Debate

Conditions under which Surveillance may be Ethically Justifiable: Remarks on Kevin Macnish's proposed normative theory of surveillance

Elin Palm

Linköping University, Sweden.
elin.palm@liu.se

1. Introduction

In 'Just Surveillance? Towards a Normative Theory of Surveillance', Kevin Macnish identifies the need for a framework suitable for systematic analysis of the normative implications of surveillance conduct. In order to be able to incorporate the many ethical aspects that already have been identified as relevant in relation to surveillance, Macnish proposes an ethical assessment-model based on Just War Theory (JWT). This theory, he claims, comprises all relevant ethical issues and excludes none. Also, it offers a tool for a coherent analysis.

Certainly, the ethics of surveillance is an under-researched area. Whereas the impact of surveillance on values and principles like privacy and autonomy (Lyon 2001; McArthur 2001; Fairweather 1999; Introna 2003; Albrechtslund 2006; Palm 2007, 2009a, 2009b) have been investigated to a large extent, the influence on other aspects such as dignity (Stoddart 2008; van der Ploeg 2002), identity (Behrens 2013), freedom of movement/liberty (Palm 2013), fairness (Introna 2003; Palm 2004) and distributive justice (Introna 2000) have received little attention. When researched, these issues are typically analysed in isolation from each other. Few attempts have been made to take a broad grip on the ethics of surveillance. A unified approach, incorporating most of the relevant ethical aspects is lacking so far.¹ Macnish aims at filling this gap.

Drawing on JWT, Macnish proposes a set of ethical guidelines that can be applied to prospective usage of surveillance systems. JWT requires a two-step evaluation of the ethical acceptability of warfare. First, it commands that the *reasons* for war are legitimate and second, that the *means* of war are ethically defensible. Criteria are offered for both steps. Applied to surveillance conduct, it would be necessary to consider the reasons for surveillance before the actual implementation and use of surveillance systems. And, once the reasons have proven to be acceptable, that which can be considered ethically justifiable surveillance should be investigated. Surveillance conduct should adhere to pre-established criteria. Underlying Macnish's approach is the idea that surveillance technology is rather neutral *per se* but since surveillance-capable systems can be put to more or less ethically sound use, they should be carefully monitored in order for unnecessary harm to be avoided.

¹ However, an attempt has been made to encircle, for surveillance conduct, legally relevant principles that to a large extent correlate with Macnish's guidelines, see: <https://en.necessaryandproportionate.org/text>

In the following, the relevance of using Just War Theory as a basis for a comprehensive ethical assessment-model for surveillance will be critically discussed. Ways in which Macnish's proposal can be strengthened will be suggested.

2. Laws of War (LoW)—Just War Theory (JWT)

An assumption underlying the Just War doctrine is that war is something evil (*mala in se*) that should be avoided as far as possible but that may, under certain circumstances, be necessary. Proponents of JWT claim that despite an evil thing, war should still be subject to moral standards and deemed more or less just. Depending on the extent to which nation states comply with the Laws of War, warfare can gain more or less support from the international community. JWT consists of six basic principles that have been incorporated into (Western) international doctrines, such as the Geneva and Hague Conventions, and politics have committed themselves to respect and follow these principles. It is distinguished between the justification for the resort to armed force (*jus ad bellum*) and justified conduct when using force within a war that has been deemed legitimate (*jus in bello*). *Jus ad bellum* concerns: (1) just cause, (2) right intention, (3) legitimate authority, (4) necessity or last resort, (5) proportionality and (6) reasonable hope of success (Macnish separates 'necessity' and 'last resort' as distinct aspects). *Jus in bello* comprises three principles: (a) discrimination, (b) necessity or minimal force, and (c) proportionality. These criteria are intended to differentiate between justifiable and unjustifiable uses of armed force and to show how military interventions can be restricted, made more humane, and contribute to the overarching aims: peace and justice. Both sets of criteria must be fulfilled in order for a war to be just. A war fought for unjust reasons cannot become just by adherence to the second set of criteria only.

Applied to surveillance conduct

Having highlighted some key-characteristics of JWT, the extent to which it seems proper to use this theory as a basis for an assessment model for surveillance conduct will be investigated. At least two issues deserve articulation beyond what Macnish offers in his proposal.

First, the reasonableness of borrowing the basis for an evaluation model from Just War Theory is dependent on the extent to which JWT is a sound theory to begin with. Potentially compromising aspects of the original model should be considered. Macnish's choice of theory is primarily motivated by the following reasons: (1) that JWT comprises all relevant ethical issues of importance to surveillance without neglecting any, and (2) that the theoretical model is well-anchored and widely recognised.

Certainly, the suggested model comprises all ethical issues that Macnish has listed as relevant to surveillance conduct. But, have all pertinent values and principles been encircled to begin with? Although the suggested model is impressively inclusive, some key values highlighted in ethical analyses of surveillance-based control seem to be missing. For instance, Macnish stresses the importance of privacy but leaves aside classical values such as autonomy and liberty. Surely, depending on what theoretical approach to privacy one takes, autonomy may be included. Following privacy scholar Beate Rössler, privacy is intimately linked to autonomy—the former is an enabling condition of the latter (Rössler 2005). Rössler argues that the reason why we should take measures to secure privacy is that we thereby safeguard the more fundamental value: personal autonomy. But even if autonomy (under one understanding) can be considered intimately linked to privacy, the values are not symmetric. Autonomy may be negatively affected without privacy being infringed upon (at least not to the same extent), hence why the impact of surveillance on these values should be investigated separately. This can be illustrated with Tesco's plans to introduce cameras that scan (and estimate) the sex and age of customers entering their premises. Such data will be used to tailor-make video advertising on screens. According to the system owner, the technology concerns face detection rather than facial recognition. Neither does it identify individual shoppers, nor does it collect or store biomorphological information. Whereas ordinary consumer profiling is based on processing large sets of person-specific and person-related data, in the Tesco case, focus is

limited to the age and sex of individual by-passers as a basis for customised commercials. Hence, informational privacy is only mildly affected. Yet, the autonomy of the scanned bypassers may be significantly impaired by targeted advertisements—at the very least, measures are taken to steer their customer behaviour.

When identifying ethical issues discussed in relation to surveillance, Macnish primarily (but not exclusively) draws on analyses conducted within the field of sociology. Certainly, sociological concepts such as ‘social sorting’ are ethically significant but, in this model, their normative relevance remains to be articulated. It could be instructive to consider discussions within the fields of philosophy, ethics and applied ethics for a more inclusive set of values to be recognised. An interesting and perhaps relevant statement made within the domain of Information and Communication Technology (ICT) ethics, is that privacy, equality, liberty and autonomy are values relevant to most any novel ICT (Brey 2000). At the very least, an explanation as to why key aspects such as freedom of movement and autonomy have been left aside in the development of an ethical check-list for surveillance conduct should be offered.

Regarding the status of the role model JWT, even if it is well-established (in terms of a long-standing tradition) and influential, the theory must not necessarily be sound. It should, for example, be noted that JWT has been subject to extensive debate (cf. Johansson 2011, 2013), often accused of being difficult to apply due to internally contradicting principles. For instance, that which should count as a legitimate reason for waging war is unclear. Aggression has typically been considered permissible if the purpose is to retaliate against a wrong already committed e.g. if one nation seeks to pursue and punish an aggressor, but in recent years, the support for nation states’ right to undertake pre-emptive measures has increased in the West. Furthermore, the case has been made that certain weapons have altered the conditions for just wars, hence, JWT is outdated and/or must be adjusted. Michael Walzer (1977) argued that the advent of nuclear weapons altered the conditions of war to an extent that it would no longer be meaningful to adhere to the JWT principles (Walzer 1977). More recently, it has been claimed that novel military technology may influence the ways in which war is conducted and as such calls for amendments of some of the laws of war. For instance, it has been noted that today’s military use of drones may lower the threshold for waging war since, with these weapons, civilian casualties can be avoided (clinical warfare) (Johansson 2011, 2013). But even if such weapons change the nature of warfare (e.g. the timing, range, and potential devastation), they do not render the need to consider their use within a moral framework superfluous: a nuclear warhead remains a weapon as do (armed) Unmanned Aerial Vehicles, and such weapons can still be morally or amorally employed.

Taken together, whereas JWT successfully incorporates all the values that Macnish have listed, his list is not fully comprehensive and would benefit from attempts to incorporate values pin-pointed as central in ethical analyses of surveillance conduct. The problems identified with JWT are not grave enough for us to abstain from using the theory as a model for the evaluation of surveillance conduct, but imperfections in the form of poor action-guiding capacity and internal contradictions between the JWT-criteria should be recognised and attempts made to deal with such issues. There seems to be reason to believe that these problems may arise in the context of surveillance as well.

Second, the question of responsibility for employing the proposed model deserves clarification. While clear in the original model, it is less obvious by whom the proposed assessment tool for surveillance conduct should be used. Following Just War Theory, agents that can wage and fight war are nation states. On the one hand, nations are entitled to self-determination. JWT in general, and the principle of ‘proper authority’ in particular, relies on the sovereignty principle according to which *legitimate* nation states are entitled to control and protect their territories. If subject to aggression, they are typically considered to be within their right to retaliate in order to protect their territory and interests. On the other hand, when in conflict, nation states are obligated to justify their actions to concerned parties (the other party or parties of the conflict and the international community), demonstrating why war is declared. In order to *rightfully*

wage war, a nation state must show that the above-mentioned principles have been met, that alternative, peaceful (diplomatic) solutions have been exhausted and that violence is unavoidable. War should always be a last resort. Countries that fail to adhere to these rules may, in different ways, be punished by the international community e.g. by diplomatic and economic sanctions. Justifications must not be self-interested but other-regarding and acceptable to other states. Most importantly, there is an overarching aim of just war—the upholding and restoration of order and peace. This aim is taken to be an intrinsic good, valued and desired by all people/s.

In his proposal, Macnish is not ascribing responsibility for employing the ethical check-list to any specific agent or agency. He merely demonstrates criteria according to which ethical reviews should be carried out, the many different categories of surveillants and the multitude of interests at stake in surveillance conduct. Thus, it remains to be explained: is the model intended as a self-assessment tool? Should the surveillant prove that his or her actions are justifiable? Perhaps the ethical reviews are intended to be carried out by ethicists? Or, should the assessments be dealt with in yet other ways? And, to whom should the justifications be addressed? More important still, in line with what overarching aims should the justifications be formulated? As we have seen, in the case of warfare, the key concern is the establishment or restoration of peace and order. It is against this goal that nation states' reasons for declaring war *jus ad bellum* are deemed ethically right or wrong. In the second step, one of the criteria *jus ad bellum* stipulates that measures should be proportional in relation to the aim specified *ad bellum*. A complicating factor in the case of surveillance conduct is that there is no shared view of what surveillance should contribute with—which values it should realise. Rather, there are many competing interests that must be balanced. In order to gain more force, Macnish's proposed model would need a value basis. Formulating aims and values that surveillance conduct (ideally) should bring about would also strengthen the case for an assessment model that otherwise risks 'to be spinning in the void'.

Certainly, Macnish stresses that the analogy between war and surveillance-based control neither is nor must be perfect. For his purposes, it is sufficient that there is a significant similarity between the *ethics* of war and the *ethics* of surveillance. This seems to mean that the requirements for considering negative implications of war lend themselves to (an ethical assessment of) surveillance conduct. While agreeing with Macnish that there is no need for a perfect analogy between war and surveillance, only between the ethics of war and surveillance, in order for the ethics of surveillance to be an analogue of the ethics of war certain structural similarities seem necessary. Preferably, overarching goals similar to the promotion of peace and order in JWT should be articulated in the ethics of surveillance. Without such, reasons typically held forth in favour of surveillance, such as the need to protect national security, stifle criminal activity and safeguard effectiveness/competitiveness will clash with values like privacy and dignity without us being able to tell how the competing claims should be balanced. In order for the JWT-inspired model to be enforceable, it seems crucial to find an answer to what surveillance should bring about in order to evaluate the extent to which surveillance conduct promotes desirable values.

According to Macnish, the criterion 'legitimate authority' is desirable but not necessary. Due to the many different agents conducting surveillance (nation states, private enterprises, neighbours, peers, etc.) the question of legitimacy becomes complicated. Although a complex matter, this issue is of the highest relevance and deserves further development—not least since, to an increasing extent, surveillance has become a supranational undertaking. Surveillance-based migration control is one example (Franko Aas 2005; Palm 2011, 2013; Johansen et al. 2013). Increasingly, irregular migration is framed as a security risk and a threat to the stability and cohesion of developed nations (cf. de Haas 2008). Not seldom are surveillance systems employed as security measures in response to a perceived risk (Dijstelbloem 2009, 2011; Palm 2013). Just like armed force has been used as a response to threat and a means to preempt further aggression, surveillance regimes have been employed with the aim to prevent mass influx of immigrants (Johansen et al. 2013; Palm 2013). In this context, the traditional, sovereignty-based view is out-dated and the question of legitimacy reactualised. Thus, the question of legitimacy deserves more

rather than less attention.

3. Recommended amendments

Having considered some weaknesses and identified a need for further development of the proposed model, in the following, an attempt will be made to make an addition that could strengthen an, all in all, promising ethical assessment model. It will be suggested that the model should be three-fold instead of two-fold and that the ethical evaluation of surveillance (systems and conduct) should be considered an iterative process. Arguably, ethical reviews should be conducted continuously rather than at one specific point in time.

A common problem with surveillance is that once monitoring systems have been implemented in one domain, their (alleged but seldom verified) effectiveness is often used as a reason to adopt the same or similar solutions in other domains. As noted by David Lyon (2007), surveillance systems originally intended to perform narrowly specified functions are expanded as a reaction to new (political) circumstances, often sidestepping or pushing back the limits of the original legal framework and safeguards. Scholars have also pointed at how surveillance technology has become normalised. New strategies for control in the form of surveillance infrastructures are continuously developed and novel uses of already existing surveillance networks are extended. It has been illustrated how discrete surveillance systems are converged to an assemblage, and groups which were previously exempt from routine surveillance are now increasingly being subject to monitoring (Haggerty and Ericsson 2000). Practices that before September 11th would have found little acceptance such as biometric identification and authentication processes, dataveillance and large-scale information sharing between countries etc., have been normalised (Salter 2004). Ordinary travellers are now subjected to practices previously exclusive to suspects, such as biometric verification and register checks. Not only are travellers subject to close scrutiny. Sophisticated surveillance systems are entering most any domains of society under the pretext of security enhancement. Whether or not these means actually promote security however remains uncertain since their effects are seldom (critically) investigated.

A rapid proliferation of surveillance technologies and normalisation of surveillance conduct require potent countermeasures. Once surveillance regimes have been implemented these systems are seldom modified to be less invasive or withdrawn altogether—unless in conflict with the existing legal framework or met with (exceptional) public outrage. To the contrary, their range and scope is often extended. In order to better tackle the proliferation of surveillance technology, it will be suggested that Macninch's diptyche model should be extended to comprise a third aspect—deregulation and downsizing of surveillance systems already in use. The proposed third component would draw on a recently introduced third category of JWT—*jus post bellum* (Orend 2002; di Meglio 2006; Österdahl 2012). This category is intended to govern the justice of war termination and peace agreements, as well as the prosecution of war criminals. The *Jus post Bellum* is meant to serve as the normative framework for the efforts to stabilise the post-conflict situation. Furthermore, it has the future peaceful, and arguably democratic and human rights respecting, development of the post-conflict society in view (Österdahl 2012). Once the aims for introducing surveillance technology in the first place have been fulfilled, surveillance may not be necessary anymore. Adopting a third component would allow the author to further underline that surveillance should only be used in so far as absolutely necessary and *as long as* it remains the most potent means to obtain the intended (legitimate) aim. By adding this third step in the evaluation model, he would not only be able to require that the least intrusive means that achieves the desired aim should be employed but that, once in use, overly intrusive systems should be replaced with less invasive such. The third step can prevent unreflected routine use of surveillance. It is important to recognise that the context in which surveillance systems were implemented may have changed over time and therewith the need for control. Surveillance that once filled a function may have become superfluous—especially since the advent of a monitoring device may alter the ecology where it is implemented. It is important not to assume

that the desired aim requires surveillance to be upheld. After some time in use, the reasons for introducing surveillance regimes should be reassessed. Careful investigations should be made as to whether or not surveillance must continue and if so, in what form. Is the need for camera surveillance still there? Could less invasive measures do? As a rule of thumb, alternative, less intrusive strategies should continuously be sought and the ambition should be to, if not stop, at least reduce surveillance as far as possible.

4. Conclusion

Kevin Macnish's proposal is a most welcome contribution to the challenging task of social and ethical shaping of surveillance conduct, reducing negative implications while highlighting positive such. Just War Theory can serve as a starting point for systematic reflection on the ethical acceptability of surveillance conduct. In the same way that JWT is intended (1) to prevent the onset of war by demonstrating criteria that must be fulfilled before declaring war, and (2) to stifle an uncontrolled escalation of aggression, applied to surveillance conduct, such criteria can serve to motivate surveillants seeking justification for surveillance practice and identify alternative means to obtain the intended aim. By adding a third component, the diptyche model is transformed into a triptyche model and a way to downsize rather than upscale surveillance conduct is offered. Some aspects of the model are in need of further explication, such as the question of who should use the ethical check-list—whether it should be a form of self-assessment or an external assessment conducted by experts. Also, the values to be incorporated need further consideration since some key values are missing. Taken together, Macnish's proposal is a much promising contribution to the field of Surveillance Studies in which models for systematic ethical analysis are lacking. The suggested model can answer a most important question: under what conditions, if at all, can surveillance technology/conduct be ethically justifiable? Importantly, this question can be given different answers depending on the particular context in which surveillance is taking place.

References

- Albrechtslund, A. 2006. The Postmodern Panopticon: Surveillance and Privacy in the Age of Ubiquitous Computing, Sixth International Conference of Computer Ethics: Philosophical enquiry, CEPE.
- Behrens, M. 2013. Identity as Convention. *Journal of Information, Communication & Ethics in Society* 12(1): 44-59.
- Brey, P. 2000. Disclosive Computer Ethics: The Exposure and Evaluation of. Embedded Normativity in Computer Technology. *Computers and Society* 30(4): 10-16.
- Broeders, D. 2007. The New Digital Borders of the European Union. *International Sociology* 22(1): 71-92.
- Broeders, D. 2009. Breaking Down Anonymity: Digital Surveillance of Irregular Migrants in the Netherlands and Germany. *Doctoral Thesis from the University of Amsterdam*, Amsterdam University Press, The Netherlands.
- Dijstelbloem, H. 2009. Europe's new technological gatekeepers. Debating the employment of technology in Migration Policy. *Amsterdam Law Forum* 1 (4): 11-18.
- Dijstelbloem, H. and A. Meijer. 2011. *Migration and the New Technological Borders of Europe: Migration, Minorities and Citizenship*. Basingstoke: Palgrave Macmillan.
- DiMeglio, R. P. 2006. The Evolution of the Just War Tradition: Defining *Jus Post Bellum*. *Military Law Review* 186: 116-163.
- Fairweather, B. N. 1999. Surveillance in Employment: The Case of Teleworking. *Journal of Business Ethics* 22: 32-49.
- Franko Aas, K. 2005. *The securitization of migration: whose justice and whose security?* Conference paper online: http://org.uib.no/imer/14Nordic/Papers_fra_14_Migrasjonsforskerkonferanse/Aa
- De Haas, H. 2008. Migration and Development – A Theoretical Perspective. *International Migration Institute*, James Martin 21st Century School, University of Oxford, Working paper, Paper 9. <http://www.imi.ox.ac.uk/pdfs/imi-working-papers/WP9%20Migration%20and%20development%20theory%20HdH.pdf>
- Haggerty, K.D. and R.V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51(4): 605–622.
- Introna, L. 2000. Workplace Surveillance, Privacy, and Distributive Justice. *Computers and Society* 33(4): 30-39.
- Introna, L. 2003. Workplace Surveillance 'is' Unethical and Unfair. *Surveillance & Society* 1(2): 210-216.
- Johansson, L. 2011. Is it Morally Right to Use Unmanned Aerial Vehicles (UAVs) in War? *Philosophy & Technology* 24(3): 279-291.
- Johansson, L. 2013. *Autonomous Systems in Society and War – Philosophical Inquiries*, Doctoral Thesis, Stockholm University.
- Johansson, N.B., T. Uglevik and K. Franko Aas. 2013. *Krimigrasjon? Den nye kontrollen av det fremmede*. Universitetsforlaget, Oslo, Norge.
- Lyon, D. 2002. *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. London: Taylor & Francis.
- Lyon, D. 2007. *Surveillance studies—An overview*. Cambridge: Polity Press.
- Noll, G. 2003. Visions of the Exceptional: Legal and Theoretical Issues Raised by Transit Processing Centres and Protection

- Zones. *European Migration and Law* 5: 303-341.
- Orend, B. 2002. Justice after war. *Ethics & International Affairs* 16: 43-56.
- Österdahl, I. 2012. Just War, Just Peace and the *Jus post Bellum*. *Nordic Journal of International Law* 81 (3): 271-294.
- Palm, E. 2004. An Ethical Questioning of Work Place Monitoring – strengthening employees’ negotiating power. In: *Challenges for the Citizen of the Information Society*, eds T.W. Bynum, N. Pouloudi, S. Rogerson and T. Spyrou, Ethicomp 2004. Proceedings of the Seventh International Conference. University of the Aegean, Syros, Greece, 14 – 16 April 2004. pp.727-736
- Palm, E. 2007. The Ethics of Workspace Surveillance, Doctoral Thesis, Royal Institute of Technology, Stockholm, Sweden.
- Palm, E. 2009a. Expectations at Work—What is Reasonable and Why? *Ethical Theory and Moral Practice* 12 (2): 201-215.
- Palm, E. 2009b. Securing Privacy at Work: The Importance of Contextualized Consent. *Ethics and Information Technology* 11 (4): 233-241.
- Palm, E. 2013. Rights that trump - Surveillance-based migration governance and the need for a substantial right to mobility. *Journal of Information, Communication & Ethics in Society* 11(4): 201-215.
- Van der Ploeg, I. 2002. Biometrics and the body as information: normative issues of the socio-technical coding of the body. In: *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, ed. D. Lyon, 57-73. New York: Routledge.
- Rössler, B. 2005. *The Value of Privacy*. Cambridge: Polity Press.
- Stoddart, E. 2008. Who Watches the Watchers? Towards an Ethic of Surveillance in a Digital Age. *Studies in Christian Ethics* 20(3): 362-381.
- Walzer M. 1992. *Just and Unjust Wars*, 2nd edn. Basic Books.