the conclusion of the falling person example, asserting that 'a

[7] For reasons of space, we ignore the distinction between fact-relative and evidence-relative threats. If X aims an unloaded gun at you with the apparent intention of pulling the trigger, X is an evidence-relative threat (from your perspective), even if they are not one in the fact-relative sense. Since virtually all of us could be infected with Covid-19, virtually all of us are evidence-relative threats to others. We have slightly modified Nozick's original example, in which it is a villain who throws the bystander into the well, to avoid the moral complication to which the presence of a culpable human agent gives rise. Thomson exemplifies a similar point in a slightly different way. In her example, *the falling man*, a man is having a picnic on a cliff just above you (and unluckily, you cannot move, because your leg is stuck). A third person pushes the picnicking man off the cliff, and his fall will be lethal for you, but the man will survive. However, you can choose to unfold your umbrella, impale the falling man and survive (Thomson 1991).

[8] As an anonymous reviewer pointed out, governments might not even need to go this far. They could demand the data from the mobile phone companies, giving precise location of the phone at all times, thus, providing useful information for identifying and stopping disease transmission chains.

person cannot be morally constrained from being involuntarily acted upon by physical forces' (McMahan 2009: 388). However, others might not find this exchange particularly relevant, on the grounds that when it comes to Covid-19, most of us are not *innocent* threats to others. This is where the second argument to which we referred comes into play.

Consider a person who acts in a way that results in a significantly heightened risk that he or she might pass on the disease to others, e.g., because she refrains from installing a Covid-19 tracking device on her smartphone despite interacting with others in ways where she could transmit Covid-19 to them.[9] True, such a person is different from the paradigmatic aggressor in theories of just war and self-defence in that they do not *aim* to harm or wrong others. However, this might simply show that a threat can be non-innocent, and therefore liable to defensive force for reasons other than those at play in the paradigmatic cases of just war and self-defence theories. More specifically, it shows that an individual can become liable to defensive force through *negligence* (see McMahan 2009: 160).

Negligence can take many forms. The relevant form here seems to amount to an inappropriately limited concern for the vital interests of others, in order to avoid what is at most a rather minor setback of the individual's own non-vital interests. A person who refuses to install an infection-tracing app is perhaps a bit like one refusing to quarantine when told to and, therefore, knowingly exposing many others to the risk of infection. Or, to elaborate upon Nozick's well-known example, they are like a person who negligently ventures outside for no particular reason and refuses to download a 'wind gust-meter' on their smartphone that would prevent them from being turned into a human projectile and posing a risk to others.

At this point, some might object that it is somewhat ad hoc to claim that negligence can render the individual liable to the use of self-defensive force, even rather mild forms of self-defensive force, such as the compulsory installation of an infection-tracking app on a smartphone or compulsory test and self-isolation in relation to an infection-tracking app detection of a high risk of infection. However, this worry is ungrounded. In just war theory, a country can be a just

[9] While one can be liable to surveillance for reasons not having to do with the omission to download a tracking app, our view is that one's omission to do so is itself a source of liability and a factor that affects the degree of forceful intervention that one becomes liable to (see the discussion in the section on 'Consent of Liable Bearers of Infectious Diseases'). In a discussion of McMahan's view that a conscientious driver who is responsible for posing a threat to a pedestrian he is about to run down as a result of an unpredictable mechanical malfunction is liable to defensive force (see footnote 4). Quong (2020: 35) suggests, pace McMahan, that conscientious driving does not make on liable to defensive force, because the practice of driving is an advantage to everyone and is morally permissible despite the known fact that each year a number of pedestrians will be run down accidentally. This view applied to infections would imply that one does not become liable simply by interacting with others, thus, imposing a risk on a lethal infection on them. However, Quong's view would not apply to interacting with others without an infection tracking device, provided that this is an effective and costless way of avoiding imposing risk on others.

aggressor through negligence, e.g., by omitting to take proper precautions against accidentally launching missiles. Similarly, in theories of self-defence, if I start firing a gun in the direction of a bunch of innocent people—not to harm them, but simply to check whether the gun works—I become liable to defensive force intended to prevent the threat that I myself pose negligently. Indeed, this defensive force may be just as severe as it would be had I shot at them with the intention to kill.

Suppose that negligence can render people liable to the use of defensive force. This might not be particularly relevant to Covid-19-related surveillance if few of us ever negligently expose others to the risk of our transmitting the disease to them, or if the defensive measures in question were disproportionate. However, none of these suppositions seems true. First, we conjecture that most people at least occasionally interact with others while failing to observe the rules of social distancing, handwashing, etc., and know that they do so.[10] In addition, many people might negligently put themselves in a position where they risk being infected, e.g., by attending large gatherings (WHO 2020). In itself, this might not make them liable to any defensive measures. However, it might if, at the same time, they engage in behaviour that means they risk transmitting the disease to others. Second, the defensive measures in question—e.g., downloading a tracing app, submitting to a test if the app detects a high risk of having contracted the infection, and compulsory self-isolation for one or two weeks if the test is positive—are quite modest ones (in democracies at least, where risks of state of abuse are relatively minor) compared to the defensive measures normally justified in theories of just war and self-defence and in the light of the risks involved in contracting serious infections such as Covid-19. Naturally, being liable does not imply a *carte-blanche* for infection-related right-infringements. However, it will justify some forms of morally permissible (self-)defence against further infection, e.g., mandatory self-isolation. In this context, downloading a tracking app seems like a relatively easily justifiable intervention.

In the light of the above, we are inclined to infer that many of us, if not most of us, are indeed negligently exposing others to a risk of contagion. It therefore seems relevant, for a wide range of cases, to approach the issue of infection-related surveillance via the lens of just war and self-defence theory. If this is correct, it raises an important question about the significance of consent in connection with infection-related surveillance, which we will address in the following section.

[10] Admittedly, some people might be innocent threats. The exact number depends on the threshold required for innocence—e.g., whether an individual who acts according to official guidelines is a non-responsible threat, who arguably would be wronged if others intervened to prevent them from spreading Covid-19.

Consent of Liable Bearers of Infectious Diseases and Tracing Apps

Infection-tracking smartphone apps, which are intended to inform citizens about contact with infected persons, are one of the most common and widespread surveillance initiatives in the context of Covid-19 (Stanley and Granick 2020).

The developers and health agencies in many European countries attach great value to smartphone holders consenting to the use of these apps. However, developers and users in other countries attach less significance to whether users provide valid consent. For instance, in some countries, the state makes it impossible for citizens to perform certain acts that entail a risk of contagion, e.g., buying a train ticket, if they don't have the app on their smartphone or if the app classifies them as likely carriers of Covid-19 (see e.g., Dukakis 2020). If you're treated for Covid-19, healthcare authorities confiscate your smartphone and enter information regarding your health status. They even use the information provided by your app to identify and contact those with whom you have had contact, to force *them* to take a Covid-19 test. In the light of our discussion in the second section, the following question arises: does the consent-centric approach attach too much moral significance to valid consent on the part of users of Covid-19 tracking apps?

To see why this question is relevant, we must return to the ethics of war and self-defence. In this context, we argued that non-innocent, negligent threats are liable to defensive force and that most of us are negligent threats to others.[11] If this view is correct, then a corollary seems to be that there is no moral requirement that non-innocent threats consent to their being exposed to defensive force. The reason for this is that generally speaking, we do not have the right to refuse the imposition upon us of relatively minor forms of harm, etc., to prevent us from transmitting serious infections to others, which we have the moral power to relinquish. A crucial element that enables the possibility of giving normatively valid consent is missing. Consider a relevant and similar example from the ethics of self-defence. If I start firing a gun in your direction, with the aim of testing whether it works, you do not need my consent to tamper with my smartphone if that would somehow prevent you from being negligently shot by me. You do not even need my consent before it is permissible to return fire. Similarly, if I regularly venture out, despite having symptoms that could be indicative of Covid-19, or despite having recently been with others who have visited areas with high levels of contagion, then I impose a significant risk on you of contracting Covid-19. In that case, you do not need my consent to tamper with my smartphone to install a tracking device. Nor, if the tracking device indicates high risk of infection and you

[11] We also mentioned that according to some views, even non-innocent threats might be liable to defensive force. We are sceptical of this view. However, note that if it is correct, then that strengthens our scepticism about the significance of consent.

persist in imposing a high risk on others which they cannot avoid or can avoid only at great cost to themselves, do you need my consent to a quick test and, if the test is positive, to quarantine me for a limited period of time, if doing so would somehow significantly reduce your risk of getting infected with a potentially lethal virus.[12]

If we say that consent is not morally required for the negligent threat not to be wronged by the imposition of defensive force, that is not to say that there is no moral significance in the negligent threat accepting such an imposition. Let us consider a standard example in the ethics of self-defence. If, say, the negligent shooter has consented in advance to being subjected to defensive force should they negligently start firing their gun in the direction of innocent people, then, plausibly, the fact that subjecting the negligent shooter to defensive force will harm them constitutes even less of a moral objection to defending yourself against the negligent threat. Similarly, the view defended here is consistent with saying that while it is not morally required to obtain the consent of negligent potential bearers of Covid-19, the fact that they consent lessens any moral objection to them being subjected to Covid-19-related surveillance.[13]

In fact, if people have the option to consent to download a Covid-19 tracking app, then not consenting is arguably morally significant in a different way.[14] To refuse to consent to download it, when you reasonably believe that you might impose a risk on others of contracting the disease, could in itself constitute a form of morally objectionable negligence.[15] After all, you are provided with a relatively cost-free option that enables you to avoid causing harm to others. By declining to take this option, you arguably make it the case that a fair distribution of the risk of harm implies that you should suffer the harm of non-consensual tracking devices on your smartphone rather than risk others becoming infected with Covid-19. One argument in defence of this view appeals to the fact that most people would find it acceptable to demand that those who suspect they are infected with Covid-19 should self-isolate. Arguably, mandatory self-isolation is a greater intervention in daily life than downloading a tracking app (even if the latter lasts longer). Hence, if this demand is morally justified, then so too is the demand to download an app.

[12] We are assuming—justifiably so in the context of democracies, at least—that installing the infection tracking device, etc., has no serious harmful side effects for the innocent threat.

[13] Strictly speaking, they might not be able to consent, since they do not have a right against us that we do not surveil them. To accommodate this point, we could say that you can quasi-consent to an intervention against your body, mind, or property by communicating to others that you accept it, even if you do not have the right to refuse such an intervention.

[14] The same line of argument applies to omitting to self-isolate if the test is positive.

[15] This assumes, of course, that the tracking device is (reasonably believed by the person who refuses to download it to be) misused by the state to gain access other sorts of sensitive information about the app user. Perhaps this assumption is not satisfied in the case of some of less than fully democratic states in which the use of infection tracking apps is not fully consensual.

One interesting upshot of this is the following: superficially, by ticking the 'I agree' box on digital social media platforms and apps for mobile phones, we consent to sharing our personal information with a third party under conditions spelled out in the consent policies. However, privacy scholars have underlined that the consent policies are often very long and very difficult for laypersons to understand (Nissenbaum 2011). Also, the (social) price to users of opting out of such platforms is too high, which means that people are forced to accept the provider's terms. Hence, when ticking the 'I agree' box, we might not be sufficiently well informed, and the option of not consenting may not sufficiently acceptable for our consent to count as valid (Solove 2008; Tavani 2008).

By way of an example of Nissenbaum's concern, consider the Danish version of the Covid-19 tracking app. When you consent to the conditions of use, you consent to the health agencies keeping the information *as long as they consider it relevant*. Arguably, the fact that it is very hard to determine how long that will be, together with the use of impenetrable legalese, means that a tick in the 'I agree' box does not constitute valid consent (Adam Henschke and Patrick Taylor-Smith's chapters in this volume discuss some of these temporal issues with emergency pandemic surveillance).

A cynical response to this concern about the significant costs involve in knowing what one consents to is to say that the user can simply put greater effort into understanding the policies before accepting the terms of use—or alternatively, simply not use these apps and devices. However, one problem in this argument to the context of Covid-19 and the infection-tracking app is that the social cost of not downloading the app is not similar to that of opting out of social media platforms, where opting out typically involves significant costs, in the form of isolation from increasingly socially important fora etc.[16] Even so, other factors might render the option of not agreeing to the terms of use of Covid-19 tracking apps very costly. To return to our example two paragraphs ago, by appealing to social awareness, moral concern and respect for our fellow citizens ('*samfundssind*'), the Danish authorities have (so far) been very successful at promoting the use of the official Covid-19 tracking app.[17] Some worry, however, that in practice, the social shame associated with Covid-19-related irresponsible behaviour implies that people are subjected to a sufficient degree of coercion that their ticking the 'I agree' box does not to amount to valid consent.[18]

[16] See e.g., Solove's discussions on consent without a real choice (2008: 35).

[17] The Danish app has been downloaded 2.2 million times according to (Styrelsen for Patientsikkerhed 2021), which amounts to over one-third of the Danish population.

[18] Tech observers and scholars in Denmark have raised various worries concerning the Danish Covid-19 tracking app, e.g., Stine Bosse, who is Director of the Danish Tech Commission, Associate Professor at Copenhagen Business School Nanna Bonde Thylstrup, and Senior Researcher at The Danish Institute for Human Rights Rikke Frank Jørgensen (Jørgensen 2020).

If our argument is sound, then for some purposes at least, we can simply bypass such discussions about whether the sort of consent people give, when they tick 'I agree' boxes, amounts to valid consent. We can at least do so for the purpose of determining whether they are wronged, since, generally, their consent is not morally required in the first place. Again, this does not mean that this discussion might not be relevant for other purposes. Some might say, e.g., that current consent policies are manipulative, and that even manipulating people whose consent is not required can be wrongful in certain ways. However, such concerns are not those at play in most discussions of whether people's consent on social media, etc., is valid.

Why Consent Might Matter Morally, Despite Liability

Suppose that our argument in the previous section is sound. If so, then consent is not morally required in relation to installing tracking apps on the smartphones of the many potential bearers of Covid-19 who negligently expose others to risk of infection. By negligently exposing others to the risk of death or serious harm, they have no right to refuse others taking certain relatively non-draconian defensive measures against them, such as installing Covid-19 tracking apps on their smartphone. This seems to run counter to the widespread assumption in many European countries that the use of such apps requires the consent of the user. Hence, in closing, we want to explain why our argument in the previous section does not imply that a consent-based approach to Covid-19-related tracking apps is not the morally preferable approach, even if other approaches not based on consent are morally permissible.

One set of concerns that might, in some cases at least, favour the voluntary use of tracking apps is purely pragmatic. If, for instance, it is not politically feasible to enforce a ban on *not* downloading the app, then it might be morally better to try to persuade people to download it voluntarily, even if we know that far from everyone will do so, rather than to seek to make it legally mandatory to use the app. Similarly, if we know that if they are forced to download tracking apps, many people will simply not turn on their smartphone (or, simply, turn off Bluetooth, in which case the tracking app does not function) in situations where they might transmit the disease, then making tracking apps legally mandatory will defeat the purpose.

These pragmatic concerns are important but perhaps less theoretically interesting.[19] Here, we are primarily interested in a different, non-pragmatic concern,

[19] The forced use of the apps in some countries such as China suggests that it is possible, if not politically favourable, to overcome these pragmatic difficulties. We thank a reviewer for pointing out the need to clarify this point.

related to the sort of disrespect that is argued to be inherent in paternalistic policies. Many believe that paternalistic policies are based on the supposition that people do not act in ways that promote their own good—or at least, not as much as the state does—and that basing policies on such a presupposition disrespects the citizens. Since the state ought not to treat its citizens with disrespect, it follows that the state ought not to treat it citizens paternalistically (Anderson 1999: 330; Quong 2011; Shiffrin 2000).[20]

However, imposing the non-consensual use of Covid-19 tracking apps on smartphone users is not a paternalistic policy. At least, it is not the case that when the state forces a particular citizen to download a tracking app, it does so for the good of that particular citizen. Rather, it does so first and foremost to benefit other citizens.[21] Hence, the state forces citizens to take action to help other citizens, because it foresees that forcing citizens to download the app better serves this end than leaving the decision up to the citizens themselves. This supposition is analogous to the supposition behind paternalistic policies that citizens will not make the right choices from the perspective of their own good. Here, however, the supposition is that citizens will not make the morally right choice. It seems undeniable that a supposition of this kind lies behind the drive to make the tracking app compulsory.[22] Our next claim is that if the state disrespects citizens when it does not trust them to promote their own good, then it also disrespects them when it does not trust them to make morally good choices, such as downloading a tracking app to reduce the risk to others of contracting Covid-19. In support of this conditional claim is the fact that we tend to be more offended when others criticize us for making immoral choices than when they criticize us for making imprudent ones.[23] Hence, if much liberal critique of paternalism is justified, then there is a reason to rely on consensual Covid-19 tracking apps, even if people are actually liable to having such apps imposed on them non-consensually.[24]

[20] For present purposes, we will leave open what the source of this moral injunction might be, e.g., whether treating citizens with concern and respect is a condition for the right to rule (Dworkin 2000) or whether it is a duty that the state owes to each citizen.

[21] We set aside the complication that, possibly, the state might be said to be engaging in collective paternalism, i.e., by forcing each citizen to act in a particular way it makes all citizens better off (reducing the risk of acquiring Covid-19).

[22] Some might deny this on the ground that the state might act out of a concern to avoid free riding, i.e., it supposes that the great majority of citizens will voluntarily use the app, but also that a tiny minority will free ride on others' moral choices.

[23] Some might object that this can hardly be disrespectful, since it is a fact that a lot of citizens will make immoral choices, and that the state does not disrespect anyone by supposing what is obviously true. Whether or not this is so, note that exactly the same line of argument applies to allegedly disrespectful policies, since it is a plain fact that all of us will often make imprudent choices.

[24] Note that similar concern about disrespect does not apply in paradigmatic cases of self-defence. For example, once I load my gun and point it in your direction, preparing to negligently see if it works by shooting, I can no longer complain that you disrespect me by assuming that I am about to make an immoral choice—I am in the process of doing so.

Conclusion

All of us are threats to others, in the sense that we might transmit serious infection to them. Most of us are non-innocent threats, in that we are responsible for objectively unjust threats to other people's lives or health. Plausibly, infection tracking apps can help us fight epidemics, including the Covid-19 pandemic. Assuming that one does not live in an autocratic state in which there is a significant risk that the data that such apps generate will be misused for non-infection-related purposes, most of us are liable to have an infection-tracking app installed on our smartphones and to various relative moderate and appropriate interventions motivated by the information provided by those devices, e.g., compulsory testing and avoidance of risky behaviour. Accordingly, we are not wronged when this happens, and our consent is not required for such an intervention not to wrong us. Even so, there may be pragmatic as well as principled reasons why consensual surveillance schemes are morally preferable (e.g., in the absence of significant counterweighing moral costs, such as a much lower degree of use of the tracking app). In particular, we have argued, based on reasoning similar to that which grounds many liberals' view that paternalistic policies are disrespectful, that non-consensual surveillance schemes might be disrespectful, in that they send the message that citizens are likely to make immoral choices.

References

Anderson, E. 1999. 'What Is the Point of Equality?' *Ethics* 109 (2): 287–337.

Bellaby, R. W. 2012. 'What's the Harm? The Ethics of Intelligence Collection'. *Intelligence and National Security* 27 (1): 93–117.

Clark, M. 2000. 'Self-Defence against the Innocent'. *Journal of Applied Philosophy* 17 (2): 145–55.

Diderichsen, A. and K. V. Rønn. 2017. 'Intelligence by Consent: On the Inadequacy of Just War Theory as a Framework for Intelligence Ethics'. *Intelligence and National Security* 32 (4): 479–93. https://doi.org/10.1080/02684527.2016.1270622

Dukakis, A. 2020. 'China rolls out software surveillance for the COVID-19 pandemic, alarming human rights advocates', *ABC NEWS,* 14 April 2020, available at: https://abcnews.go.com/International/china-rolls-software-surveillance-covid-19-pandemic-alarming/story [accessed 30 April 2023].

Dworkin, R. 2000. *Sovereign Virtue*. Cambridge, MA: Harvard University Press.

Jørgensen, R. F. 2020. 'DEBAT: Den danske smittestop-app har flyttet sig fra statslig overvågning til tech-giganter', *Danish Institute for Human Righs*, available at: https://menneskeret.dk/nyheder/debat-danske-smittestop-app-flyttet-statslig-overvaagning-tech-giganter [accessed 30 April 2023].

Kleinig, J. 2009. 'The Ethical Perils of Knowledge Acquisition'. *Criminal Justice Ethics* 28 (2): 201–22. doi:10.1080/07311290903181218.

Lever, A. 2016. 'Democracy, Privacy and Security'. In *Privacy, Security and Accountability. Ethics, Law and Policy*, edited by Adam D. Moore, 105–24. London: Rowman & Littlefield.

Lippert-Rasmussen, K. 2020. 'Covid-19 "Tracing Apps", Quarantine, and Innocent Threats'. *Stockholm Centre for the Ethics of War and Peace*: http://stockholmcentre.org/covid-19-tracing-apps-quarantine-and-innocent-threats/

Lyon, D. 2014. 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique'. *Big Data & Society*. doi: https://doi.org/10.1177/2053951714541861

Macnish, K. 2014. 'Just Surveillance? Towards a Normative Theory of Surveillance'. *Surveillance & Society* 12 (1): 142–53.

Macnish, K. 2015. 'An Eye for an Eye: Proportionality and Surveillance'. *Ethical Theory and Moral Practice* 18: 529–48.

Macnish, K. 2018. 'Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World'. *Journal of Applied Philosophy* 35 (2): doi: 10.1111/japp.12219

Marx, G. T. 1998. 'Ethics for the New Surveillance'. *The Information Society* 14 (3): 171–85.

McMahan, J. 1994. 'Self-defense and the problem of the innocent attacker'. *Ethics* 104 (2): 252–90.

McMahan, J. 2009. *Killing in Wars*. Oxford: Oxford University Press.

Nathan, C. 2017. 'Liability to Deception and Manipulation: The Ethics of Undercover Policing'. *Journal of Applied Philosophy* 34 (3): 370–88.

Nissenbaum, H. 2011. 'A Contextual Approach to Privacy Online'. *Daedalus* 140 (4): 32–48.

Nozick, R. 1974. *Anarchy, State, and Utopia*. Oxford: Basil Blackwell.

Quong, J. 2011. *Liberalism without Perfection*. Oxford: Oxford University Press.

Quong, J. 2020. *The Morality of Defensive Force*. Oxford: Oxford University Press.

Rønn, K. V. and K. Lippert-Rasmussen. 2020. 'Out of Proportion? On Surveillance and the Proportionality Requirement'. *Ethical Theory and Moral Practice* 23 (1): 181–99.

Shiffrin, S. 2000. 'Paternalism, Unconscionability Doctrine, and Accommodation'. *Philosophy & Public Affairs* 29: 205–50.

Solove, D. J. 2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Stahl, T. 2016. 'Indiscriminate Mass Surveillance and the Public Sphere'. *Ethics and Information Technology* 18 (1): 33–9.

Stanley, J. and S. G. Granick. 'The Limits of Location Tracking in an Epidemic'. *AUCL* (8 April), available at: https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf [accessed 30 April 2023].

Stoddart, E. 2014. 'Challenging "Just Surveillance Theory": A Response to Kevin Macnish's "Just Surveillance? Towards a Normative Theory of Surveillance"'. *Surveillance Society* 12: 158–63.

Styrelsen for Patientsikkerhed. 2021. "Smitte|stop." 2021. https://smittestop.dk [accessed 8 April 2021].

Tavani, H. T. 2008. 'Informational Privacy: Concepts, Theories, and Controversies'. In *The Handbook of Information and Computer Ethics*, edited by K. E. Himma and H. T. Tavani, 131–64. Hoboken, New Jersey: John Wiley & Sons, Incorporated.

Thomson, J. J. 1991. 'Self-Defense'. *Philosophy and Public Affairs* 20 (1): 53–66.

Uniacke, S. 2011. 'Proportionality and Self-Defense'. *Law* and *Philosophy* 30 (3): 253–72.

Vaughan, A. 2020. 'There are many reasons why covid-19 contact-tracing apps may not work', *New Scientist*, 17 April, available at: https://www.newscientist.com/article/2241041-there-are-many-reasons-why-covid-19-contact-tracing-apps-may-not-work/ [accessed 30 April 2023].

WHO 2020. 'Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing' 28 May 2020, *World Health Organization*, available at: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1 [accessed 30 April 2023].