

Philos. Technol. (2017) 30:39–54
DOI 10.1007/s13347-016-0218-2



RESEARCH ARTICLE

Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence

Katerina Hadjimatheou¹

Received: 31 October 2015 / Accepted: 7 April 2016 / Published online: 20 April 2016

© The Author(s) 2016. This article is published with open access at Springerlink.com

Abstract The potential of surveillance practices to undermine the presumption of innocence is a growing concern amongst critics of surveillance. This paper attempts to assess the impact of surveillance on the presumption of innocence. It defends an account of the presumption of innocence as a protection against wrongful criminalisation against alternatives, and considers both the ways in which surveillance might undermine that protection and the—hitherto overlooked—ways in which it might promote it. It draws on empirical work on the causes of erroneous convictions to suggest that surveillance can be used in ways that prevent innocent people being erroneously charged and convicted with crimes, by providing a source of exculpatory evidence for use in police investigations. It is argued that surveillance practices do not necessarily undermine the presumption of innocence but can be reformed in ways that both reduce the risk that they will cause wrongful criminalisation and increase their power to protect those already under suspicion.

Keywords Surveillance technologies · Presumption of innocence · Wrongful conviction · Trust · CCTV · ANPR · Police investigation

It is of paramount importance that law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science. Such real evidence has the inestimable value of cogency and objectivity. It is in large measure not affected by the subjective defects of other testimony. It enables the guilty to be detected *and the innocent to be rapidly eliminated from enquiries.*

– Lord Steyn [2004] UKHL 39

✉ Katerina Hadjimatheou
k.hadjimatheou@warwick.ac.uk

¹ Interdisciplinary Ethics Research Group, Department of Politics and International Studies, University of Warwick, Coventry, UK

The words of Lord Steyn draw our attention to something seldom acknowledged: that the use of evidence gathered by surveillance technologies can protect us against being wrongfully suspected or convicted of crimes. To the extent that his assertion is correct, it should lead us to revise our assessments of the costs and benefits of surveillance. In particular, it should lead us to recognise that, as well as increasing security, surveillance can be used in ways that protect important civil *liberties*—in this case, freedom from wrongful criminalisation.

Freedom from wrongful criminalisation has traditionally been protected via the legal principle of the presumption of innocence. This paper draws on recent empirical work on the causes and prevention of erroneous convictions to show how it may also be protected by the use of evidence gathered by surveillance technologies. The implications of this claim for overall assessments of the impact of surveillance on the presumption of innocence are considered in the light of recent attempts by surveillance scholars to demonstrate the corrosive effects of its use on that principle.

The paper proceeds as follows. First, current debates around the proper understanding of the presumption of innocence are outlined. Then, reasons are given in support of the account of the presumption of innocence as a principle protecting citizens against wrongful criminalisation by the state. This account is defended against alternatives, in particular those grounding the presumption in a right of citizens to be trusted. The claim that surveillance undermines the presumption of innocence is then assessed. Criticisms of surveillance that rest on assertions that it necessarily treats people as presumptively untrustworthy or criminal are rejected. It is argued that surveillance can be done in ways that do not undermine the presumption of innocence, and that mass surveillance is generally practiced in ways that are less undermining of the presumption of innocence than targeted surveillance.

The paper then draws on the results of recent empirical work on the causes of erroneous charges and convictions to illustrate that surveillance data can and should be used to protect the presumption of innocence, by providing evidence to exculpate those suspected of or charged with crimes. The final section of the paper considers the implications of what has been argued for our understanding of the impact of surveillance practices on the presumption of innocence. It argues that, despite the apparently contradictory impacts of surveillance on the presumption of innocence, measures designed to reduce the risk of the former need not inhibit the latter. On the contrary, a reduction in the use of surveillance that undermines the presumption of innocence is compatible with an increase in the use of surveillance that protects it.

1 The Presumption of Innocence in Debates About Surveillance

Privacy has traditionally been the core interest or 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 scholarly concern (Lyon 2002; Bou-Habib 2008; Ryberg 2011). Today, a new strand of critique focuses on the presumption of innocence, presenting it as the latest of our freedoms to become a casualty of surveillance practices (Minaj and Bonnici 2014; Galetta and de Hert 2012; Pavone and Pereira 2008).

Specific surveillance practices which have been criticised as undermining or curtailing the presumption of innocence include the mass monitoring of electronic

communications represented by the US National Security Agency's PRISM programme (EU Parliament 2013¹); retention of telecommunications data as prescribed by the EU Data Retention Directive² (Minaj and Bonnici 2014); the use of ANPR (license-plate recognition cameras) and open-street CCTV (Haggerty and Ericson 1997: 42; Monahan 2010:99; Galetta 2013: 280); and the use by telecommunications companies of deep packet inspection (DPI) techniques to detect illegal file sharing (Fuchs 2012: 50; Privacy International 2009).

Scholars identify a range of ways in which the presumption of innocence is apparently undermined by these practices. Some point to the stigmatising effects on those surveilled as criminal or potentially criminal (Campbell 2010). Others point to the implication of untrustworthiness visited on innocent individuals (Nance 1994; Duff 2013). Others still identify and object to the creation of an 'ethos' or 'culture' of suspicion (Kimmelman 2000; Minaj and Bonnici 2014) or to an 'erosion' of the trust that forms the basis of social relationships in a liberal society (Lyon 1994). These critiques all share an expansive interpretation of the presumption of innocence. They all argue that the presumption of innocence should not be understood merely in narrow legal terms, as a particular aspect of the right of defendants to a fair trial. Instead, they argue, it should also be understood as a general moral entitlement, part of which is protected via a legal right.

These reconceptualisations of the presumption of innocence have been criticised by legal theorists who worry about the unintended consequences of expansive interpretations. One major concern is that the normative clout of the presumption of innocence as a legal principle will be undermined by attempts to extend its protections from those at risk of the serious injustice of wrongful conviction to those at risk of, for example, the rather mundane intrusion of being subject to CCTV surveillance. It is not hard to see how this might occur. Currently, the presumption of innocence enjoys the legal status of a fundamental right and is thus treated as resistant to pressures from moderate increases in utility (e.g. in the number of guilty people convicted) that proposed restrictions to it may yield. But moderate increases in security may be thought quite reasonably to justify measures that risk visiting measures of suspicion such as increased CCTV surveillance or inclusion on police databases. Conflating the protection of the innocent from wrongful conviction with the protection of the innocent from suspicion or mistrust risks eroding commitments to the former in light of the relative triviality of the latter. Conversely, claims that surveillance undermines the presumption of innocence may well encourage, amongst those not versed in the details of the debate, the mistaken view that it actually results in greater numbers of miscarriages of justice, thus leading people to object to it with a force stronger than is properly merited.

Theorists who are moved by these concerns tend to favour limiting the scope of the presumption of innocence to the legal rules of trial, namely the rule that the burden of proof should be borne by the state. This limited presumption of innocence remains undiluted, thus retaining its moral and legal force and continuing to enjoy the status of a

¹ In 2013, the EU Parliament announced the launch of an inquiry into the compatibility of PRISM, declaring '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 the *Inquirer*, 9th July 2013).

² 'Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC'

fundamental right, which can only be restricted in exceptional circumstances. According to those who favour this approach, those concerned about stigmatisation or mistrust should stick to talking about stigmatisation and mistrust and any attempts of theirs to help themselves to the considerable rhetorical force of the presumption of innocence should be resisted.

Some of those who favour expansive readings of the presumption of innocence have attempted to meet these concerns by claiming that there is no single presumption but rather a range of presumptions, each of which protects people from different aspects of unfair coercion by the state in the name of criminal justice (Duff 2013). This move recasts the presumption of innocence as an umbrella principle, which includes protections against wrongful conviction alongside protections against wrongful mistrust or suspicion. The success of this move is questionable, though its conciliatory and inclusive spirit is welcome. This is partly because it deflects rather than addresses the problem of the normative status of the presumption: while before we were faced with the difficulty of agreeing about how important ‘the’ presumption is, we are now faced with the difficulty of deciding how important each presumption is and how they relate to each other.

Unfortunately, the proliferation of presumptions of innocence has not been accompanied by the kind of normative analysis that sets out the *importance* of the interests or values protected by each presumption and the *seriousness* of the apparent moral harm or wrong done to these by surveillance techniques. As a result, the multiple-presumptions approach invites normative paralysis if, upon examination, it turns out that surveillance practices undermine one presumption of innocence while at the same time protecting or promoting another.

The difficulties faced by the multiple presumptions approach could be avoided partially if we jettisoned the language of presumptions of innocence altogether and focussed instead on describing the specific burdens we want to highlight. It may be argued that these burdens—of stigmatisation, of privacy intrusions—are what make surveillance problematic, rather than the fact that they are called by a particular name. Yet neither is this move entirely satisfactory, for it denies the commonality between this particular class of burdens imposed by surveillance, a commonality which many identify intuitively with infringements or diminishment of the presumption of innocence and which undeniably resonates both within and beyond scholarship. What might this commonality consist in?

A recent stand of legal philosophy conceptualises the presumption of innocence as a protection against *wrongful criminalisation* (Tadros 2007; Tomlin 2013). This approach restricts the scope of the presumption to *criminal* justice, rather than (as we shall see with trust-based accounts) a basic principle of interpersonal morality that also happens to apply to state-citizen relations. Yet it also broadens the scope of the presumption of innocence beyond the confines of the trial to apply to all criminalising state practices, potentially including surveillance. This approach has a number of advantages that make it an attractive option. For example, it seems to capture and express well people’s core concerns about the impact on the presumption of innocence of contemporary surveillance practices: people invoke the presumption of innocence not merely because surveillance often involves paying attention to individuals in a way that interferes with, say, privacy but that it does so *in the name of an implied criminality* of some sort. It is this perceived criminalisation of those interfered with that both unites contemporary

objections to surveillance practices and makes them continuous conceptually with objections to wrongful conviction. In addition, accepting the wrongful criminalisation account enables us to move beyond debates about whether or not those objecting to surveillance can legitimately lay claim to the presumption of innocence in support of their cause: they can, if they can demonstrate that surveillance practices criminalise people unfairly.

This paper will endorse the wrongful criminalisation account of the presumption of innocence. But before it can do so, it must first defend that account against its most prominent current alternative, namely the trust-based account. In what follows I point out what I argue is a serious problem with that account and suggest that we should reject it. Many of the current criticisms of surveillance practices that appeal to the presumption of innocence speak of their inevitable negative impact on trust. My rejection of the trust-based account will also involve a rejection of some of these criticisms. I then apply the reasoning used to reject those criticisms of surveillance practices to the question of whether surveillance practices undermine the presumption of innocence by criminalising people wrongfully.

2 The Presumption of Innocence as a Right to be Trusted

As mentioned above, some legal theorists, notably Nance (1994) and Duff (2013), have attempted to recast the presumption of innocence as a moral right to be treated as trustworthy (for more recent proponents of this view, see Stewart 2014; DeAngelis 2014). 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. Nance argues that 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).

Building on Nance’s work, Antony Duff proposes grounding the presumption of innocence in the principle of civic trust. This principle is very similar to the principle of civility, but it includes a duty to treat people as if they will continue to act in accordance with their important obligations. This makes the principle of civic trust forward-looking, unlike the principle of civility, which is purely retrospective. According to Duff, failure to accord people appropriate civic trust is to fail 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, of which crimes are paradigmatic.

The claim that a failure to trust people equates to actively mistrusting them (DeAngelis 2014) is a persistent feature of accounts of the right to be trusted. Criticisms of surveillance often involve this claim, asserting that the fact that surveillance interferes in the absence of individualised suspicion means it subverts the presumption of innocence by presuming everyone to be guilty (understood as untrustworthy) until the

evidence it reveals proves otherwise. Thus, for example, 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]; see also Monahan 2010:99; Norris and Armstrong 1999:24). Mass or indiscriminate surveillance such as the use of open-street CCTV is also said to cast a shadow of mistrust or suspicion over populations (Minaj and Bonnici 2014: 421).

But the claim that failure to actively trust equates to active mistrust is a fallacy. It assumes, mistakenly, that trust and distrust are the only two trust-related attitudes it is possible to adopt. In fact, they exist at opposite ends of a spectrum of attitudes. As Ullmann-Margalit points out in her 2002 article on this issue, 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 reasonable and fair. Indeed, 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, as Duff and Nance do, implies that that is precisely what morality does require.

The nuanced view of trust elaborated by Ullman-Margalit is lent support by the work of social psychologist Toshio Yamagishi, whose seminal study distinguishes mistrust—that is, the assumption that someone cannot be trusted—from vigilance—that is, the prudent seeking of assurances in the absence of a prior basis on which to trust (Yamagishi 2011: 28). Yamagishi's work reflects better our psychological and social practices than assertions of a crude dichotomy between trust and mistrust. It can help us to distinguish between those practices of surveillance that communicate mistrust and those that should be interpreted as vigilance. Let us consider how.

Yamagishi's account of trust, mistrust, and vigilance can help us to provide a rationale for those surveillance practices that involve requiring people to prove their credentials in the advance of accessing certain goods or areas. One example is airport security practices. It would be wrong to claim that people are required to go through security checks at airports because there is an assumption that everyone who travels by air is suspicious or untrustworthy. Rather, such measures provide the necessary assurances people need in order for them to agree to engage in a potentially highly dangerous collective activity. Similar points can be made about surveillance that serves to protect the vulnerable from harm. As I have argued elsewhere, individuals who wish to work with children are not required to submit to criminal record checks on the ground that their desire to work with children makes them suspicious (Hadjimatheou 2014). Rather, such checks demonstrate a recognition that children are vulnerable and deserve special protection.

As this suggests, a belief in untrustworthiness is not necessarily the only or even the most rational explanation for these kinds of mass surveillance practices. The use of ID cards, CCTV, ANPR, data retention practices, and so on are compatible with the belief that the vast majority of people are well-intentioned, law-abiding citizens

who are of no interest to the criminal justice authorities. While it is true that they necessarily rest on an assumption that *some* criminal wrongdoing will be engaged in by someone, this merely reflects the facts. To assume otherwise would be not only irrational but a dereliction by states of the duty to protect individuals from crime. For this reason, it seems wrong to claim that such practices, merely in virtue of the fact that they involve some monitoring of the population, treat everyone as presumptively untrustworthy.

To push the point a bit further, let us imagine what a policy that *did* presume that all people are guilty of criminal transgressions would look like. Surely, it would look most like policies put in place to control inmates in a prison. Indeed, a presumption of guilt would support a policy of literally watching people all of the time and thus look similar to Bentham's infamous panopticon or Orwell's Big Brother, both of which were designed to control those already proven to be guilty and therefore presumptively untrustworthy. Most current uses by liberal democracies of surveillance by state security agents come nowhere near to being as comprehensive, intrusive, or communicative of mistrust as that. A great deal of information about us is indeed collected, but by a diverse range of separate agencies and for diverse reasons; there is no single consciousness, individual or corporate, that is aware of our every move. To be sure, police forces often express a desire to increase access to sources of information. But on-going debate about this issue in liberal parliaments and recent wranglings with technology companies illustrate that it is by no means inevitable that they will ever get it (The Guardian, 14 March 2016). The fact that most crimes not only go unsolved and unpunished, but are never brought to the attention of criminal justice agencies, further illustrates how far from Orwell's all-perceiving thought police we still are (UK Office for National Statistics 2013: 1–2).

Let us take stock for a moment of what has been argued and what we have learnt about the presumption of innocence and the effect of surveillance on it. In the preceding section, it was proposed that the wrongful criminalisation account of the presumption of innocence presented a sound basis for contemporary understanding of the principle. In this section, arguments have been put forward suggesting that its main rival interpretation, the trust-based account of the presumption of innocence, is unsound conceptually. From now onwards, the paper will proceed on the assumption that these arguments are correct and that the wrongful criminalisation account of the presumption of innocence should be embraced.

This section has also argued that, contrary to what is claimed by critics of surveillance who appeal to that account, mass surveillance practices do not necessarily treat people as presumptively untrustworthy. In the following section, I extend these latter arguments to the question of whether surveillance practices undermine the presumption of innocence by criminalising people wrongfully.

3 Surveillance and Wrongful Criminalisation

Wrongful criminalisation was defined above as treating someone as if they have a particular propensity towards criminality or indeed are already involved in criminal activity, without proper grounds for doing so. Wrongful criminalisation is at its worst when it results in the conviction of innocents, something that the legal right to be presumed innocent is designed to prevent (Stumer 2010), and at its mildest when it results in minor interferences with privacy. Whether or not something qualifies as

wrongful criminalisation will depend both on how we actually treat criminals and what counts as proper grounds for treating someone as criminal. In relation to the latter issue, we can say that proper grounds consist in evidence is reliable enough and that indicates criminality strongly enough to justify the particular preventive or punitive measure proposed. Thus, in Anglo-American jurisdictions, ‘reasonable suspicion’ might be the epistemic threshold for arrest, while ‘beyond a reasonable doubt’ is that for conviction. The question of whether surveillance practices wrongfully criminalise people will be answered by reference to these notions. Finally, in order to answer the question fully, we need to consider whether surveillance practices result in wrongful criminalisation necessarily or whether they can in principle be used without doing so.

Many of the claims just put forward in relation to the implications for trustworthiness of mass or indiscriminate surveillance practices apply to their implications for wrongful criminalisation. It is difficult for conceptual reasons to show that mass surveillance practices criminalise people wrongfully. Criminality is deviant or transgressive by definition, and (in liberal democracies at least) the belief that everyone is criminal would imply that the criminal law has failed to keep up with societal norms and should be reformed. Even in authoritarian, illiberal societies that practice highly intrusive forms of mass surveillance designed to deter and detect dissenters, it seems more accurate to describe such practices as implying that people are *enemies of the state* rather than criminals. There is something wrong with those practices, but it is debatable whether it is wrongful *criminalisation*. In any case, it seems reasonable to conclude that mass surveillance need not criminalise people wrongfully and therefore that it is not in principle incompatible with the presumption of innocence.

Things become more complicated when we consider surveillance practices that single out certain groups or individuals for monitoring or similar differential treatment. Any measure that distinguishes between people on grounds of suspected propensity for potential or actual criminality is criminalising to some degree. For example, racial and ethnic profiling by police has been strenuously objected to on the grounds that it criminalises not only the individuals it subjects to police interference but entire racial or ethnic groups (Lever 2007; Hadjimatheou 2012). In some cases, criminalisation occurs even if the measure is justified all things considered. For example, border officials may respond with surveillance to intelligence about a people trafficking ring operated by individuals from a certain ethnic background travelling between specific locations. The surveillance may be criminalising of people with that ethnic background, even if the victims that the policy is designed to protect share that background, but the criminalisation would not be wrongful if the evidence is reliable enough. We can conclude from this discussion that surveillance that targets groups or individuals is not inherently wrongfully criminalising but can be and indeed is used both in ways that criminalise wrongfully and in ways that do not.

It is not necessary for the purposes of this paper to try to determine which kinds of surveillance are more likely to criminalise wrongfully and therefore which can be said legitimately to undermine the presumption of innocence. The aim of the paper is to try to understand the impact on the presumption of innocence of surveillance practices in general and in light of the possibility that they can and are used in ways that protect people from wrongful charge and conviction. The first part of that project is now complete: surveillance practices can and do but need not be used in ways that undermine the presumption of innocence by treating people wrongfully as criminal. We can now turn to the second part of

the project which is concerned with developing a better understanding of how surveillance practices might prevent erroneous charge and convictions.

4 Reducing Erroneous Convictions: the Role of Evidence Gathered from Surveillance

This section proposes the following, unintuitive, and no doubt controversial thesis: surveillance practices can and to some extent already do protect innocent people from being erroneously charged and convicted with crimes and thus *promote* the presumption of innocence. They do so primarily by providing a source of data that can be used as evidence to rule out suspects from investigations and thus spare them the significant burdens of being charged or convicted with crimes they did not commit. This is achieved in three ways: first, by correcting tunnel vision in police investigations; second, by reducing the rate of false confessions; and third, by increasing exculpatory evidence available to the defence. Recent empirical work from the USA and UK on the causes of erroneous charge and conviction is drawn upon to develop these claims.

Social scientists are testing and substantiating theories about the causes of erroneous charge and conviction that are compelling and should influence the direction and focus of this debate over the impact of surveillance on the presumption of innocence. One such insight is that, contrary to what some legal theorists assume (Naughton 2007), erroneous convictions are not caused to any significant extent by the relaxation of rules of evidence, such as the admission of hearsay or bad character evidence (Gould et al. 2013). Rather, they are the result of one or more of the following factors: eyewitness misidentification, false confessions, poor defence and/or prosecution, and (much less significantly) error in the interpretation of forensic evidence (Ibid). All factors are both causes of and caused by the presence of ‘tunnel vision’ amongst police: that is, the common heuristics and logical fallacies that lead police to ‘focus on a suspect, select and filter the evidence that will “build a case” for conviction, while ignoring or suppressing evidence that points away from guilt’ (Martin 2002:847–848). As a result of this and other research, tunnel vision is now widely recognised to be a pivotal factor in erroneous conviction.

Tunnel vision tends to set in early in a criminal investigation. It is therefore unsurprising that the research also suggests that the causes of erroneous charges and convictions lie in errors that are most effectively corrected by measures taken in the relatively early stages of a case. Because research suggests that such errors become entrenched and amplified with each stage of the criminal justice process, relying on relatively late-stage court-room procedures to correct them is not the most effective strategy. Corrective interventions must be made much earlier and preferably before suspects are officially charged with criminal offences (Gould et al. 2013: 85).³

³ The results of this research complement recent, empirically informed normative work on systemic unfairness in the criminal justice system, which has been effective in highlighting the impact of crime-preventive surveillance practices by police on the outcomes of the criminal justice system. An excellent example is Bernard Harcourt’s work predicting the impact of racial profiling on highways by police on the relative crime rates of different ethnic groups as well as the overall rate of crime (Harcourt 2006). This strand of research is not directly relevant to the issue of wrongful criminalisation, but it draws attention to the fact that investigative choices about who to single out for and who to exclude from suspicion, even at a very preliminary stage of crime prevention, can have predictable, morally significant knock-on effects on the outcomes of criminal trials.

How might surveillance practices, such as open-street CCTV, ANPR, and DNA databases, play a part in the reduction of erroneous charge and conviction? There are at least three ways. First, evidence gathered via surveillance holds the potential to correct or obstruct the development of tunnel vision in police and thus to counteract what the research suggests is the single most significant factor in erroneous convictions. The most obvious way in which this might be done is by incorporating the collection of evidence from surveillance into measures designed to combat tunnel vision. For example, in countries such as Canada and the Netherlands, recent attempts to reform police investigatory practices in ways that counter tunnel vision include the appointment of ‘contrarians’ or devil’s advocates (Salet and Terpstra 2013). These are individual officers acting in an independent capacity, often brought in from an external force, whose role is to challenge investigative decisions with a view to preventing the development of biases or assumptions that risk influencing the direction of an investigation. It is unclear as yet how successful such initiatives have been but expectations are high (Ibid). Contrarians can and should point out to investigative officers where data gathered by surveillance technologies could provide evidence that might exculpate suspects and should therefore be collected.

Now, it may be argued that technology is a tool and that, no matter how reliable it is, it will not help improve criminal justice unless it is used properly. The example of contrarians just given lends support to this: it is the appointment of the contrarian that will make the real difference, not the availability of surveillance data. As long as the approach of a police unit to criminal investigation is geared to the confirmation of a hypothesis rather than the discovery of the truth, the technology will be used in the service of that purpose and the problem of tunnel vision will persist. Unless and until we change the mindset, it might be argued, talk of the potential of technologies is largely irrelevant.

While this argument has some merit, it is a little too quick. If used as a matter of routine, certain technologies *can* correct tunnel vision and thereby reduce the risk of wrongful conviction. The most obvious example is the use of DNA, fingerprinting, and other forensic techniques. The success of DNA testing in particular in the correction of miscarriages of justice is undeniable. When DNA evidence is available and reliable, it can provide the much-needed objectivity to cut through tunnel vision and protect innocent suspects from becoming defendants or even convicted criminals. Might some of the advantages of DNA evidence also be shared by evidence gathered by surveillance? There is reason to think it might.

Let us consider CCTV. The routine collection (but not examination of) footage collected by CCTV from around a crime scene could help to combat tunnel vision by providing exculpatory evidence. Though the UK is famous for being one of the most videoed countries in the world, most CCTV footage is deleted within 3 weeks of being recorded. Even assuming that investigating police decide they want to access the footage, it may have been deleted by the time they get around to it. In practice, police in the UK will often fail to access footage of a crime scene unless they need further evidence to recommend prosecution of the person they believe has committed the crime.⁴ Suspects in criminal cases are increasingly requesting access to such footage, which they claim will be exculpatory, and finding that it has been deleted.⁵ Retaining

⁴ Private conversation with police officer from London’s Metropolitan Police Service

⁵ Conversation with UK defence barrister Simon McKay

footage as a matter of course and analysing it at least in those cases in which it promises to reveal evidence material to the innocence or guilt of a suspect is one way in which evidence gathered from surveillance technologies could be used to reduce the risks of unjust convictions.

These points will gain force in the future as facial recognition techniques become more and more reliable. In the UK, the use of super-recognisers, that is individuals who are exceptionally good at identifying individuals from even quite poor-quality CCTV footage and photographs, is increasing in recent years, both in the pre-trial and in the trial phases of a criminal case. Super-recognisers are far more effective at identifying individuals from footage and images gathered from surveillance than any current facial-recognition technology on the market.⁶ At the time of writing, efforts are being made to develop certification for such individuals, which would establish their credentials as forensic experts in court. The use of super-recognisers in conjunction with CCTV footage could also reduce the reliance on line-ups and other opportunities for witness identification. The unreliability of witness identification is notorious, yet evidence shows that it is still relied upon by police and prosecutors, and thus continues to be a persistent factor in erroneous conviction (Gould et al. 2013: 95).

In the light of these developments, the requirement to gather CCTV footage from crime scenes may conceivably (and arguably should) acquire a legal status in the future. While police are required to reveal exculpatory evidence already in their possession, they are in most jurisdictions not required to gather it in the first place. UK regulation goes further than most countries in requiring police investigators by law to pursue all 'reasonable lines of inquiry'. As public knowledge of available sources of evidence grows, it is possible that police may find themselves the targets of legal action if, for example, those convicted of crimes claim the existence of potentially exonerating CCTV evidence that police could have but failed to retrieve. As MacFarlane (2008) notes, this route to legal challenge is not often of much use to defendants today because much hangs on what is 'reasonable' and because it relies on an after-the-fact challenge from the defendant, rather than building in safeguards from the start. Nevertheless, as digital evidence-gathering and analysis techniques become easier and cheaper, legal perceptions of what is reasonable may shift to incorporate routine gathering of evidence from surveillance.

Second, routine collection and retention of surveillance data relevant to a crime—such as CCTV footage, ANPR data, and communications metadata—can reduce the rate of false confessions by reassuring those accused that their innocence can be revealed. In the USA, one in four cases of exonerations via DNA evidence revealed wrongful conviction on the basis of a false confession.⁷ In the UK, recent psychological work shows that between 10 and 20 % of repeat criminals report having made false confessions (Gudjonsson 2011). One of the main causes is pressure or manipulation by police interrogators, and a compounding factor is the perception amongst suspects that their case will result inevitably in a guilty verdict. If such suspects knew their defence team would have access to all available data from their communications as well as

⁶ See 'The Police Super Recognisers Putting Names to Faces' Lauren Potts, *BBC News*, 19 Oct. 2015 at <http://www.bbc.co.uk/news/uk-england-34544199>.

⁷ See the USA's Innocence Project for explanation of the causes of false confession: <http://www.innocenceproject.org/causes-wrongful-conviction/false-confessions-or-admissions>.

open-street surveillance such as CCTV and ANPR, they may well be more confident about their chances of being found innocent and decide not to plead guilty.

Third, making surveillance evidence available to the legal teams of those accused can help them defend more successfully their clients, thus addressing another major factor in wrongful convictions. Writing in relation to the UK, Naughton describes how the current system puts the entire responsibility and indeed right to gather evidence on the shoulders of the police and prosecution and thus:

...renders suspects of crime passive, which simultaneously justified minimal resources to the defence, whilst the 'burden' places pressure on, and directs the bulk of the resources to, the police and prosecution to chip away at the presumed innocent stats and construct cases from only incriminating evidence that might obtain a conviction, rendering innocent victims vulnerable to wrongful convictions (Naughton 2011: 41).

Naughton proposes making evidence-gathering techniques available to defence teams as well as police and prosecutors (Ibid). Giving defendants automatic access to all the data that has recorded their own activities and has been retained already would go some way to empowering defendants to protect themselves against wrongful conviction.

Before we go on to consider the normative implications of the claims put forward in this section about the potential impact of surveillance evidence on the rate of wrongful charges and convictions, it is important to acknowledge that they are speculative. At the time of writing, no empirical study has yet been published examining the current and potential role of evidence gathered by surveillance in the ruling out of suspects from criminal investigations or even in their acquittal in trials. This should be contrasted with the considerable amount of work done that attempts to assess the impact of surveillance techniques and powers on the prevention, detection, and prosecution of crime.⁸ The disparity is explained by the fact that the democratic authorisation of such techniques and powers is justified by reference to their role as a means of increasing security against crime and not as a means of promoting the presumption of innocence.

One upshot of this is that it is difficult to assess the extent to which data that is already gathered for crime prevention and detection purposes could be put to use in ways that prevent quite serious kinds of erroneous criminalisation. For the purposes of this paper, however, it is sufficient to have shown that surveillance data has significant potential to be put to such use and that to some extent that is already occurring. It is worth noting, too, that erroneous charge and conviction are much more harmful to individuals than many of the most common kinds of interferences imposed via surveillance, such as for example being wrongfully singled out for a search at an airport. What are the implications of this conclusion for our assessment of the impact of surveillance practices on the presumption of innocence, given what has already been argued about their potential to undermine it by wrongfully criminalising some people?

⁸ For example, many studies have been undertaken around the world into the effectiveness of CCTV as a crime prevention and detection measure (Germain et al 2013).

5 The Normative Implications of the Impact of Surveillance on the Presumption of Innocence

If what has been argued thus far is correct, surveillance practices have the potential both to undermine the presumption of innocence, by wrongfully criminalising some via the imposition of suspicion, *and* to promote it, by protecting others from being erroneously charged or convicted. How should these conclusions determine our understanding of the impact of surveillance practices overall on the presumption of innocence? Is it possible to say that surveillance protects the presumption of innocence overall, because the criminalisation it has the potential to prevent (i.e. erroneous conviction) is more serious than that it inflicts (i.e. wrongful suspicion)? Or must we say that surveillance *both* undermines *and* protects the presumption of innocence?⁹

Neither solution is without its difficulties. On the one hand, the fact that the criminalisation of innocents *overall* might be reduced by surveillance practices does not mean we are justified in failing to acknowledge the wrongful criminalisation suffered by some. Yet at least this aggregative approach gives us a basis on which to make some assessment of the all-things-considered impact of those measures on the presumption of innocence, an assessment that can feed into decisions about the overall justifiability of such practices. On the other hand, the second option, which does not aggregate wrongful suspicion and erroneous conviction, seems to describe more accurately the impact of surveillance on the presumption of innocence. Yet, at first glance at least, it seems less helpful than the first, because it does not yield any clear overall assessment that can inform broader policy considerations.

Notwithstanding these considerations, there is at least one compelling reason why we should prefer the second, non-aggregative option above the first. The aggregative option is the kind of crude aggregative utilitarian approach to determining interference with the presumption of innocence, which would weigh the wrongful suspicion inflicted by surveillance against the erroneous charge and conviction prevented. This utilitarian reasoning would also take into account the fact that erroneous charge and conviction involves harm to interests that are *more vital* to people's well-being than those affected by wrongful suspicion, and conclude therefore that the prevention of the former outweighs the prevention of the latter.

This approach would not be accepted by theorists of a deontological persuasion as a valid basis for assessment, as it assumes that unfairnesses to some can be justified by reference to the benefits gained by others. The opposition to such trade-offs could not be more formidable. Two of the twentieth century's most important political philosophers, Rawls and Nozick, have argued that trade-offs between individuals are incompatible with respect for people, because it fails to recognise what has become known as the 'separateness of persons'. In the words of Nozick: 'To use a person [for another's benefit] does not sufficiently respect and take account of the fact that he is a separate person, that his is the only life he has. He does not get some overbalancing good from his sacrifice' (Nozick 1974: 33.). Not everyone would agree that this objection is fatal, but it is serious enough to suggest that an alternative to the utilitarian approach should be explored.

⁹ The choice between these two options is not a choice between two normative implications but a choice between two ways of *conceptualising* the impact.

One possible alternative is suggested by considering a further objection to the aggregative utilitarian position: that objection from what has become known as the ‘doctrine of acts and omissions’. The doctrine of acts and omissions states that it is worse to inflict harm than to fail to intervene to prevent it. Though support for this doctrine is waning in moral philosophy, it still features regularly in moral arguments, in part at least because there is a clear sense in which it chimes with common sense moral intuitions.¹⁰ Philosophical proponents of this position assert that the state’s duty to refrain from harming innocents must take priority over its duty to prevent harm inflicted on innocents by others (Kagan 1992). Applied to the issue at hand, it would suggest that wrongful suspicion caused by surveillance is a harm against innocents and should therefore be avoided *even if the practices that cause it also prevent erroneous conviction*. In other words, the doctrine of acts and omissions yields a clear argument for states to refrain from surveillance when and to the extent that it visits on innocent individuals’ wrongful criminalisation in any of its forms. If this argument were accepted, it seems we may have sufficient grounds not only to reject the aggregative utilitarian approach to assessing the impact of surveillance on the presumption of innocence but also to resolve the apparent dilemma posed by the non-aggregative approach: if we are prohibited from inflicting wrongful criminalisation of any kind, then we are prohibited from carrying out many of those very surveillance practices that might also help prevent erroneous convictions.

However, there are strong reasons to reject this line of argument, reasons that could be accepted even by those whose intuitions insist on some distinction between acts and omissions. Let us consider two such reasons. First, the doctrine of acts and omissions can be interpreted more flexibly than it has been presented above. Therefore, it need not be taken to mean that inflicting harm is *always* worse than failing to intervene to prevent it, a principle which seems implausible. If using evidence gathered from surveillance can prevent a *great amount* of criminal harm by inflicting on innocents a *very small* rise in the numbers of people being treated as criminally suspicious, it may be reconcilable with some more moderate version of the distinction between acts and omissions.

Second, and more importantly, in relation to surveillance practices, the objection to the aggregative approach offered by an appeal to the doctrine of acts and omissions assumes a conflict in practice between the imperative to refrain from wrongful criminalisation and the duty to prevent erroneous conviction. In fact, there is no such conflict. The tendency of surveillance practices to inflict wrongful suspicion on some innocents can be reduced *without at the same time reducing the potential of those practices to be used in ways that protect individuals from erroneous charge and conviction*. This is the case because, as was argued before, surveillance need not (although it has been in practice) be used in ways that undermine the presumption of innocence by imposing suspicion on people and thus criminalising them, wrongfully. The adjustments that would need to be made to avoid such wrongful criminalisation do not prejudice in any way the availability of the kind of data that could be used to exculpate or otherwise rule out of suspicion those already subject to police investigation. In other words, it is possible to practice surveillance in such a way as to reduce the number of individuals wrongfully criminalised at the low end of the spectrum of

¹⁰ Teson (2005) offers one of the few well-thought out contemporary defences of the principle.

suspicion, while at the same time increasing the protection for those at risk of much more serious criminalisation.

Therefore, the second non-aggregative option put forward above, namely to try to recognise both the ways in which surveillance undermines and the ways in which it protects the presumption of innocence, need not lead to normative paralysis. Instead, combined with the claims made above about the actual and potential impact of surveillance practices on wrongful suspicion and erroneous conviction, it yields a clear take-home message, namely that we should adapt state use of surveillance so that the former is reduced and the latter strengthened.

Too often criticisms of surveillance consist of lists of the various ways in which it undermines our most treasured and fundamental values. Rarely are systematic attempts made to reflect upon the potential benefits to such values, especially those other than security. This paper has attempted to go some way towards rectifying this and to reflect on the normative implications of its analysis in a way that supports clear recommendations for action.

Acknowledgments This work was supported by the European Commission's Seventh Framework Programme Security Research Fund, under the 2012-15 SURVEILLE project (Surveillance: Ethics, Human Rights and Efficiency) [Grant number 284725].

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

- Bou-Habib, R. (2008). Security, profiling and equality. *Ethical Theory and Moral Practice*, 11(2).
- Campbell L. (2010). A rights-based analysis of DNA retention: "non-conviction" databases and the liberal state. *Criminal Law Review*.
- DeAngelis, P. (2014). Racial profiling and the presumption of innocence. *Netherlands Journal of Legal Philosophy*, 2014(1).
- Duff, A. (2013). Who must presume whom to be innocent of what? *Netherlands Journal of Legal Philosophy*, 42(3).
- Fuchs, C. (2012). 'Implications of deep packet inspection (DPI) internet surveillance for society'. At <http://www.projectpact.eu/documents-1>.
- Galetta, A. (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*.
- Galetta A, De Hert, P. (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_DI_MASTER_DOCUMENT_17Dec20121.pdf.
- Germain et al. (2013). A prosperous "business": the success of CCTV through the eyes of international literature. *Surveillance and Society*, 11(1/2).
- Gould et al. (2013). Predicting erroneous convictions: a social science approach to miscarriages of justice. USA Department of Justice Report. AT <https://www.ncjrs.gov/pdffiles1/nij/grants/241389.pdf>.
- Gudjonsson, G. (2011). Suspect interviews and false confessions. *Current Directions in Psychological Science*, 20(1), 33–37.
- Hadjimatheou, K. (2012) 'Moral Risks of Profiling in Counter-Terrorism' research paper for the EU-funded FP7 Security project DETECTOR (Detection Technologies, Terrorism, Ethics and Human Rights). At <http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiKq2prMrLahWJwxQKHSt1BS0QFgggMAA&url=http%3A%2F%2Fwww.detector.bham>.

- ac.uk%2Fpdfs%2FD5_4_Moral_Risks_of_Profiling_in_Counter-Terrorism.doc&usg=AFQjCNGXIA9XDd5YA-1ldeqPiW58hVquEg. Last Accessed 19.03.16.
- Hadjimatheou, K. (2014). The relative moral risks of targeted and untargeted surveillance. *Ethical Theory and Moral Practice*, 17, 187–207.
- Haggerty and Ericson. (1997) *Policing the Risk Society*. Clarendon Studies in Criminology, Oxford: Clarendon
- Harcourt, B. (2006). *Against prediction: profiling, policing, and punishing in an actuarial age*. Chicago: University of Chicago Press.
- House of Lords Constitution Committee, (2009). ‘Surveillance: Citizens and the State’. 2nd Report of Session 2008-09, 2.
- Inquirer. (2013). European Parliament votes for PRISM snooping investigation. At <http://www.theinquirer.net/inquirer/news/2280187/european-parliament-votes-for-prism-snooping-investigation>.
- Jarvis-Thomson, J. (1975). ‘The right to privacy’. *Philosophy and Public Affairs*, 4(4), 295–314.
- Kagan, S. (1992). *The limits of morality*. Oxford: Clarendon.
- Kimmelman, G. (2000). The promise and perils of criminal DNA databanking. *Nature*, 18(7).
- Lever, A. (2007). What's wrong with racial profiling? Another look at the problem. *Criminal Justice Ethics*, 26(1) 20–28.
- Lyon, D. (1994). *The electronic eye: the rise of surveillance society*. University of Minnesota Press.
- Lyon, D. (2002). *Surveillance as social sorting. Privacy, risk, and automated discrimination*.
- MacFarlane, B. (2008). ‘Wrongful convictions: the effect of tunnel vision and predisposing circumstances in the criminal justice system’, prepared for the Inquiry into Pediatric Forensic Pathology in Ontario, The Honourable Stephen T. Goudge, Commissioner. Downloadable at https://www.attorneygeneral.jus.gov.on.ca/inquiries/goudge/policy_research/pdf/Macfarlane_Wrongful-Convictions.pdf.
- Martin, D. (2002). Lessons about justice from the laboratory of wrongful convictions: tunnel vision, the construction of guilt, and informer evidence. 70 *UMKC L Rev.*, 847.
- Minaj, J., & Bonnici, J. (2014). Unwitting subjects of surveillance and the presumption of innocence. *Computer Security and Law Review*, 30(4).
- Monahan, T. (2010). Surveillance as governance: social inequality and the pursuit of democratic surveillance. In K. Haggerty and M. Samatas (eds.), *Surveillance and democracy*. Routledge.
- Nance, DA. (1994). Civility and the burden of proof. *Harvard Journal of Law and Public Policy*, 17.
- Naughton, M. (2007). Rethinking miscarriages of justice: beyond the tip of the iceberg. Basingstoke: Palgrave Macmillan.
- Naughton, M. (2011). How the presumption of innocence renders the innocent vulnerable to wrongful conviction. *Irish Journal of Legal Studies*, 2(1).
- Norris, C., & Armstrong, G. (1999). *The maximum surveillance society*.
- Nozick, R. (1974). *Anarchy, State, Utopia*, New York: Basic Books.
- Pavone, V., & Pereira, M. (2008). The privacy vs security dilemma in a risk society: insights from the PRISE project on the public perception of new security technologies in Spain. 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, J. (2011). Racial profiling and criminal justice. *Journal of Ethics*, 15(1)
- Salet, R., & Terpstra, J. B. (2013). Critical review in criminal investigation: evaluation of a measure to prevent tunnel vision. *Policing*, 8(1), 43–50.
- Stewart, G. (2014). The right to be presumed innocent. *Criminal Law and Philosophy*, 8(2).
- Stumer, A. (2010). *The presumption of innocence*. Oxford.
- Tadros, V. (2007). ‘Rethinking the presumption of innocence’. *Criminal Law and Philosophy*, 1(2), 193–213
- Teson (2005). Liberal security. In *Human rights in the age of terror*. Cambridge: Cambridge University Press.
- The Guardian, 14th March 2016. ‘Facebook, Google and WhatsApp plan to increase encryption of user data’. At: <http://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increase-encryption-fbi-apple>. Last accessed 16.03.16.
- Tomlin. (2013). The golden thread? Criminalisation and the presumption of innocence. *Journal of Political Philosophy*.
- UK Office for National Statistics (2013). Crime in England and Wales, statistical bulletin. At <http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-june-2014/info-what-does-csew-cover.html>. Last Accessed 16/03/16.
- Ullmann-Margalit, E. (2002). ‘Trust out of distrust’. *Journal of Philosophy*, 99(10) 532–548.
- Warren and Brandeis (1890). The right to privacy. *Harvard Law Review*, 4(5)
- Westin, A. (1967). *Privacy and freedom*. New York: Athenaeum.
- Yamagishi, T. (2011). *Trust: the evolutionary game of mind and society*. Springer.