FP7-SEC-2011-284725

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency

Collaborative Project

SURVEILLE Deliverable 4.5: Surveillance, the moral presumption of innocence, the right to be free from criminal stigmatisation and trust

Due date of deliverable: 30.09.2013

Actual submission date: 30.09.2013

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP04 Prof. Martin Scheinin (EUI)

Author: Katerina Hadjimatheou (UW)

Table of Contents

Executive Summary

1. Surveillance stigmatises people as criminal when it marks people out as potentially having failed to uphold or being thought likely to fail to uphold the criminal law.
2. The harms of being stigmatised as criminally suspicious include: humiliation; alienation from wider community; mistrust of and reduced willingness to cooperate with surveilling authorities; reduced security for society as a result of this reduced willingness to cooperate; increased risk of exposure to greater risks of discrimination and social exclusion by others; reduced equality, social cohesion, and policing legitimacy as a result of the former costs; and an increased risk of exposure to future measures of suspicion by police.
3. The most stigmatising surveillance practices are those that: single people out most visibly for scrutiny, imply the strongest suspicion of criminality, connect criminality to salient traits (e.g. ethnic appearance) and apply a stigmatic label that is difficult to remove or that adheres to a person over a long period of time.
4. The criminal stigmatisation caused by surveillance is disproportionate when it is more stigmatising or applies a stigmatic label for longer than is necessary to the aims of the investigation.
5. The right to be free from criminal stigmatisation is violated when surveillance practices impose a stigmatic label on individuals that is impervious to evidence of innocence.
6. Neither the use of profiling nor the creation of pools of pre-suspects conflicts in principle with the right to be free from stigmatisation, though some actual examples of these techniques may conflict with it in practice, if they are applied disproportionately.
7. The content of both formal and informal lists of pre-suspects should be responsive to evidence of innocence and of guilt. Individuals should be given opportunities to provide such evidence, wherever this is consistent with national security and the pursuit of ongoing investigations. In many cases it is appropriate to consider a lack of further evidence of guilt tantamount to evidence of innocence once a predetermined period of time has elapsed.
8. Surveillance does not impinge upon the right to be trusted if evidence is proportionate to the suspicion inflicted ***or*** if it can be justified most convincingly by appeal to reasons other than the untrustworthiness of those surveilled; when these reasons are those actually given in practice by the surveilling authorities; and when the policy is not inconsistent with an attitude of trust towards people in general.
9. Surveillance practices undermine trust as a social good if they are based on a presumption that people in general are untrustworthy, if they exaggerate though excessive heavy-handedness the untrustworthiness of particular groups of people singled out as suspicious, or if they draw attention to the presence of crime too forcefully so that people begin to overestimate the threat posed.

1. Introduction

Privacy has traditionally been the core value thought to be threatened by surveillance practices (Warren and Brandeis, 1890; Westin, 1967; Jarvis-Thomson, 1975). In recent years, equality and norms of antidiscrimination have also become a focus of concern by those examining the moral costs of surveillance (Lyon, 2002; Bou-Habib, 2008; Ryberg, 2011). Today, a new strand of critique focuses on the presumption of innocence, which is thought to be the latest casualty of surveillance practices.[1] This deliverable reviews and discusses this third line of critique; it examines the extent to which different surveillance techniques might undermine the presumption of innocence; and it draws on this analysis to reach conclusions about their ethical acceptability.

Traditionally, the presumption of innocence has been discussed only in narrowly legal discourse, as one component of the right of criminal defendants to a fair trial. But this is not what is intended by 'the presumption of innocence' as it often appears in contemporary moral and political debate about the justifiability of surveillance practices. What is meant instead is something like a right *not to be treated as criminally suspicious unless one has done something to warrant such suspicion*. This moral right to be presumed innocent is conceived as applying to all individuals who are subject to criminal suspicion or who are at risk of being subject to criminal suspicion. Its function is to protect people from being burdened with the harms of criminal suspicion unfairly.

This movement to recognise a broader, moral right to be presumed innocent has been prompted by recent developments and trends in police practices. Preventive policing practices including surveillance have come under particular criticism. Sometimes this is because they appear to treat with suspicion people who have done nothing in particular to merit such suspicion. Sometimes it is because they appear to justify such treatment on the basis of evidence that is weak and speculative. Surveillance techniques which have been criticised as undermining or curtailing the moral right to be presumed innocent include the mass monitoring of electronic communications represented by the US National Security Agency's PRISM programme (EU Parliament, 2013[2]); the use in the UK of CCTV cameras to monitor a mainly Muslim residential area in which it was speculated that terrorist sleepers may be operating (Galetta, 2012: 280); and the use by telecommunications companies of

[1] See in list of references Galetta and de Hert for IRISS, 2012: 283-291; Pavone for PRISE, 2008: 22; PACT,

[2] As reported in the *Inquirer*, in July 2013 the EU Parliament announced the launch of an inquiry into the compatibility of PRISM with rights including the presumption of innocence: "The Civil Liberties Committee inquiry [will] assess the impact of the alleged surveillance activities on EU citizens' right to privacy and data protection, freedom of expression, the presumption of innocence and the right to an effective remedy," (EU Parliament quoted in Inquirer, 9 July 2013 'European Parliament Votes for PRISM Snooping Investigation'. At http://www.theinquirer.net/inquirer/news/2280187/european-parliament-votes-for-prism-snooping-investigation

DPI (deep packet inspection) techniques to detect illegal file-sharing (Fuchs, 2012: 50; Privacy International, 2009).[3]

The right not to be treated as suspicious has been grounded in the interests people have in not suffering the harms of being stigmatised as criminal or potentially criminal (Campbell, 2010). It has also been grounded in a moral right to be treated as trustworthy (Nance, 1994; Duff, forthcoming). Some critics also appeal to the presumption of innocence to identify and object to the creation of an 'ethos of suspicion' (Kimmelman, 2000) or an erosion of the trust that forms the basis of social relationships in a liberal society (Lyon, 1994).

Given the increasing importance given in current debates about surveillance practices to the presumption of innocence broadly understood, and given also the fact that the SURVEILLE project has not as yet considered of such practices the risk to this particular ethical value, this paper makes the presumption of innocence its focus. It critically examines both the stigmatisation and the trust-based accounts of the moral presumption of innocence, drawing on academic work in these areas to reach conclusions about the ethical risks of specific surveillance techniques and practices.

2. The presumption of innocence as the right to be free from stigmatisation

Appeal to the presumption of innocence to criticise surveillance practices sometimes implies a right to not be stigmatised as criminally suspicious.[4] Concerns about the stigmatising effects of preventive surveillance practices have been expressed since the very first counter-terrorism measures were taken in the EU and USA in response to the September 11 attacks of 2001. For example, the German policy of data-mining for and surveillance of potential terrorist sleepers known as the *Rasterfahndung* was struck down by the German Federal Constitutional Court partly on the ground that it had a 'stigmatising effect' on those singled out, associating them unfairly with a propensity to terrorist crime. The court argued that this imposed harms on those suspected which could not be justified on the basis of the evidence (Breuwer 2009:23). Concerns about the stigmatising effects of surveillance have been raised most strongly in connection with measures that single people out on the basis of their ethnic (including racial and religious) traits (Bou-Habib, 2011; Ryman, 2011). They have also been expressed in relation to the creation of pools of 'pre-suspects' or individuals who are thought likely to become suspects in a police investigation in the future (S and Marper; Campbell).

2.1 Surveillance and the harms of criminal stigmatisation

[4] See, for example, 'taint of suspicion' (*S and Marper* 14) resulting from inclusion in the database and the implication that arrestees were 'less than wholly innocent' (*S and Marper* 89).

The harms inflicted by being stigmatised as criminally suspicious are rarely identified and examined in detail. It is worth doing so here, because this can help us to understand what is at stake for individuals when they are subject to such measures, and therefore how much weight, morally speaking, we should give to a right to not be stigmatised.

One standard understanding of stigmatisation defines it as the process of marking a person out as having an undesirable characteristic (Courtwright 2011; Arneson 2007). For the purposes of this paper, the undesirable characteristic associated with people who are marked out as suspects is *failure to meet the justified moral standards of behaviour of the community as these are contained in the criminal law*. When surveillance marks people out as suspects, it marks them out as potentially having failed to uphold or having violated a rule they are prima facie obliged to follow. In relation to the criminal law, the rules are those people are normally obliged to follow either because they have explicitly consented to do so or because they enjoy the benefits that accrue from a situation in which the rules are followed collectively.

The harms of stigmatising people as criminally suspicious can affect both individuals and society as a whole. On an individual level, being stigmatised as having failed to maintain the moral standards of the community can be humiliating. People are humiliated when they cannot prevent appearing to others in ways that are demeaning (Bou-Habib, 2011:44). Humiliation is not an intended outcome of the imposition of criminal suspicion, but it is often a foreseeable side-effect of such suspicion, even if the interference by police is proportionate and well-founded. If individuals who are humiliated as a result of their stigmatisation perceive the suspicion to be disproportionate or unfounded, they may feel anger or indignation at what they perceive to be an unjust implication of wrongdoing. This may create knock-on social costs, by eroding their trust in the surveilling authorities, which in turn may reduce their willingness to cooperate with those authorities and to support the enforcement of other rules (Fundamental Rights Agency of the EU FRA 2010: 21).

Stigmatisation can also make those affected feel alienated from others, as they perceive that others' estimation of them has fallen. This can affect negatively people's self-confidence and their willingness and ability to connect and engage effectively with others. It can also lead people to become socially isolated if they react by withdrawing from contact with others (Courtwright 2011:2). At the same time, social isolation of those stigmatised may be imposed from outside, if other individuals avoid or reject them or otherwise treat them as criminally suspicious as a result of surveillance policy. Thus the actions of police in the sphere of criminal justice can have knock-on effects in other spheres of life.

When particular groups of people who share salient traits –such as religion or race– are stigmatised as suspicious, as has arguably been the case with some measures of preventive profiling, this may exacerbate existing prejudices against them (Kennedy 1997; Schauer

1997; Lever 2004), or even create new ones (O'Connor and Rumann 2003). When stigmatisation based on ethnic grounds reflects ethnic prejudice it can be experienced as particularly humiliating both by those surveilled and indeed by those who are not themselves surveilled but who share the traits that trigger the suspicion and for that reason are implicated (Parmar 2011: 9). As all this suggests, stigmatisation can be harmful to individuals and can distort social relationships in ways that impede the pursuit of important social goals, including security and equality.

Stigmatisation can occur even if the fact that an individual is being surveilled is not made known to members of the public. As Campell points out in her discussion of DNA databases, being fingered as a suspect involves the official labelling of an individual as suspicious or potentially so. Merely the knowledge that one has been singled out by police as a suspect is sufficient for one to feel humiliated and alienated and thus suffer those harms resulting from the 'internalisation of a stigmatic label' (Campbell, 2010: 903).

All of these potential costs are likely to increase along with the importance of the crime one is suspected of having committed. Being stigmatised as a suspected illegal file-sharer is neither as humiliating nor as likely to lead to social isolation or discrimination as being stigmatised by police as a potential paedophile. The costs of stigmatisation are also likely to intensify the greater the implication of guilt conveyed in the measure of surveillance: a bag search is less stigmatising than a house search, which in turn is less stigmatising than being taken to the police station for questioning. The extent to which people are stigmatised may also be affected by the number and identity of any witnesses to the surveillance: other things being equal, the greater the number of people who witness or become aware of the stigmatisation and the more influential or important those people are, the more severe both the individual and social costs are likely to be.

Stigmatisation can also result when the individual surveilled is not made aware of the suspicion they have come under, for example, if the surveillance is covert or never revealed. These costs result from the differential treatment by police of suspected individuals. In particular, it has been argued that a stigmatic label sticks if records of people's interactions with police or of their identities and suspected crimes are kept in databases for the purposes of assisting police to solve future crimes (Campbell, 2013). For example, in the UK records of the police's interaction with individuals are maintained in a National Police Database. The NPD includes information on individuals who have been subject to some kind of suspicion as well as those who might be vulnerable to crime, amongst others.[5] This information is shared amongst police forces and may be used to assist police investigations

[5] For an overview of aims and functionality, see: 'The Police National Database: Making a Difference: a guide to getting the most from the PND'. National Policing Improvement Agency, 2010. Downloadable at http://www.logica.co.uk/~/media/United%20Kingdom/Media%20Centre%20Items/Brochures/Making_A_Difference_Oct2010.pdf. Last Accessed 24.09.13.

by, amongst other things, identifying potential suspects. In addition, police forces in many countries maintain DNA databases that include the records of individuals who have been convicted of crimes, some of which also include the records of individuals who have only been arrested of crimes.[6] This process has been described as the creation of a 'pool of pre-suspects' (i.e. people who are thought likely to become suspects in a police investigation in the future).[7] Being included in a pool of pre-suspects may be stigmatising because it implies that a person is more likely to be involved in future crime. The costs associated with this kind of stigmatisation relate to the increased likelihood they are exposed to of being treated as a suspect- and thus also potentially stigmatised again- by police in the future.

The removal of stigmatic labels

Some stigmatic labels are more adhesive than others, and the harms of applying these may be difficult to contain. Being arrested on suspicion of having committed a crime is stigmatising, but the stigmatic label that attaches as a result of arrest is removable if the person is subsequently released without charge and someone else goes on to be convicted of the offence in question. In such a case, the fact that someone else has been convicted of the crime is decisive evidence of the person's innocence. As a result, the police will allow an individual to drop off their radar and no trace of suspicion should remain.[8] If people other than the police continue to treat the individual as criminally suspicious on the basis of the arrest-- say, by ostracising them-- the individual concerned can point to the fact that another person was found guilty of the crime as a sufficient reason to stop considering them suspicious. In this example, the harms suffered by the suspected individual should be short-lived and few if any of the social costs identified above should result.

But sometimes the stigmatic label applied by a police action may remain, at least in the eyes of the public, even when it is officially removed by police. For example, some arrests, such as those involving sexual abuse, occur in response to an accusation involving the specific individual concerned. In such cases, the stigmatic label may adhere to the individual even if the case is dropped on grounds of insufficient evidence, *unless* the accusation is also demonstrated to be baseless. In some cases in which individuals have been accused but not convicted of sexual offences, especially child abuse, the stigmatisation may be very harmful to them and may persist for a long time. Concerns about such cases have prompted debate over whether the harms suffered by those accused but not convicted of sexual offences are

[6] For an overview of European systems see ENFSI (European Network of Forensic Science Institutes) *DNA-DATABASE MANAGEMENT REVIEW AND RECOMMENDATIONS*. ENFSI DNA Working Group. April 2012). At http://www.enfsi.eu/sites/default/files/documents/enfsi_document_on_dna-database_management_2012_0.pdf. Last Accessed 17.09.13

[7] It is worth noting that much looser, less official practices can also result in the creation of a pool of pre-suspects of this kind, such as when police rely on their knowledge and experience of a community and the individuals who populate it to make decisions about, for example, who to approach with questions when a crime is committed.

serious enough to warrant protection through legally enforced anonymity until a conviction is established.[9]

Profiling on the basis of broad generalisations about the propensity of certain type of people for certain types of crime may also inflict stigmatic labels that are hard to remove. This is because the correlation between the profiled traits and criminality, which has been asserted as the basis for the suspicion, exists independently of any specific criminal investigation. Thus it may continue even after the investigation or preventive measure has been discontinued. For example, if police were to systematically target young black men for preventive stop-and-search (as they did in London in the 1980s and have been accused of continuing to do more recently[10]) they encourage both police and people in general to associate being black, young and male with criminality. Once made, such associations stick in the mind and may be hard to undo, even if they cease to be accurate representations of criminal trends. In this way, even if the stigmatic label imposed by police profiling is officially lifted, it may continue to be applied in society at large, and indeed by individual police officers unofficially. As a result, people may find themselves treated as criminally suspicious long after the surveillance has been discontinued. In these cases, public statements by police supported by evidence dissociating the group in question from crime could help lift the taint of suspicion.

To summarise, the harms of criminal stigmatisation are:

1. Individual humiliation
2. Individual alienation from wider community
3. Individual mistrust of and reduced willingness to cooperate with surveilling authorities
4. Reduced security for society as a result of (3)
5. Individual exposure to future measures of suspicion by police
6. Individual exposure to greater risks of discrimination and social exclusion by others
7. Reduced equality, social cohesion, and policing legitimacy as a result of (2), (3) and (6)

Generally speaking, the most stigmatising surveillance practices are those that:

---

[9] In the UK proposals to legally enforce anonymity of those accused of rape enjoy wide support and were included as a manifesto pledge by the third party, the Liberal Democrats in 2006. For an overview of the debate in relation to a recent case see, 'Should Rape Suspects Get Anonymity?' Marie Jackson. 11 Sept. 2013. BBC News. http://www.bbc.co.uk/news/uk-24037910

[10] Lord Scarman, 1981, *The Brixton Disorders April 10-12 1981: Report of an Enquiry,* London: HMSO. For a more recent critical review of the proportionality of stop and search in the UK see Equality and Human Rights Commission (2010) 'Stop and Think: A Critical Review of the Stop and Search Powers in England and Wales'. Downloadable at http://www.equalityhumanrights.com/uploaded_files/raceinbritain/ehrc_stop_and_search_report.pdf. Last Accessed 24.09.13.

a) single people out most visibly for scrutiny
b) connect criminality to salient traits that can be used as a basis for discrimination in other spheres of life (e.g. racial profiling)
c) imply the strongest suspicion of criminality
d) associate an individual with the most serious kinds of wrongdoing and
e) apply a stigmatic label that is difficult to remove or that adheres to a person over a long period of time.

Stigmatisation and surveillance in relation to surveillance techniques used in MERPOL scenario

Most of techniques applied in the criminal investigation scenario provided by SURVEILLE project partners MERPOL (Merseyside Police, see Annex 1 of D2.6) exhibit only (c) and (d) of these features. For example, the use of recording bugs and the deployment of surveillance teams are highly intrusive practices that require strong suspicion of criminality for authorisation, at least in most EU member states. But they do not involve visibly singling people out. Neither do they involve selecting people on the basis of salient traits. Thus they do not create an impression of criminality in the eyes of either the individuals monitored or other people more generally. Neither do they risk leading to discrimination. If the investigation were abandoned for lack of evidence, but the suspects were still considered suspicious enough to be entered in a register of pre-suspects for future reference or on a watch-list for further surveillance then the stigmatic label may remain, bringing (e) into play.

Other techniques used in the MERPOL scenario, such as open-source internet surveillance, or the running of money laundering checks, neither visibly single people out nor imply strong suspicion of criminality. Nor do they persist once the search has come out clear. They are therefore less stigmatising than the use of recording bugs and the deployment of surveillance teams.

Only those surveillance practices which - like those just discussed- target people or types or groups of people for suspicion are stigmatising. Mass surveillance practices, such as the use of open-street CCTV throughout a city centre or the use of ANPR cameras to monitor all vehicles entering and exiting an urban area single out and therefore stigmatise no one. Neither do measures such as the use by Internet service providers of DPI techniques to carry out speculative monitoring of data traffic to detect illegal file sharing.

2. 2 Justifying the harms of stigmatisation

Surveillance practices that stigmatise people as criminal or potentially criminal can be harmful for that reason.[11] The harms of stigmatisation provide us with a reason to recognise a right in not to be stigmatised, and to impose a corresponding moral duty on police to refrain from stigmatising people as criminally suspicious without good enough reason. It is generally accepted that evidence linking a specific individual to a particular future or past crime is sufficient grounds for treating them as a suspect, and inflicting on them the costs of such treatment. The stronger the evidence, the more justified the use of highly stigmatising measures of suspicion.

2.2.1 Stigmatisation, surveillance, and profiling

Some argue that only certain kinds of evidence can justify interferences with the right to be free from stigmatisation. For example, it has been argued the individual right to be free from stigmatisation trumps 'collective demands or ends' such as the pursuit of security (Campbell, 2010: 904). This, it is argued, means that only those who have forfeited their claim to that right by behaving in a way that gives rise to suspicion can be legitimately stigmatised as suspicious. Implicit in this account of the right to be free from stigmatisation is the claim that the only basis for limiting or people's rights is their own, freely chosen, behaviour. This way of justifying stigmatisation puts the responsibility for the harms inflicted on the shoulders of the suspect. Thus it is consistent with the general moral principle that people should only suffer harms and disadvantages on the basis of features about themselves over which they have some control.

However, there are problems with this way of justifying criminal stigmatisation. In particular, it implies a clear and observable distinction between behaviour that is objectively 'suspicious' as opposed to 'normal' or 'innocuous', and it implies that those who engage in the former are freely choosing to act in such a way as to expose themselves to scrutiny by police. But it is not the case that people typically know in advance what kind of behaviour is likely to attract police attention. Nor is it typically the case that can they choose whether or not to engage in it and therefore whether to risk being targeted with surveillance and bearing the costs of the criminal stigmatisation this brings. Some kinds of behaviour *are* objectively suspicious (chasing someone down the street brandishing a kitchen knife, for example). It seems correct to claim that people who choose to act in such ways are responsible to an extent for the harms that a proportionate police response to such behaviour brings. But not all behaviour that is in fact indicative of criminality or criminal

[11] Of course, criminality is stigmatised for good reason, namely that it is harmful and, generally speaking, a violation of the social contract and therefore unjustified morally. Indeed it is desirable that those who engage in criminal behaviour are stigmatised for that reason both for retributive reasons and as a means of deterrent. Stigmatisation is not therefore an unintended side-effect but an intentional consequence of criminalisation.

intentions is objectively or predictably so. Some kinds of otherwise entirely innocuous behaviour become suspicious just because it is known (or suspected) by police that a criminal or type of criminal tends to act or is acting that way. To claim that treating people as suspicious on the basis of this kind of behaviour always violates the right to not be stigmatised would restrict the range of cases in which stigmatising surveillance is justified too much to be coherent with a range of common and accepted police practices.

We may illustrate the point with a fictional example. Sometimes evidence might suggest a pattern of behaviour in certain kinds of criminal rings: we might image, for instance, that more than one drug-smuggling outfit has been discovered to operate between specific countries, using certain routes of travel, to travel on from airports to specific destinations, and to use mules who fit a certain age and gender profile. There is nothing objectively suspicious or dangerous about any of the features of this criminal gang, yet there is reason to believe that when all of those features are found in a group of travellers, a serious crime may be being committed. Police may decide to tackle such crime by applying a profile to travellers, and surveilling those who fit it by pulling them out of line in a passport queue, searching their bags, retaining them for questioning and/or following them from the airport to their destination, amongst other things. If they do, then it is possible that some innocent individuals will come under suspicion and be subject to the stigmatising effects of the surveillance they receive. The imposition of such stigmatisation cannot be justified by reference to the suspect's choice to engage in suspicious behaviour because there is nothing obviously suspicious about their behaviour. Moreover, the suspect is unaware that their otherwise innocuous behaviour has become suspicious by virtue of its link with criminal activity and thus has no opportunity to avert the suspicion.

Is profiling of this sort unjust as a result? It is not. As long as police follow procedures that ensure that surveillance will be stopped as soon as it becomes clear that insufficient evidence exists for continued suspicion, the measure can be defended as proportionate and legitimate. The suspicion and attendant stigmatisation suffered by innocent people who behave in apparently innocuous ways but nevertheless fit a criminal profile is un*deserved*. But it need not be considered un*fair* if it is inflicted only to the extent proportionate and necessary to the pursuit of an effective means of crime-reduction. The right not to be stigmatised as suspicious must be balanced against the need for police to have sufficient powers at their disposal to be able to prevent and investigate crimes. These powers must be sufficiently broad to enable police to cast a net wide enough to catch criminals and to pursue leads that are tentative. As long as it is based in sound evidence, the application of a criminal profile that is bound to result in false positives seems justified in principle. In practice, the extent to which the stigmatisation resulting from profiling is justified will depend on how necessary it is to the investigation and the strength with which it is supported by the evidence.

2.2.2 Stigmatisation, surveillance, and pre-suspects

Unlike other security officers, such as border guards, police have powers of discretion that authorise them to create and maintain both formal and informal pools of pre-suspects for surveillance, and to act on their own personal knowledge of individuals and of particular communities. This particular aspect of discretion is justified on the basis that it assists police in acting proportionately and effectively to reduce crime. Police routinely receive intelligence of and experience encounters with people who they have good reason to believe are involved in criminal activities. For a range of reasons, these grounds for suspicion sometimes do not result in arrest let alone conviction. The power to retain, share, cross-reference and, more importantly, act on this information is essential to the ability of police to address crime. It should be exercised proportionality. While police may keep in mind a list of potential suspects for particular crimes, that list should be regularly updated to reflect, among other things, the time that has passed since a person acted suspiciously, and should not lead to a situation in which a group of usual suspects is unfairly fingered each time a certain kind of crime is committed. If a police force is trusted as sufficiently professional, impartial and incorruptible, then the exercise of such powers is unlikely to result in unfair suspicion and stigmatisation that is systematic.

It has been argued, however, that the right to be free from stigmatisation precludes 'the formalised entrenchment of a category of suspects who are subject to increased State intervention because of prior suspicion' [Campbell, 2010:8]. But this would leave potential victims too exposed to serious crime. We can see why by considering some, hard-to-prosecute types of crime, in which police powers of discretion to apply suspicion and to act on knowledge of an individual's past behaviour are essential to the prevention of serious harm. For example, it is notoriously difficult to prosecute individuals who are violent towards their partners, in part because of the fear and resulting reluctance of those partners to bring charges or to provide evidence. Yet in 2010-11 domestic violence resulted in the deaths of 2 women per week in the UK, which amounts to one-third of all homicides. As a result, police in the UK have been criticised for *not* acting with sufficient force on their knowledge about the proclivity for violence towards their partners of certain individuals.[12] Here, the difficulty of pursuing traditional criminal justice channels have led police to institute preventive measures including surveillance and disruption in order to reduce the threat to victims. For example, in one area of Scotland where domestic violence rates are very high, police maintain a list of violent individuals who are then preventively warned by police or otherwise deterred from violence around the time of key events, such as football matches, which have been shown by research to trigger attacks.[13] Similarly, Essex police

[12] See Laville, *The Guardian Newspaper*, Thursday 13 June 2013. 'Police to reveal details of partners' pasts to tackle domestic violence'. At http://www.theguardian.com/society/2013/jun/13/domestic-violence-police-partners-tackle

[13] The Detective Chief Inspector leading the McPike explained 'If we think it's appropriate, we might knock on the person's door and … give them a warning and say 'we know you've done this before, don't do it.' See Hirsch, Aufa 'Is there a happy ending to Scotland's Minority Report?' *The Guardian* 16 May 2010.

maintain a dossier on individuals with a history of violence towards partners, which is then made available upon request to partners embarking on a relationship with those individuals. It is also common practice for police to inform parents embarking on a relationship with convicted sex offenders of their partner's history as this may trigger surveillance of the family for child protection purposes.

These strategies have been accused of undermining the presumption of innocence (Ibid). But this cannot be right. The function of the presumption of innocence is to protect innocent suspects being unfairly stigmatised, not to shield dangerous people from proportionate and evidence-based preventive police interference. It is true that issuing warnings or conducting surveillance in advance of specific evidence suggesting that a crime is imminent involves stigmatising police interference. But the scope of any given individual's claim to have a right not to be stigmatised as criminal must be limited both by the existence of demonstrable evidence that they are acting or are about to act criminally and by the need to prevent serious crime. Were suspected wife-beaters coercively tagged with surveillance equipment in advance of each of their team's matches, instead of merely warned and checked up on, then the proportionality of the stigmatisation may be rightly questioned. But to claim that the right to be free from stigmatisation precludes in principle the creation of a pool of pre-suspects seems too restrictive to be consistent with the aims of the right- to protect individuals from *unfair* stigmatisation as criminal. It is also too restrictive to be consistent with the protection of individuals at serious risk of violent crimes - crimes that inflict harms far graver than those of criminal stigmatisation. It is not difficult to imagine what would happen if police refrained from acting on their knowledge of individuals' proclivity to domestic violence: strong historical evidence exists to show that the result is high numbers of avoidable deaths and even higher numbers of serious injuries.[14]

It seems reasonable to conclude that the kinds of interference described above and similar pre-suspect practices do not seem disproportionate given:

1. the strength of the evidence of prior wrongdoing;
2. the rate of recidivism of those convicted of such crimes;[15]
3. the seriousness of the harm threatened; and
4. the difficulty of obtaining evidence that an attack is imminent that is reliable enough to justify coercive preventive measures.

---

http://www.guardian.co.uk/law/afua-hirsch-law-blog/2010/may/16/scotland-crime-minority-report. Last accessed 15.03.2013.

[14] According to the UK Office of National Statistics, 2 million cases of domestic violence were recorded in 2011-12. 51% of female homicides were carried out by partners. ONS (2013) 'Focus on: Violent Crime and Sexual Offences, 2011/12'. At http://www.ons.gov.uk/ons/dcp171778_298904.pdf. Last Accessed 20.09.13.

[15] In 2010/2011, repeat victimisation accounted for 73% of all incidents of domestic violence, 44 % were victimised more than once and 24% of victims had been victimised three times or more (Chaplin et al., 2011, quoted on CAADA Coordinated Action Against Domestic Violence website) http://www.caada.org.uk/policy/statistics.html. Last Accessed 10.09.2013.

In contrast, surveillance that results in the stigmatisation of individuals as criminally suspect is disproportionate if it is more intrusive or continues for longer than is necessary to the aims of the investigation or the prevention of crime. Many of the criticisms of surveillance that make appeal to the presumption of innocence focus on practices that impose a stigmatic label on individuals that persists beyond the end of an investigation and/or is excessively difficult to remove.[16] The imposition of suspicion on innocent individuals in criminal investigations is tolerable in part because it is meant to be a temporary harm that will stop once the lack of evidence in support of guilt is revealed. Likewise, the stigmatic label attached to an innocent criminal suspect is tolerable because of the prospect and promise that it will be removed and the mistaken implication of criminality corrected.

Surveillance practices impose a stigmatic label on individuals that is impervious to evidence of innocence, violate the right to not be stigmatised. Respect for the right to be free from stigmatisation requires the establishment of clear criteria for both including and excluding people from pools of suspects and pre-suspects. The decision to include a person in a pool of suspects or pre-suspect should be responsive to new evidence regarding the criminality of the individuals listed. Evidence here might take different forms, depending on the kind of crimes people are suspected of. The decision to include an individual in a sex-offenders register, or in a register of individuals involved in organised crime, both of which are used in some jurisdictions as a basis for surveillance, may be responsive to different kinds of evidence than the decision to include an individual on a travel watch-list.

In the case of surveillance triggered by a match with a criminal profile, as described above, one form of evidence might be evidence resulting from the measure of surveillance itself. For example, if an individual is questioned, searched, and covertly followed from the airport but no evidence of criminality is uncovered, this would count as evidence sufficient to require removal from the list of suspects. Another kind of evidence might be provided by other sources, such as intelligence or new, more sophisticated profiles, suggesting some individuals on the list are not suspicious. Another kind of evidence might result from the consideration of time-lapses as a proxy for evidence of innocence: if a certain amount of time has passed and no confirmation of the individual's suspiciousness has been provided, they could be removed from the list. In some cases, it may be appropriate to provide

[16]See, for example, the release of FBI documents in 2011 suggesting that 'The Federal Bureau of Investigation is permitted to include people on the government's terrorist watch list even if they have been acquitted of terrorism-related offenses or the charges are dropped' Charlie Savage 'Even those cleared of crimes can remain on FBI's watchlist.' New York Times, Sept. 27, 2011. At http://www.nytimes.com/2011/09/28/us/even-those-cleared-of-crimes-can-stay-on-fbis-terrorist-watch-list.html?_r=4&hp=&pagewanted=all&. Last Accessed 25.09.2013. See also UK civil liberties campaign group Liberty's criticism of the use of Terrorism Prevention and Investigation Measures, which targets cannot contest with the use of evidence. http://www.liberty-human-rights.org.uk/human-rights/terrorism/control-orders/index.php. Last Accessed 24.09.13.

suspects with the opportunity to provide evidence supporting their exclusion from suspicion.[17]

The right to not be stigmatised can provide a basis for criticism of measures of surveillance that are targeted. The right to not be stigmatised cannot be drawn upon to criticise measures of mass, indiscriminate surveillance or data retention that single no one out for suspicion, such as that undertaken by open-street CCTV systems. Indeed, a solution to the problem of stigmatisation could be to surveille *all* citizens instead of just some. But many of the criticisms against surveillance that appeal to the presumption of innocence take issue with precisely these forms of mass monitoring (Haggerty and Ericson 1997: 42; Monahan, 2010: 99). If we want to identify the most convincing ethical basis for claims that such measures of suspicion can conflict with a right to be presumed innocent, then we must look to other proposals for how that right should be understood in the context of preventive policing. The following section takes up one such proposal, which interprets the right to be presumed innocent as a right to be trusted.

3. The presumption of innocence as the right to be trusted

Like arguments from a right to be free from stigmatisation, arguments from the right to be trusted have also been drawn upon to object to measures which single people out as suspicious. But unlike the right to be free from stigmatisation, the right to be trusted can in principle be violated by mass surveillance: while it is not possible to mark everyone out as suspicious, it is possible to treat everyone as if they are untrustworthy.

There are two lines of argument about the ethical acceptability of mass surveillance that appeal to the notion of trust. The first claims that mass or speculative surveillance is based on the premise that everybody is untrustworthy; that in doing so, it acts on a presumption of guilt; and that this conflicts with a duty to presume people innocent of criminal activity in the absence of evidence to the contrary. A philosophical basis for this argument can be provided by drawing on the work of some legal philosophers who have attempted to connect a moral right to be presumed innocent to a moral right to be treated as trustworthy by the state (Duff, 2012; Nance, 1994; Stewart, 2013).[18]

[17] Many measures affecting terrorist pre-suspects do not allow individuals to do so. See, for example, the FBI's terror watch lists in footnote 16 above; US practices towards individuals and organisations designated Unindicted Co-conspirators and/or Joint Venturers (see ACLU 'Unindicted Co-conspirators and the Presumption of Innocence' 2008 at https://www.aclu.org/national-security/unindicted-co-conspirators-and-presumption-innocence. Last accessed 25.09.2013.

[18] Specifically, the right to be treated as trustworthy has been justified as a corollary of either the 'principle of civility' or the 'principle of civic trust', or both. The principle of civility imposes a duty on all people to treat each other as if they have been and are acting in accordance with their important social obligations, including but not limited to respect for the criminal law (Nance, 1994). Failure to treat people in ways consistent with the principle of civility presumption equates to a failure to accord them "dignity associated with the status of membership in the community that is governed by the norms whose breach is at issue" (Nance 1994: 653). The

The second line of objection claims that surveillance engenders mistrust between citizens and states and between citizens by 'promoting the view that everybody is untrustworthy' (Norris in House of Lords 2009: 27[107] [19] or by 'spreading a widespread sense of suspicion' (Lyon 1994:10).[20] While this latter line of argument appeals to trust as the value motivating a presumption of innocence, it is concerned less with violations of individual rights to be trusted and more with the role of trust as a value that makes certain social interactions possible and improves the moral quality of those interactions in general (Hardin, 2002; O'Neill, 2002). It suggests that the use of mass surveillance in preventive policing contributes to the diminishment of trust in society and is objectionable morally for that reason (Wood et al, 2006; Goos et al, 2012). In contrast to the first line of argument, which views trust as something that can be claimed as a moral right, this strand of thought views it as a social good to be promoted.

Each of these positions will be examined in turn, with a view to drawing conclusions about the ethical acceptability of specific surveillance practices.

3. 1. The right to be trusted

Determining whether a particular measure of surveillance conflicts with the right to be trusted is more difficult than determining whether it conflicts with the right to be free from stigmatisation. This is because stigmatisation is an outcome that can often be predicted and observed, whereas trust and mistrust are attitudes. Motivations and the attitudes behind them are not always transparent. More than one motivation and attitude can be behind a particular policy or practice. So it is not always obvious whether a particular surveillance

---

principle of civic trust is very similar to the principle of civility, but includes a duty to treat people as if they will continue to act in accordance with those obligations and thus makes the principle of civility forward-looking and not merely retrospective. Failure to accord people appropriate civic trust fails to treat them 'as agents who can recognise, and guide their actions by, appropriate reasons for action' (Duff:10). In other words, failure to presume people innocent of norm-breaking behaviour or intentions is incompatible with respect for them as moral agents: as people who can recognise and be guided by moral reasons not to do certain things, like engage in actions that cause harms to others. Campbell has also moved towards this interpretation of the pre-trial moral right to be presumed innocent in a more recent paper (Campbell, 2013: 690).

[19] Clive Norris argued in his testimony to the UK House of Lords' inquiry into surveillance that mass surveillance 'promotes the view…that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting the view that as citizens we cannot be trusted' Norris in House of Lords 2009: 27[107]

[20] Some closely related objections to surveillance from the presumption of innocence connect to the importance of preserving a *social ethos* of trust as opposed to one of suspicion. For example, Kimmelman argues, in relation to the extension of records included in DNA databases beyond convicted offenders that: "storing information on otherwise unsuspected individuals that would be primarily used for criminal investigations in effect expresses an ethos of suspicion. Although such defensive policing might deter some crimes and solve others, it nevertheless creates a chilling dynamic between the government and its citizens, and undermines the long-standing legal tradition in the US of presumption of innocence" (Kimmelman, 2000: 695)This position will not be treated separately here as many of the arguments put forward in this section of the paper would apply to it equally well.

practice is motivated by mistrust or by some other, morally unproblematic attitude. Policies of surveillance that might at first glance appear to communicate mistrust may be justifiable by appeal to reasons that have nothing to do with the trustworthiness of the people they affect.

For example, measures of preventive surveillance such as airport security screening, or the use of security checks for individuals who work with children may appear to communicate suspicion or mistrust. But it is equally possible that the reason that people who work with children are required to demonstrate credentials is connected to the fact that children are exceptionally vulnerable to harm and society has a duty to take special measures to protect them. Similarly, it is possible to justify airport screening by pointing to the fact that travelling by air is a risky activity which people will only volunteer to engage in if their fellow-passengers agree to submit to surveillance in order to reassure each other they are following the rules.

These arguments, which appeal to the importance of minimising risks and protecting the vulnerable, provide a better- that is, more rational- basis for justifying these kinds of surveillance than the argument that they reflect a presumption of untrustworthiness. There is no rational reason why people travelling by air or working with children should be considered less reliable in upholding the criminal law than people who do not travel by air or work with children. What is more, subjecting all air travellers to surveillance in the form of screening is compatible with an assumption that people are for the most part trustworthy with regard to the criminal law and the safety regulations of air travel.

When a policy of surveillance can be most convincingly justified by appeal to reasons other than the untrustworthiness of those surveilled; when these reasons are those actually given in practice by the surveilling authorities; and when the policy is not inconsistent with an attitude of trust towards people in general, then the surveillance can be said to be compatible with the right to be trusted. If this is correct, it follows that the use of background checks for individuals working with children and the use of blanket screening techniques at airports do not conflict with the right to be trusted.

Legal philosopher Anthony Duff has offered an alternative means of defending the compatibility of mass surveillance with the right to be trusted. He begins by acknowledging that where there is no mistrust there is no role for deterrence punishment (because if people were presumed to be trustworthy they would not need deterrents to persuade them to refrain from crimes). But he claims that the existence of a system of deterrence is compatible with the right to be treated as trustworthy if we can understand it ‘not as system by which a law-abiding ‘we’ deter a criminally-minded ‘them’, but as one by which we aim to persuade ourselves, as fallible humans, to refrain from conduct that we know to be wrongful’ (Ibid. 10).

This argument provides a good explanation of the need for deterrence in the form of surveillance for some kinds of law breaking but it is less convincing as an explanation for the need for deterrence against the most serious forms of crime. To illustrate, speeding is generally recognised to be dangerous to life and therefore most people can agree that speed limits should be imposed and respected. However, many of these same people might be tempted to break those limits when they are in a hurry, even though they recognise and support the moral reasons for refraining from speeding. This might be explained in part by people's tendency to be excessively confident in their estimation of their driving skills and to underestimate the risks of driving. The fact is that in the absence of the strong deterrent presented by the presence of speed cameras, there are likely to be significantly greater numbers of deaths from speeding than would otherwise be the case. And for that reason the very same people who might otherwise be tempted to speed may be grateful for the presence of a deterrent (in the form of a very effective means of detection) that prevents them from doing so.

This kind of argument is less successful at explaining the need for deterrence for serious crimes such as murder or rape. Most people do not need to be threatened with lifetime imprisonment to refrain from murder or rape. Insofar as criminal punishment has a deterrent function, this can only be explained by reference to its effect on the motivations of those very few whom are already considering committing such crimes. But the existence of such deterrence is perfectly compatible with the presumption *that the vast majority of people* are responsible moral agents who do not need such deterrence to refrain from crime. Therefore it seems unnecessary to try to justify such deterrents as justified in the light of everyday human fallibility. Recognising the existence of an untrustworthy few and designing a system of deterrence with them in mind does not amount to treating everyone as untrustworthy.

It might be argued in response that everyone has an *individual* right to be treated as presumptively trustworthy, which means that they must not be monitored for criminal justice purposes unless there is evidence linking *them in particular* to a particular crime. Statistical facts about crime rates cannot, on this view, justify surveillance of individuals for whom there is no evidence of criminality. But we do not need to support such a demanding right in order to ensure that surveillance policy treats people with respect or dignity. It is perfectly consistent with respect for individuals to allow the state to act on evidence about the criminality of people in general in order to gather evidence of the criminality of specific individuals. As long as individuals are not treated as criminal suspects -—that is, as long as they are not treated as if there were individually incriminating evidence against them when there is not—subjecting them to indiscriminate preventive interference on the basis of statistical evidence is not inconsistent with treating them with respect.

A right not to be treated as untrustworthy is more defensible as a basis for regulating preventive interference by the state for security purposes. Such a right would require that evidence be given to demonstrate the necessity and proportionality of any monitoring of individuals, though as we have seen statistical evidence could in principle support indiscriminate monitoring. Respect for such a right would also be consistent with the automatic mass retention of data of all kinds, including DNA data, communications data, and PNR (Passenger Name Recognition) or other location data. To claim that such practices are consistent with respect for the right not to be treated as untrustworthy is not the same as claiming that they are justified all things considered. The blanket retention of data may be opposed on grounds of concerns of mission creep; error, vulnerability to misuse and abuse and other privacy-related concerns amongst others. But this paper is concerned exclusively with the compatibility of such measures with the moral right to be presumed innocent. And there is good reason to think that they are not in principle incompatible.

There are additional reasons for rejecting assertions of an individual right to be trusted and proposing instead recognition of a more modest, negative right not to be treated as untrustworthy (in the absence of sufficient evidence). Such a right would better explain existing criminal justice practices and it would also reflect better our formation of interpersonal trust-related attitudes. Taking the second of these points first, it is important to recognise that trust and distrust are not the only two trust-related attitudes it is possible to adopt but exist at opposite ends of a spectrum of attitudes. (Ullman-Margalit, 2002). In our relations with other people, we usually require *grounds* for trusting or mistrusting people, usually in the form of evidence drawn from our knowledge of their character or past conduct. When such evidence is lacking or insufficient, adopting an attitude that lies somewhere between trust and mistrust and acting in ways that reflect that attitude is both reasonable and fair. An absence of evidence of individual wrongdoing is not equivalent to evidence of innocence of wrongdoing. Therefore it would be unreasonable to require individuals to treat each other as trusted in the absence of evidence demonstrating trustworthiness. It would be equally unreasonable to require police to treat all individuals for whom there is no individually incriminating evidence of wrongdoing as if there existed evidence of their innocence with respect to the criminal law. But asserting a right to be trusted implies that that is precisely what morality does require.

The argument that surveillance presumes everyone to be guilty (understood as untrustworthy) until the evidence it reveals proves otherwise (Norris and Armstrong, 1999:24) often appears to imply the view that a failure to trust people equates to actively mistrusting them. This may explain why mass or indiscriminate surveillance such as the use of open-street CCTV is sometimes said to cast a shadow of mistrust over populations (Norris in House of Lords 2009: 27[107]). But the presumption that all people are guilty of criminal transgressions would support measures that are far more intrusive and controlling than most current uses by liberal democracies of open-street CCTV or profiling. Indeed, it would

support something like Bentham's panopticon, which was designed to control those already convicted of crimes and thus proven to be untrustworthy. Most current uses of surveillance by state security agents come nowhere near to being as comprehensive, intrusive, or communicative of mistrust as that.

Many uses of surveillance reflect different gradations of trust placed in different individuals. Most obviously, airport security systems sometimes employ complex profiling systems which create tiers of passengers who are subjected to different kinds of screening depending on the security risk they are thought to pose. For example, the USA's TSA trusted passenger scheme creates a tier of trusted individuals who have provided information about themselves demonstrating their low-risk status. These passengers are then subject to less intrusive screening than most other passengers. At the same time, profiles are used to select higher-risk passengers for additional screening.[21]

3.2 Trust and speculative preventive surveillance

These points could be drawn upon to analyse the compatibility with this aspect of the presumption of innocence of measures of surveillance that monitor the activity of large numbers of people speculatively (i.e. in advance of any evidence of wrongdoing) for evidence of criminality. The use of such techniques has been accused of infringing the presumption of innocence by assuming the existence of wrongdoing and justifying interference on the basis of this assumption but in advance of evidence of it. For example, it has been argued that the use by telecommunications companies of DPI (deep packet inspection) techniques to monitor web traffic infringes the presumption of innocence. One example of such a technology was proposed by telecoms company Virgin Media as a means to detect illegal file sharing on its network. The technology, called CView, monitors Web traffic, identifies peer-to-peer packets, and then inspects them using information provided by record companies to detect copyright infringement. Privacy International has argued that this practice constitutes a 'paradigm shift with regards to the balance of justice' by acting on an assumption that 'all consumers are guilty of copyright infringement until their communications data proves otherwise'. Instead, they argue, 'the onus should be on the injured parties to provide their own evidence that an infringement has occurred' (Privacy International, 2009 in Fuchs, 2012: 50).

There are two problems with this criticism of speculative surveillance. First, contrary to what is claimed by Privacy International, it is not at all obvious that the use of DPI surveillance is premised on an assumption that *all consumers* are guilty of copyright violation. Instead, the only assumption necessarily revealed by such a policy is the assumption that *some as-yet-*

[21] For a media description of the TSA's trusted passenger programme see http://www.dailymail.co.uk/news/article-2014991/TSA-pilot-trusted-traveller-program-faster-airport-screening.html

unidentified consumers are guilty of copyright violation, and that just seems an accurate assumption to make given the historical evidence. It is difficult to see how it could be convincingly argued that anyone's moral rights are violated by a policy just in virtue of the fact that it acts on an accurate assumption about the prevalence of illegal activity.[22]

Secondly, Privacy International's objection to the use of DPI provides an example of a common misapplication of the burden of proof aspect of the presumption of innocence to surveillance activities. PI argues that the onus should be on the injured parties to prove that an individual has infringed their claim to own the rights to a piece of music. This is a direct application of the legal principle placing the burden of proof in criminal trials on the prosecution. That principle is often justified morally in instrumental terms, on the basis of its tendency to support fair criminal justice outcomes: placing the burden of proof on the prosecution redresses the disadvantage of the defendant relative to the state and thus protects them from wrongful conviction (Lippke, 2010; Findlay and Scott, 2006). File-sharing surveillance is not equivalent or tantamount to requiring individuals to prove their innocence in court. Because any accusation of illegal file sharing *follows* the collection of evidence, it cannot be said to place the burden of proof on individuals to prove their innocence in the absence of evidence of guilt. Neither is there any reason to think it increases the risk that individuals are wrongfully or mistakenly accused of illegal activity and thus undermines the function of the rule placing the burden of proof on the accuser.

There *is* a sense in which the burden of proof should be on the surveilling authorities, but this is not contradicted by the use of DPI for illegal file-sharing. The liberal principle of non-interference requires that there be a burden of proof on the authorities to demonstrate a good reason for any measure of surveillance. In the case of DPI surveillance, good reason is provided in the form of evidence from injured parties that their copyright is being infringed by unidentified individuals. The existence of such evidence provides a reason to interfere only as much as is necessary to gather evidence of illegal activity sufficient to support a formal accusation. This is perfectly consistent with the principles and procedures governing police investigation practices. And it need be considered no more sinister than a measure to install surveillance equipment to monitor employees in a shop in which money has been going missing from the till.

[22] It would be a different matter if the argument related to the proportionality of the interference represented by the use of DPI surveillance, given the seriousness and prevalence of illegal file-sharing. For example, if DPI technology was used to monitor the online activity of far greater numbers of individuals that was necessary to the detection of illegal activity, then this would constitute a reason for arguing that the surveillance should be scaled down. But the assumption that some illegal activity is occurring is not by itself an illegitimate ground for speculative surveillance.

3. 3 Surveillance and trust as a social good

As mentioned in the introduction to this section, it has been argued that surveillance by police contributes to a diminishment of trust in society and/or the spread of a sense of suspicion.[23] This criticism of surveillance should be distinguished from that which claims that some surveillance programmes are premised on mistrust of individuals, although in practice it is likely that the spread of mistrust would in practice result primarily from such programmes. This criticism does not focus on the appropriateness of the grounds for a particular measure of surveillance but on the undesirability of the outcomes. Trust between individuals, it is implied, is an important social good. To the extent that surveillance has the effect of diminishing that social good, it is problematic ethically.

The social benefits of trust are well-rehearsed in the academic literature. Trust creates opportunities for mutually beneficial cooperative activity of all kinds: we do not agree to work with people unless we have some trust in them to uphold their side of the cooperative agreement (McLeod, 2011). Controls such as enforcement may guarantee compliance and thus substitute for trust but this is a more expensive and complicated kind of cooperation (it involves checking up on each other) than cooperation based on trust (Luhmann 1979). It has been argued that trust could also be 'the very basis of society, insofar as trust in fellow citizens to honour social contracts makes those contracts possible' (Ibid). Trust has also been described as a type of "social capital," that makes it possible for "people to work together for common purposes in groups and organizations" (Fukuyama 1995, 10; quoted in Hardin 2002, 83). It has been suggested that "high-trust" societies can build social networks and economies that are more resilient than in "low-trust" societies (Fukuyama 1995; Inglehart 1999).

There is very little empirical evidence demonstrating the impact of surveillance practices on interpersonal trust (Ellis et al, 2013). However, it is possible to hypothesise that if surveillance is based on a presumption that people in general are untrustworthy, or if it appears to exaggerate though excessive heavy-handedness the untrustworthiness of particular groups of people singled out as suspicious, then it may discourage people to trust each other.[24] If surveillance practices rely on individuals to act as covert informants, then

[23] For example: "Especially important, and still debated, is the question about what impact an increasing amount of surveillance is having on an open society, if it does not in the end produce more suspicion than trust" (The Co-evolution of Surveillance Technologies and Surveillance Practices. Kerstin Goos, Michael Friedewald, Fraunhofer ISI, William Webster, Charles Leleux, in IRISS D1.1 Fighting crime and violence. p.69 http://irissproject.eu/wpcontent/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf,). See also the claim that surveillance 'fosters suspicion' negatively affects 'social cohesion and solidarity' WOOD, D. M. (Ed.), Ball, K., Lyon, D., Norris, C. & Raab, C. (2006) *A Report on the Surveillance Society*. Wilmslow, UK: Office of the Information Commissioner/Surveillance Studies Network. <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf See also Lyon, 1994:10.

[24] PACT Summary of PACT deliverables D1.1 - D1.6, cit., p. 95.

the deception and betrayal lurking behind everyday social interactions would also be likely to increase interpersonal mistrust. If surveillance practices draw attention to the presence of crime so that people begin to overestimate the threat it poses, then this may increase insecurity and discourage trust. This phenomenon has been termed the creation of a 'security paradox'. Some recent country-specific research suggests this paradox does not occur in relation to the use of open-street CCTV, but it is difficult to know how far we can extend these findings to other countries and the use of other surveillance practices.[25]

It is possible that some surveillance practices have no significant impact on interpersonal trust. Surveillance practices might be used as a substitute for trust, if they are used to gather evidence necessary to reassure people that others are cooperating according to the rules. For example, it is possible that in the absence of the reassurance of airport security screening, some passengers may avoid flying. Trust is a preferable basis for cooperation than surveillance. But in cases where the cooperation is risky and involves people who have few if any opportunities to draw conclusions about each other's trustworthiness, it may be very difficult to find ways of fostering well-founded trust. In such cases, blanket surveillance may substitute for trust without undermining it.

The selective mistrust that may potentially result from measures such as profiling, which single people out for surveillance, will not be discussed here. An implication of untrustworthiness is an inevitable aspect of criminal stigmatisation. The costs of the mistrust have been extensively discussed in Section 2 above in relation to discrimination against those stigmatised and greater exposure to criminal suspicion.

Conclusion

This paper has attempted to analyse the impact on the moral presumption of innocence of the use of surveillance by the state. It has considered two, compatible accounts of the moral basis for such a presumption. One sees the right to be presumed innocent as grounded in a right to be free from criminal stigmatisation. The other views it as grounded in a right to be trusted, or more convincingly perhaps, as the right not to be treated as untrustworthy. Neither of these moral norms given compelling reasons to think either targeted or mass surveillance is morally impermissible in principle. However, they do give us grounds on which to object to surveillance that stigmatises individuals disproportionately or which apply stigmatic labels that are insufficiently responsive to evidence of innocence. They also give us grounds on which to object to practices that monitor or gather data on a mass scale without sufficient evidence of pre-existing criminality or the utility of such a measure in

[25] Video surveillance in public spaces – is it really efficient? Study of the Katholieke Hogeschool Zuid-West-Vlaanderen, Expertisecentrum Maatschappelijke Veiligheid for the Belgian Ministry of the Interior (Flemish version: June 2013).

terms of crime-reduction. The impact of surveillance on trust as a social good is also considered. However, the lack of empirical evidence demonstrating a causal link between surveillance and trust means it is difficult to draw any firm conclusions about specific measures.

References

Arneson R (2007) Shame, stigma and disgust in the decent society. *Journal of Ethics* 11(1)

Bendrath, Ralf and Milton Mueller, "The End of the Net as we know it? Deep Packet Inspection and Internet Governance", New Media & Society, Vol. 13, No. 7, 2011, pp. 1142–1160

Bou-Habib (2008). Security, Profiling and Equality. *Ethical Theory and Moral Practice* 11 (2

Bou-Habib P (2011) 'Racial profiling and background injustice'. *Journal of Ethics* 15(1–2)

Breuwer (2009) 'Towards a European PNR System? Questions on the Added Value and the Protection of Fundamental Rights'. DG INT Study. At http://www.europarl.europa.eu/RegData/etudes/etudes/join/2009/410649/IPOL-LIBE_ET(2009)410649_EN.pdf

Campbell L. (2010) 'A rights-based analysis of DNA retention: "non-conviction" databases and the liberal state' *Criminal Law Review*

- (2013) 'The European Convention on Human Rights, and the Right to be Presumed Innocent' *Modern Law Review* 76(4)

Courtwright (2011) Stigmatisation and public health ethics. Bioethics 27(2)

Den Boer, M. (2012) 'Security Clouds: Towards an ethical governance of surveillance in Europe' in *Journal of Cultural Economy*

Duff (forthcoming) 'Who Must Presume Whom to be Innocent of What?' *Netherlands Journal of Legal Philosophy*

Ellis Darren, Harper David and Tucker Ian (2013) 'The Dynamics of Impersonal Trust and Distrust in Surveillance Systems' *sociological research online*. Volume 18, Issue 3, (1.2)

ENFSI (European Network of Forensic Science Institutes) *DNA-DATABASE MANAGEMENT REVIEW AND RECOMMENDATIONS*. ENFSI DNA Working Group. April 2012). At http://www.enfsi.eu/sites/default/files/documents/enfsi_document_on_dna-database_management_2012_0.pdf. Last Accessed 17.09.13

Findlay and Scott (2006) 'The Multiple Dimensions of Tunnel Vision in Criminal Cases' in *Wisconsin Law Review*, 291

Fundamental Rights Agency of the EU (FRA) (2010) *Towards more effective policing. Understanding and preventing discriminatory ethnic profiling: A Guide* http://fra.europa.eu/fraWebsite/attachments/Guide_ethnic_profiling.pdf

Fuchs, Christian, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", Privacy & Security Research Paper #1, PACT Project, Uppsala, 2012.

Fukuyama, F. (1995) *Trust: The Social Virtues and the Creation of Prosperity*, New York, NY: The Free Press.

Galetta Antonella, De Hert, Paul. (2012) 'Effects of surveillance on the rule of law, and on the presumption of innocence' IRISS Deliverable 1.1: Surveillance, Fighting crime and violence. http://irissproject.eu/wpcontent/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf

Galetta, Antonella (forthcoming, October 2013) 'The Changing Nature of the Presumption of Innocence in Today's Surveillance Societies: Rewrite Human Rights or Regulate the use of Surveillance Technologies?' in *European Journal of Law and Technology*.

Harcourt, B. (2006) *Profiling, Punishing, and Policing in an Actuarial Age* (Chicago Uni. Press)

Hardin (2002) *Trust and Trustworthiness*, New York, NY: Russell Sage Foundation.

Inglehart, R. (1999) "Trust, Well-being and Democracy." In Warren ed. *Democracy and Trust*, Cambridge: Cambridge University Press.

Jacobs, B. (2009) 'Keeping our Surveillance Society Nontotalitarian' Vol 1, No 4. .

Katholieke Hogeschool Zuid-West-Vlaanderen, Expertisecentrum Maatschappelijke Veiligheid for the Belgian Ministry of the Interior (Flemish version: June 2013). *Video surveillance in public spaces – is it really efficient?*

Kennedy R (1997) Race, law and suspicion. In: Race, crime and the law, Vintage Books, New York

Kimmelman, (2000) ‘‘The Promise and Perils of Criminal DNA Databanking’’ *Nature* 18(7), July

Lever A (2004) Why racial profiling is unjustified. Philosophy and Public Affairs 32(2)

Lyon D (1994) The electronic eye: The rise of surveillance society. University of Minnesota Press

Lyon, (2002) *Surveillance as Social Sorting. Privacy, Risk, and Automated Discrimination*

Luhmann, N. (1979) *Trust and Power*, Toronto: Wiley.

McCartney, C., (2006) “The DNA Expansion Programme and Criminal Investigations”, *British Journal of Criminology*, 46 (2)

McCulloch and Pickering (2009) ‘Pre-crime and Counter-terrorism: Imagining Future Crime in the ‘War on Terror ’ *British Journal of Criminology*

McLeod, Carolyn (2011) ‘Trust’ in *Stanford Encyclopaedia of Philosophy*.

Monahan T (2010) ‘Surveillance as governance: Social Inequality and the Pursuit of Democratic Surveillance’ in: Haggerty K and Samatas M (eds) *Surveillance and democracy*, Routledge

Nance DA (1994) ‘Civility and the Burden of Proof’. *Harvard Journal of Law and Public Policy* 17

Norris and. Armstrong, (1999) *The maximum surveillance society*.

O’Connor M, Rumann C (2003) ‘Into the fire: How to avoid getting burned by the same mistakes made fighting terrorism in Northern Ireland’. *Cardozo L Rev* 24:1657

Parmar A (2011) ‘Stop and search in London: Counter-terrorist or counter-productive?’ *Policing and Society* 21(4)

Pavone Vincenzo and Manuel Pereira ‘The privacy Vs security dilemma in a risk society: *Insights from the PRISE project on the public perception of new security technologies in Spain* (2008) At http://prise.oeaw.ac.at/docs/conf_docs/29/clubraum/Pavone-Privacy_vs_Security-20080429.pdf. Last Accessed 13.09.2013.

Privacy International, *PI Warns that New ISP Interception Plans Will Be Illegal*. November 26, 2009. https://www.privacyinternational.org/article/pi-warnsnew-isp-interception-plans-will-be-illegal

Ryberg, (2011) 'Racial Profiling and Criminal Justice' *Journal of Ethics* 15(1)

S and Marper v *United Kingdom* (2009) 48 EHRR 50

Schauer (1997) 'Generality and equality'. *Law and Philosophy* 16

Schneider P. (2013) 'DNA Databases' *Encyclopaedia of Forensic Sciences*

Sorell (2011) Preventive Policing, and European Counter-terrorism *Criminal Justice Ethics* 30(1)

Summary of the PACT Deliverables D1.1-D1.6. Research Paper Number #3. (2012) At http://www.projectpact.eu/documents-1/privacy-security-research-paper-series/%233_Privacy_and_Security_Research_Paper_Series.pdf. Last Accessed 18.09.13.

Ullmann-Margalit, E. (2002) 'Trust distrust and in between', in Hardin, R. (Ed.) *Distrust*. New York: Russell Sage Foundation.

Warren and Brandeis (1890) 'The Right to Privacy' Harvard Law Review, Vol. 4, No. 5

Westin (1967) Privacy and Freedom