Surveillance Ethics and the Just-War Analogy:
An Interview with Kevin Macnish

Conducted by Ethan Harris

Keywords: access; control; intrusiveness; proportionality; war

Ethan Harris: What is your background in philosophy, and how did you come to be interested in privacy and surveillance?

Kevin Macnish: I fell into philosophy because it sounded interesting when I was looking at undergraduate degrees. When I was at school, I got into Marxist theory (that was in the late 80s, early 90s, around the collapse of the Soviet Union). From that, I moved into looking at political philosophy. However, having done a bachelor’s degree in philosophy, I became a bit disillusioned with it, thinking philosophy isn’t really that relevant to the real world. So I did a master’s in international relations and then went to work for the UK Government working for GCHQ (Government Communications Headquarters). After that, I came over to the US and worked for a few years at the Department of Defense. Then, I left and did a master’s in theology focusing on philosophical theology before working in a church for a few years. Afterward, I came back to philosophy proper, in about 2008.

Originally, I was looking at doing my doctorate in metaphysics and infinity, two things very different from where I ended up. However, nobody was going to be sponsoring that, and with a family to look after, I really needed some sponsorship to help me through the Ph.D. So I shifted to applied ethics, an area where there was more funding. At that time, there was a lot in the news about drone strikes, extraordinary rendition, torture, and things like that regarding Afghanistan and Iraq. That struck me as an interesting area to investigate, and so I started to look into issues around civil rights and so on and realized quite early on that there was extraordinarily little written on surveillance and ethics, which struck me as a really large gap in the market. And, of course, that’s exactly what you’re looking for when you’re doing a doctorate— an area where you can easily enter into and contribute something. So, despite having worked in surveillance while I was with the British government, that was not why I started looking at ethics and surveillance, although clearly, it helped to be able to draw on real-world experience. After that, those subjects just sort of became my thing for quite a few years, and I ended up doing a lot of my subsequent research in surveillance and privacy more generally.
**EH**: You currently work as a digital ethics consulting manager at Sopra Steria. Can you talk about the work you do there and how it is influenced by your background in philosophy?

**KM**: As a consultant, my work is focused on meeting with (potential) clients, understanding their problems, and then working with them to find solutions to those problems. As a specifically digital ethics consultant, those problems are in ethics and technology, which is an almost non-existent field of research in UK philosophy departments but has a healthy presence in the Netherlands, where I worked before joining Sopra Steria.

There’s never such a thing as a “typical” project, but the work may involve interviews and workshops, significant background reading, developing strategies in line with a client’s values, and so on. I must admit that there is a tendency to get too philosophical (and too academic), which is not what clients want or will pay for. A client is not going to say, “I’d like you to take a Kantian approach to this problem” or “what would a utilitarian say about this?” However, applied philosophy moved away from bluntly applying normative theories in real-life cases some time ago. It is more a matter of looking for the nuance and subtleties in a situation. Sometimes this might be nicely philosophical, such as, “how do you define trust?” but more often, it’s a matter of, say, “we agree that privacy matters, but how do we do it?” That gets to the heart of what I see as the leading challenge in ethics and tech right now, which is embedding ethics in corporate and government practice.

As for the skills that philosophy brings, I think, firstly, that it helps with the ability to look at the big picture, to very quickly get an overall idea about what’s going on, and to identify inconsistencies and problems as they arise or even before they arise. Another thing that it helps with is being able to see and appreciate all sides of an argument. Additionally, it helps develop a very logical, structured way of thinking. This is essential because oftentimes, with these projects, you have to put together a lot of information and organize it in a very clear way that tells a compelling story. Finally, philosophy helps with consuming large amounts of complex information really quickly. A lot of the projects I’m involved with are typically about three months in length. That’s not a lot of time to kind of do background reading and get yourself up to speed before you start dealing with the issues.

**EH**: You’ve written extensively on how the ethics of surveillance can be understood through an analogy to the ethics of war. How does this analogy work, and how might it influence how we think of policy dealing with surveillance?

**KM**: To be frank, I think that analogy (and it is my own) can be overplayed! As you say, the analogy is between the ethics of surveillance and the ethics of war. I have never tried to directly link surveillance and war. My insight was that the same questions we ask to determine if a given war is just (does it have a just cause, is it
An Interview with Kevin Macnish

proportionate, are we prosecuting it in an ethical manner, etc.) struck me as being the same questions we would want to ask to determine if a given act of surveillance is just.

With time, I have moved from a strict “you need to tick these boxes” approach (i.e., a given act of surveillance must fit all the criteria of having a just cause, being proportionate, etc.) to something more flexible. That is, a given act of surveillance may be justifiable, but it doesn’t automatically follow that you should therefore engage in it. There may be other non-ethical questions to consider or ethical questions which are specific to the particular context. Take, for example, the question of proportionality, the assessment of which can be extremely difficult. Does an occasional act of theft from a store justify permanent CCTV monitoring of all the store’s aisles as well as the entrance and exit point? However, I still think that the questions I have outlined are the key questions we should be asking of surveillance to determine whether or not it is the ethical course of action.

So, applying these thoughts to policy, what I would like to see is some real application, fleshing out the principles for justified surveillance in terms of impact assessments. We use impact assessments in all sorts of areas, such as safety, privacy, data protection, and more. These essentially review the foreseeable impact of courses of action in terms of areas like safety and privacy. I think that surveillance fits into a very similar category. If you’re about to engage in active surveillance, particularly as a corporation or a government (that is, not as an individual, but as a larger group), then you ought to carry out some sort of impact assessment.

I think these questions from the analogy would probably form a very good means of structuring that sort of assessment. Have you met all of these criteria? If so, then you’ve thought through the impacts effectively. So, an impact assessment would ask for the reason for the surveillance, the proportionality of the surveillance to be used, the discriminatory aspects of the surveillance (as in, is it targeting those who give rise to the just cause and not just any passerby), are there less intrusive alternatives, etc. If you can answer these, then you can demonstrate that you have thought through the ethics of the case to an adequate degree and will be in a position to justify the decision to employ surveillance should you be challenged on it.

To go back briefly to the analogy between the ethics of surveillance and the ethics of war, I do think that there is almost certainly a larger piece of research here that could be undertaken. Namely, do the questions asked in the just war tradition form the basis for understanding “necessary evils” more generally when something is prima facie wrong, but we feel it is justified nonetheless? That is, when one is about to engage in an activity that will be harmful to another entity, what are the grounds to justify that? It may well be that the questions asked of war are the same sort of questions we should ask in any situation where a prima facie wrong may be justified. I have come across people arguing that the just war questions should be used to inform ethical espionage and ethical economic sanctions, as two further examples. However, this broader question is something I never managed to dig into.
EH: Two aspects that you discuss are “proportionality” and “chance of success.” Can you talk more about these elements and how they function? Also, it seems that there is a necessary trade-off between these two. In other words, the more disproportionately large/harmful an act of surveillance is, the higher likelihood it succeeds. How should we navigate this trade-off?

KM: That is a really interesting point, and I think there are a few things to bear in mind here. Firstly, chance of success is a condition of *ius ad speculandum* (the justice of choosing to engage in surveillance—analogous to *ius ad bellum*, the justice of choosing to engage in war). This should be contrasted with *ius in speculando* (the justice of choosing how and where to employ surveillance—analogous to *ius in bello*, the justice of how a war is carried out). At a bare minimum, it is necessary (but not sufficient) for an act of surveillance (or, analogously, war) to have a legitimate chance of success in order for the act to be justified as part of the *ius ad speculandum* criteria.

Within the context of *ius ad speculandum*, I see the proportionality consideration as asking: Is surveillance a proportionate response to the situation? This renders proportionality a binary in this context—either surveillance is proportionate, or it is not. For example, if I suspect my 17-year-old daughter is seeing someone I don’t like, am I justified in carrying out surveillance on her? I would say not—she’s effectively an adult and capable of making her own decisions and mistakes. I should ask her and engage with her as an adult rather than spy on her.

Likewise, “chance of success” is also a binary in the *ad speculandum* context. The point behind the principle of “chance of success” is that if there is no chance of success, you shouldn’t do the action in question. The act is presumed to cause harm of some sort to some person or group, and if by causing that harm to that entity, you have no chance of achieving your (justified) end, then you shouldn’t do it. We could see it as a threshold concept in that regard—do you meet the threshold of having a chance of succeeding in your goals, yes or no?

This is analogous to war. Traditionally, when considering a potential war, we’re asking if there is a chance of success. If not, then you’re going to be throwing all sorts of lives away. If there’s no, or a very low, chance of success, you shouldn’t be doing it; you’ll just be killing people in vain. I think the same is true for surveillance. You shouldn’t be engaging in surveillance if there’s little chance that you will achieve your (justified) end through surveillance activity. It’s just going to be introducing harms that simply don’t need to be there.

We can ask, as with any threshold concept, where is the cut-off point? What if I had a 1% chance of success, given that that is still a chance? I think that both here and with proportionality that I shall come to in a moment, there is a danger of finding ourselves in a Sorites’ heap situation—why would a 50% chance be acceptable but not a 49% chance? Hence I would steer away from using a specific number as a hard cut-off point. We might also think of heroic efforts in war where people have fought rather than surrender to overwhelming odds and won. That then returns us to my
caution against using these as a tick-box exercise but rather leaning on the questions to guide reflection.

By contrast, proportionality in the *ius in speculando* sense (*ius in bello* analog) is more clearly a matter of degree; an act is more or less proportionate when judged against various factors such as how invasive it is or the risks imposed on the individual involved. Continuing with the example of my daughter, if I do think that surveillance is proportionate, I then need to decide what sort of surveillance is proportionate: should I put a tracker on her phone (or my car, knowing that she uses that), should I read her diary, should I put a microphone in her room to listen to her calls, etc.?

Interestingly, the traditional approach to *ius in bello* does not incorporate a chance of success in its criteria. With surveillance, I think that it is a fair suggestion to say that there is a chance of success with surveillance as such (*ad speculandum*) but not with this particular form (*in speculando*) of surveillance (e.g., tapping someone’s phone at random to identify a shoplifter). By extension, there are grounds to ask the same questions in a *ius in bello* context: we may have a chance of success in war, but not if we stick to fighting with swords and shields while our adversaries have guns. It is through identifying these possible insights into the long-standing just war tradition that makes the analogy such a rich one to explore.

Of course, there remains a question as to whether you can separate out the two considerations of proportionality in this manner. Can you really judge if surveillance is proportionate without knowing what sort of surveillance is involved? However, I would fall back then on the same question applying to the proportionality question in war: Can we know whether war is proportionate without knowing what sort of war? This doesn’t defend my position so much as it again points out challenges to it (which are good ones!) can also inform how we think about the ethics of war, so once more, learning from the analogy works both ways.

All of that said, we should return to your initial question of trade-offs. Within the traditional approach, that is my starting point: there should not be a trade-off. In the *ius ad speculandum/ad bellum* considerations, either there is or is not a chance of success, and either surveillance is or is not a proportionate response to the occasioning cause. As chance of success is not a traditional consideration in *ius in speculando/in bello*, there would not normally be a trade-off between an act of surveillance having a greater chance of success if it is less proportionate (i.e., more intrusive). Nonetheless, as we’ve suggested here, it is plausible to introduce chance of success into the *in speculando* considerations. In that case, you are right about the trade-off. However, requiring that an act be both proportionate and have a chance of success should lead to a balancing out of these two aspects. That is, if a chance of success requires disproportionate levels of surveillance, then it will not be justified. The flip side of that is that a proportionate level of surveillance may have very little to no chance of success. In both cases, it seems to me that the surveillance would not be justified.

**EH:** In “An Eye for an Eye: Proportionality and Surveillance,” you discuss in-
depth the proportionality aspect of just surveillance, specifically how we should weigh its benefits and harms. This seems to imply at least a quasi-consequentialist ethical scheme. How would this argument work under, say, a Kantian worldview?

KM: As an applied philosopher, especially one now working outside academic philosophy, I would tend to shy away from strict Kantian or Utilitarian responses to problems. Most deontologists would, I think, embrace some element of consequence consideration in their calculations. That is, they would consider the consequences of a particular action when they’re looking at its justification—I don’t think it’s at all illegitimate for a deontologist to consider consequences. (In fact, I think that very strict Kantians are in the minority here and would need to provide some strong defense today). On the other hand, many consequentialists will not consider any of the duties when they’re looking at consequences (unless they happen to be a duty-based consequentialist).

Saying that, I’m sure that some accommodation could be made. I certainly do see the proportionality consideration operating in a manner that embraces consequences, but I don’t think that you have to be a strict Kantian to insist that proportionality considers the categorical imperative when determining a course of action. So if there is a chance that an act of surveillance will undermine someone’s autonomy or treat them as a mere means (which is a key argument), then it would be disproportionate. This would render the criteria as a new binary that should be considered in the *ius ad speculandum* sense—namely, does the surveillance undermine someone’s autonomy or treat them as a mere means? If so, then it would never be justified.

Alternatively, we can also look at surveillance in terms of the chance of it infringing on somebody’s or some group’s autonomy, where the more likely some act of surveillance is to intrude on or diminish autonomy (and the extent to which it would diminish autonomy), the less proportionate it would be as an action, all else held equal.

This discussion of Kantian and consequentialist approaches to surveillance makes Tony Doyle’s argument (which I love) about an alien monitoring Earth particularly pertinent—is surveillance still wrong even if there are (and can be) no consequences? In his paper, Doyle imagines an alien 100 light years away is monitoring you 24/7. He has perfect knowledge about every aspect of your life, but by the time the information reaches the alien, you’re dead. And by the time the alien can do anything with the information by getting it back to Earth, it’s already 200 years after the event happened, so anyone with living memory of you is also dead. So, if you’re a famous person, it might dent your reputation. But for most of us, it’s not going to be an issue. The question that Doyle points out, then, is if there is anything wrong in what the alien is doing. It’s a really interesting thought experiment. I’ve used it with students for years, and it usually divides a room 50/50. There’s some deep level of feeling where I still feel that my privacy has been violated. But if there are no consequences coming from it, is it a problem?
EH: A big debate in the philosophy of privacy is whether privacy is a matter of control or access. What are your views on this debate, and what are the offshoots for the ethics of surveillance?

KM: This was probably the most philosophically “pure” area of discussion that I have engaged with. The debate on the nature of privacy goes back to some of the first publications by people like Judith Jarvis Thomson, Thomas Scanlon, and James Rachels in the early and mid-‘70s, and it is still continuing today (there is a group of us who email each other from time to time with the latest thoughts and challenges on the subject).

In essence, the control theory says that if you lose control of something you want to keep private, then you have lost privacy. The access theory holds that someone needs to access that thing you want to keep private to lose privacy. For example, I could be locked in a room with a CCTV camera pointing at me. I would probably feel that anything I did in that room was not private. However, if no one was watching that camera’s feed, and it was not being recorded so no one ever would watch it, then it seems to be that my actions in that room are private. I might just have an incorrect belief that they are not.

I tried to illustrate this in my paper “Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World” (a very dated title, now!) by discussing the example of a diary in a coffee shop. Say I walk out of the coffee shop and accidentally leave my diary on a table. When I realize my mistake and come back for the diary, I see that it is in the hands of someone at a different table. While I may feel (or fear) that I have lost privacy, if that person has not opened, read, and understood the diary, then I have not had my privacy diminished.

The control theory, as I read it, would say that my privacy has been violated because I lost control over my information, and someone else gained control over it. To me, this is counterintuitive. It doesn’t make sense to me to say that I’ve lost my privacy if the other person never read the diary. (Of course, it’s true that I’ve lost a degree of privacy insofar as they now know that I keep a diary, but I think that’s extraneous to the core of the argument.)

In my view, what I think the control theory represents is not privacy itself but rather the right to privacy. I would be happy to say that the right to privacy is about enshrining a right to control information about myself or a right to control my private space, for example. But I don’t think that privacy itself is about those sorts of things. To me, privacy is at heart about preserving dignity before others. Precisely how I do or am able to preserve that dignity is what the right to privacy is concerned with. Hence, while control is not (in my view) fundamental to privacy itself, controlling information about myself is fundamental to my ability to exercise a right to privacy.

This is important for how we understand acts of government surveillance. In
the past, I’ve argued that what organizations like the NSA and GCHQ (the British equivalent) were doing in terms of bulk collection of data from the internet did not constitute an infringement of privacy unless someone actually looked at (i.e., accessed) the data. Now, that’s not to say the collection of data isn’t important or that it isn’t wrong. I think that when such bulk collections of data occur and people find out about it, there’s a huge sense of a loss of security. And in some countries, the organizations collecting data may not have (now or in the past) sufficient guardrails in place to protect against abuses of data, such as handing data over to the governing party for use against dissenters or members of opposition parties, for example, which could have very real impacts on people’s lives. So there are all sorts of problems that could come up in mass data collection; I would just argue that privacy is not one of them. The most you could say, as I raised in one of my papers, is that there is an increased risk of privacy being diminished as there is now a possibility that the data could be accessed in a way that there was not previously.

There is a more recent development in the control/access debate which I think is worth mentioning. Leonhard Menges published an interesting response to this argument a few years ago from the control perspective.\(^1\) His position was that there are different forms of control. Yes, there is the simplistic scenario I gave regarding being in a room with a CCTV camera that no one watches, but there is also the scenario where someone is locked in a room but, as they never choose to leave the room, they are psychologically unaffected by being locked in. Nonetheless, it is clear that they are wrongly detained and that they lack control, even if they think that they have it. This, Menges holds, is the sort of control in surveillance where someone holds my diary (or can access the CCTV camera) when they should not. Hence it is about who has control rather than whether I have control.

I’m sure that the argument will continue. Menges’ response is very interesting and has a lot of potential.\(^2\) However, I think that it is clearly not the sort of control that people writing before Menges, like Adam Moore or Julie Inness, were talking about. Those people were talking about a theory of control much closer to the one that I was critiquing, in which control is taken to be the ability to manipulate what happens to my information. So perhaps Menges salvages the control position, but possibly at quite a high cost, or at least unsatisfactorily with regard to those earlier views.

**EH:** In “An Eye for an Eye: Proportionality and Surveillance,” you write that “intrusiveness” is a key concept when determining proportionality. Can you talk a little bit about what this concept means and how it has manifested with more novel forms of surveillance and technology?

**KM:** When I talked about “intrusiveness,” I think I did so as an intuitive way of trying to capture all the harms involved in surveillance under one umbrella term. It probably wouldn’t stand up to much scrutiny, but the basic idea was that the more intrusive something is (i.e., the deeper into your life someone peers), the worse the
wrongs would be if that surveillance were unjustified, or should something unintended happen, such as a data leak. Importantly, “intrusiveness” is a descriptive rather than a normative term.

As such, I do not mean to say that the surveillance would necessarily be unjustified if it were intrusive, just that the more intrusive it is, the greater the rationale would have to be for it to be justified. Hence the state putting CCTV cameras in my home would be extremely intrusive but not necessarily unjustified (e.g., if I were reasonably suspected of abusing my children and the police needed to gather evidence).

Connecting the concept of intrusiveness to novel technology is really interesting. We’ve seen a lot in recent years, particularly in light of the pandemic, that has indeed seen surveillance become more intrusive. For one thing, when on a video call, if I have not chosen to blur my background, you have a good insight into what my study looks like. My work colleagues know my dogs and my children far better than they would have in the pre-pandemic days. So these sorts of novel technologies we’ve adopted have certainly led to a greater degree of intrusion in terms of seeing into people’s homes in a way that a few years ago just wouldn’t have happened.

Another thing that really took off during the pandemic was so-called “bossware,” as managers wanted to keep tabs on people working from home, so cameras started to notice if someone’s eyes moved away from the monitor for any length of time and could monitor the length of toilet breaks. There was also the use of keylogging software to determine how productive one’s workers were. Pre-pandemic, some workers already experienced a degree of this (e.g., truck drivers who were monitored as to where they were and how fast they were driving), but this level of surveillance has now entered the lives of far more people.

The Internet of Things is also seeing intrusion into more and more areas of our lives. If my refrigerator is internet-linked, I can get it to order more milk, but then the manufacturer knows that I drink milk and how much. Cell phones, of course, give away so much information about us to not only the manufacturer but also app developers, and the OS, whether that’s Android, Apple, or something else.

Arguably the most intrusive, though, is Alexa, which sits quietly in a corner, listening to everything you say in case you use the trigger word. In the spirit of transparency, I have several of the devices throughout my house. I love the ease it brings, but it is far more intrusive than anything we would have considered bringing into our homes forty years ago.

The one area that remains inaccessible by others is the mind. However, I’m not sure that that will remain so for long. Totalitarian states such as Nazi Germany and Stalin’s USSR would execute people for what Orwell called “thought crime,” but that was implied as a result of actions. We continue to imply thoughts on the basis of behaviors when we use behavior-recognition systems to identify loiterers or terrorists (e.g., using automated systems to identify patterns of behavior that somehow signify that a person is up to no good). I suspect that we are not all that far from being able to
access people’s thoughts more directly, though. To me, that really does feel like the last barrier and the last defense of a liberal society. If our thoughts could genuinely be subject to surveillance, then I think that it would be impossible to maintain that we were living in a genuine liberal democracy. Freedom of thought strikes me as the heart of such a society, and while there is the ability to think that 2+2=4, we maintain some vestige of freedom from oppression. When we lose that, as again Orwell argued, we lose what it is to be human.

Kevin Macnish is a Consulting Senior Manager in Digital Ethics with Sopra Steria. Kevin is a former analyst at GCHQ and the US DOD, and assistant professor at the universities of Leeds and Twente. He has been interviewed widely and has spoken at the Houses of Commons and Lords. Kevin has published fifty academic articles, chapters and books on ethics and technology, including *The Ethics of Surveillance: An Introduction* (Routledge, 2018) and a forthcoming edited collection on *Ethics of Surveillance in Times of Emergency* (OUP, 2023). He is a visiting Research Fellow at the University of Leeds.

Notes and References
