

Research Bank

Journal article

Body-worn POV technology : Moral harm

Harfield, Clive Geoffrey

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

A point of view: Some ethical considerations arising from the use of body-worn video technology

Clive Harfield MSc LLM MA MPhil PhD
Adjunct Fellow, Griffith University, Qld, Australia
Associate Investigator, ARC Centre of Excellence in Policing & Security ¹

Unless explicitly consented to by the subject, the image-taking (and by extension, the videoing or audio recording) of an individual is a moral intrusion against personal privacy: a moral wrong for which an over-riding claim of justification must be established if the image-taking is to take place without the subject's explicit consent. ² Why should this be so?

In order to attain the moral good of self-fulfilment an individual is entitled to act in their self-interest to the extent that in doing so they do not cause unjustifiable moral or unjustifiable material harm to others. All things being equal, there should be no interference with the pursuit of individual self-interest so long as that pursuit does not unjustifiably harm others. Self-interest can include the desire to remain unnoticed by others, although this is constrained when the conduct of the individual concerned justifiably warrants the concern of others. When a user of body-worn video (BWV) technology engages or interacts with an individual who wishes to remain unnoticed (which includes the wish not to be photographed, videoed or audio-recorded), the latter's moral interests in privacy are engaged.

Privacy has two aspects: the abstract conception of privacy as exercised through control over information about self, and the physical conception of private space including the extent to which an individual can expect to be private in a public space.

Privacy is grounded on individual autonomy. Where autonomy does not exist (due to mental incapacity through youth or medical circumstance, for instance), there remain two further foundations: respect for human dignity; and the "pragmatic imperative of limiting abuses of official power". [6] Each of these conceptions has its own relevance in relation to image-taking.

Autonomy includes having control over how much information about oneself is disclosed to (and therefore available for use by) others. Discretionary disclosure - choosing to share information or choosing not to share it - enables individuals to manage relationships with others.[5] Taking images of an individual is a means of capturing information about them which could then be used to control or coerce that individual.³[8] "The power to exclude, delete or misrepresent an event is with the

wearer not the passive passer-by” creating an asymmetry of power between the image-taker and the image subject.[2] If an individual has no control over when and how information about them is gathered and used, their autonomy is compromised and so their privacy intruded upon: the unjustifiable compromise of autonomy is morally wrong.

Personal privacy is infringed when the taking of the image fails to respect the dignity of the subject. Controversy remains as to whether press photographers should have photographed Diana, Princess of Wales, as she lay fatally injured in the wreckage of a car crash. It is not obvious that the newsworthiness of the event (which could have been accurately reported without being photographed but which also distinguished her from any other car crash victim) justified photographing Diana at her most vulnerable and helpless, unable to exercise autonomy. Did broadcasters and newspaper editors have a moral justification for publication of the images that was stronger (in this case) than the moral interest in preserving respect for human dignity, particularly the moral imperative of dying with dignity? (To the extent that the images were taken because they would become valuable commercial commodities for the image-takers, to be sold to the highest bidder, the dying woman was commodified thus compounding the indignity.) However, where an individual draws attention to themselves through their own undignified conduct (or deliberate publicity-seeking) and the conduct happens to be photographed or filmed, then the subsequent harm to the subject’s dignity, and any diminution of respect for that person, is a consequence of their conduct rather than of the image being taken.

Government capacity for collating information about citizens and non-citizens, through surveillance and biometric identification technology, has increased exponentially through digital data technology. Wireless technology has removed the physical limitations that once constrained government surveillance capability and capacity.[1] Through its authority and its access to resources, a government has real power to take images not only in its direct interactions with citizens (e.g. documenting an arrested person in the police station) but also indirectly as citizens go about their daily lives (e.g. via CCTV systems in public places). Statutes defining when governments may lawfully capture images regulate the *de facto* power by defining a *de jure* (or official) power. Official power lawfully exercised grounds subsequent claims for moral justification when governments capture images without subject consent. Where images are captured by state agents outside lawful parameters, and/or in ways that intentionally or unwittingly evade proper accountability, then government power has been abused and the privacy of the image subject unjustifiably infringed: a moral wrong has been committed.

Further: miniaturization and economies of scale mean that embedded sensor technologies capable of image or audio capture, once the costly preserve of government agencies, may now be possessed by individuals: may be worn as simply, unobtrusively and as forgettably as a pair of spectacles or a lapel pin.

This, all be it briefly, establishes the connection between image-taking and conceptions underpinning personal privacy.

Location and privacy

Whether there exists a justifiable expectation of privacy or merely an entitlement to anonymity, and whether either of these may be justifiably over-ridden, varies according to location. Basic moral objections to non-consensual image-taking are strongly reinforced when it is proposed to take non-consensual images in certain types of location. There must be a correspondingly stronger counter-justification for taking images in such circumstances.

Spaces may be broadly divided into three categories of access: private; restricted; and public. This landscape is complex. Any given space may exhibit more than one access category. Whilst inside a residential house is private the driveway is considered as allowing restricted access to cater for legitimate callers such as postal workers delivering mail. Only employees may enter certain areas of work premises yet there may also be public access areas for customers. Roads and open civic areas fall within the category of public access. Anyone entitled to be at large may enter such areas. The more restricted the level of access, the greater the expectation of privacy amongst those entitled to access, the greater must be any moral justification for non-consensual image-taking.

Because an individual in a public space is liable to be casually observed by others occupying or passing through the same space there can be no reasonable expectation of being entirely private when in a public space. It does not follow from this that individuals are entitled to know the business of anyone they encounter or pass by in a public space. That an individual is there is undeniable through simple observation.⁴ But who that person is and why they are there remains their own business to the extent that they do not draw public attention to themselves. (The content of an intimate conversation is no less private because the interlocutors are walking in the public park.)

Individuals are entitled at least to anonymity in public spaces. Three conventions underpin this: that in a public space an individual should be subject to momentary and casual observation only; that the

observer should be observable; and that closer scrutiny by others is only warranted where the subject of the scrutiny draws attention to themselves “by manifestly aberrant behaviour”, or through deliberate publicity seeking.[9] Casual observation means being seen but not noticed. To take notice is to start gathering information. When an individual is not noticed, then casual observation causes no moral harm because no information has been gathered without consent and so their autonomy has not been infringed.

What are the implications of this space categorization for morally justifiable image-taking? Whether an individual is located within a private space, a restricted space or a public space refines the moral considerations based on the basic principles above. The basic moral presumption is that an individual is entitled not to be filmed or photographed without their explicit consent. This presumption is more stringent if that individual is located within their residence, a private space. At work individuals may be subject to workplace camera surveillance conducted by their employer. If such image-taking is to ensure compliance with occupational health and safety regulations, the wider benefits of such compliance (and it being enforced) over-ride the basic presumption against non-consensual image-taking of individuals, particularly where all staff are equally subject of such surveillance and no one is discriminated against.⁵ Individuals travelling through public spaces, commuting between home and the workplace, pass through spaces monitored by CCTV systems, both publicly and privately managed. To the extent that such surveillance is momentary, the surveillance mechanisms are clearly observable by the surveillance subject, and that the individual, whilst passing through the surveillance arena, will not be subject to more intense scrutiny or attempted identification unless they draw attention to themselves through their aberrant behaviour or deliberate publicity-seeking, then the individual has no more grounds for moral objection to such surveillance than they would to being casually observed by another commuter coincidentally passing through the same public space.

Such camera surveillance will not be momentary if the images are recorded either for routine analysis or for reactive analysis prompted by some trigger event. The purpose may be to identify persons passing through a public space, for instance if camera surveillance is linked to Automatic Number-Plate Recognition software and a vehicle registration database or to facial recognition software and a nominal database.⁶ In these circumstances Von Hirsch’s three-part test is failed at the first hurdle.

The moral significance of image use

The moral significance of the use to which images of individuals are put rests upon the extent to which the image subject has control over use of an image and information derived from it. Where the subject has little or no control (no opportunity to correct or contextualize the image-based information for instance), then the moral justification relied upon by the image-user must be sufficient to over-ride the basic presumption that individuals have a moral right to control such information as an exercise of their autonomy.

Where disadvantage is caused to the image-subject then the image-taking (or recording) and the use made of the image (or recording) each are independently morally objectionable on the basis that no one should suffer deliberate disadvantage at the hands of another: a moral harm additional to the intrusion of privacy and infringement of autonomy.

Weightier moral issues can override such objections. For example, image-taking as part of a police investigation may produce information leading to the arrest, prosecution, conviction and punishment of the surveillance subject. These disadvantages to the suspected individual are outweighed by community interests in securing safety through an effective criminal justice system. Such image-taking can therefore be justified within the moral theory of policing proposed by Miller and Blackler.[4] Community interests in an effective criminal justice system also justifies, from a non-authority perspective, citizens taking non-consensual images of police officers committing wrongdoing such as using unwarranted and excessive force, if such surveillance was intended to be used as a means of holding that officer properly to account for the excessive force.

Other circumstances are intuitively immoral and beyond justification. Where images are taken for blackmail purposes, then the advantage to the image-taker has no moral standing that outweighs the moral harm of the disadvantage to the image subject. Indeed, the immorality of the purpose compounds the disadvantage and the moral harm. The fact that the image subject, in acquiescing to the blackmail and meeting the demands, regains control over the images does not negate the original moral wrong. Such circumstances are not an exercise of full autonomy because the subject is under coercion and there is no choice of meaningful options available to the subject.

Between these two extremes lie scenarios less clear cut. For example, where there is no active and specific investigation in progress, are police nevertheless entitled to take images as part of their general peace-preservation function (perhaps in lieu of, or to maximise efficient use of, patrolling police officers)? In such circumstances police as image-takers would be looking for aberrant behaviour, a departure from normal patterns that warrants further scrutiny. Continuous scanning of

a population passing through a public space can constitute casual observation. The composition of the scanned population changes as different individuals enter and depart the surveillance arena. If no information is recorded about such individuals, this monitoring observation to detect aberrant behaviour equates to casual observation, albeit that it is still observation conducted for a purpose. If, on the other hand, such image-taking is retained for any period in order to distinguish the aberrant from the normal (retrospectively if necessary) then this is more than casual observation. Information is being stored and used.

Is the observer truly observable in such circumstances? CCTV cameras can be unobtrusive in design and location: discreet if not actually covert. Signage advertising the presence of CCTV may lack information about who is monitoring the images and whether the images are being recorded. And like the small-print in a contract, signs may meet regulatory requirement without being attention-catching: just so much street wallpaper.

If no aberrant behaviour is observed demanding immediate investigation, justification for retaining the images weakens and retention begins to look like the abuse of power. Privacy and the entitlement to be anonymous in public seem more substantial claims in such circumstances than the moral theory of policing. In the absence of an incident requiring specific recourse to coercive or otherwise morally harmful action, relying on the moral theory of policing as the basis for justification seems to be a claim of “just-in-case”, rather than a claim grounded in intervention against a specific harm.

A second less than clear-cut scenario falls within the emerging construction of surveillance not as social control by state agents but as seeing; as a form of social practice undertaken by individual citizens. Is any moral harm incurred by the individual subject of an image taken by a citizen rather than a state agent? If the image is taken without the subject’s consent then there has been, *prima facie*, an intrusion of privacy. But the significance of the moral harm caused will be determined by the consequences arising from the image having been taken. If I take a photograph of a public place in which strangers happen to be standing at the time I take the photograph, those individuals will be captured on the image (just as if they had passed through my field of casual observation had I viewed the scene without a camera). If all I do with the image is print the photograph and paste it in an album of keepsakes to which I occasionally refer for private pleasure, then it seems that no significant adverse consequence has arisen to any persons who happen to be captured in that image. Their anonymity remains - I do not and have no wish to identify them - and their privacy (founded on autonomy) has only momentarily been intruded upon.⁷ Had they noticed me taking the photograph it would have been open to them to raise objection with me at the time. If they do not do so, then I

may infer the individual's implicit consent (or at least absence of objection) to being photographed, in which case no moral objection on the basis of privacy intrusion arises. Even if they have not noticed me, I have still committed a prima facie intrusion.

But suppose I upload the image to internet blog-pages. In both circumstances I have taken the image as a recollection of what I saw at the time, there is no difference in my primary purpose for *taking* the image. But the *use* to which I put the image is significantly different. Via the blog anyone with internet capability can access the image. The intrusion into the privacy of those persons caught in the image is more significant because not only have I infringed their autonomy (and so intruded their privacy) but so too will *anyone else* who looks at the image. The persons captured in the image have no control over my use of the image or its information. Neither they nor I have any control over the copying and subsequent re-use and analysis of the image and its information by anyone who views it on the blog-pages. By uploading the image I have exposed the image-subjects to a vulnerability of moral (and potential actual) harm of greater significance than if I had pasted printed photographs into a private album.

The morally-relevant characteristic of the image-taker

The third specific variable is the morally-relevant characteristic of the image-taker. This is related to, but remains distinct from, the use to which image information is put.

To take a familiar example: a police officer, when acting as such, does so under the authority of the position he or she holds. All things being equal, to the extent that the officer fulfils his or her proper duties in the proper manner and according to (morally sound) law, then proportionate and necessary acts necessary to achieve this, although otherwise morally harmful, will be justified within the moral theory of policing. This includes taking and/or using images without the consent of the image-subject where it is necessary to achieve (and in the circumstances is the only means of achieving) the proper purpose of policing. (To the extent that other public servants are called upon to take images or make recordings pursuant to their lawful roles, the same principles seem to apply.)

Individual citizens taking images of others without the explicit consent of those others cannot call upon the authority or purpose of state agency as a justification that overrides the prima facie intrusion. What alternative claims are available to them?

A claim of civic duty justification presents itself in two forms, the stronger of which is the evidential claim. In the notorious cases of Rodney King and Oscar Grant the images of police using force against

King and Grant were taken by citizens (without the consent of anyone they were imaging) and used as evidence in prosecutions: consistent with the moral theory of policing even though the image-takers were not police officers.

A second civic duty claim (arguably weaker because it does not concern evidence used in the prosecution of serious crime) is that citizens are justified in filming/photographing police officers as the latter go about their duties in any case. This claim rests on the public accountability of the police. In this way the power of surveillance as a mechanism of state social control (police using exclusive official powers) is counter-balanced by sousveillance as a form of social control of the state (police being held to account by the policed).

Civic duty also overrides any intrusion harms where citizens record other citizens committing crime with the intention of passing the images to the police as evidence. But where individuals take images of other individuals with the intent of pasting the photographs in an album there seems to be no obvious justification that overrides the prima facie moral harm of intrusion. The consequences arising from the intrusion may not be very significant, but for their own pleasure the image-taker has taken an image of another individual without the latter's consent and, minimal though the actual harm might be, the pleasure has been derived at moral cost to another without any obvious overriding justification.

Where such images are published in publicly-accessible media, both the moral harm and the potential actual harm are more significant. Publishing engages (from the perspective of the image-taker) issues of free speech and of copyright, two areas of law much challenged in a media environment becoming dominated by wireless connectivity. No attempt is made here to analyse these two areas in detail suffice it to say that to overcome moral objections on the basis of privacy intrusion, the counter-claim must have a strong basis in the wider public interest. The image-taker, lacking alternative authority, must rely upon the legitimate community interest in publication of the images outweighing the image-subject's moral objections.

The morally-relevant characteristic of the image subject

The final specific variable is the image-subject. As the significant characteristic of the image-taker is the authority (official and/or moral) on which the image-taker may take an image, so the significant characteristic of the image subject is the obverse of authority: consent. Consent can either be explicitly granted/denied or implicitly granted/denied. Where the image subject explicitly consents

both to the taking of the image and the subsequent use of the image, then consent in these circumstances negates any moral objection. Where the image-subject explicitly objects to the image being taken, or to its subsequent use, then acting against the image-subject's wishes will be a moral wrong because the latter's privacy has been intruded upon and autonomy infringed. In such circumstances image-takers need a claim to moral justification that outweighs the prima facie harm.

Certain categories of person are not competent to grant consent. These include the young (because they are insufficiently mature in their reasoning) and those persons temporarily or permanently incapacitated in their mental faculties. It follows that such individuals cannot properly give consent either to being imaged or to any use to which the image-taker wishes to put the image.

Where an individual is competent to grant/deny consent, a number of additional questions arise in calculating the potential extent of moral harm occasioned by non-consensual image-taking.

Has the image subject had the opportunity to grant/deny consent? Clearly, if the images are taken without the image-subject's knowledge then there has been no opportunity to grant/deny consent. The image-taker must have a strong over-riding moral claim to justify not seeking the consent of the subject, as well a claim for taking the images without consent. Both of these conditions apply – it is not a case of either or – and if either does not, then the image-taker ought to be able to accommodate requests for deletion made by the image-subject, in ways identical or similar to those employed by Steve Mann.⁸

An individual entering a CCTV-monitored public area could be inferred as implicitly consenting to surveillance. But three issues arise: whether the image-subject is aware that he or she is in an area being monitored by CCTV; whether or not the image-subject knows who is monitoring the CCTV; and whether or not the image-subject knows to what purpose the images will be put. Implicit consent cannot reasonably be inferred, nor any justification it might offer relied upon, unless it is clear that persons in the surveillance arena are there because they know all three facts and have chosen to enter the surveillance arena on this informed basis. Nor is it necessarily obvious what is being consented to even if implicit consent can properly be inferred: the taking of the image or making of a recording; the storing of the image or a recording; the sharing of the image or a recording with others; the secondary use(s) to which those others might put the image or recording; all of these together or any permutation? Unless the image-subject and the image-takers or record-makers are clearly agreed with each other on the answers to all these questions (and the secondary use by others with whom the image is shared might not be foreseeable in any case), implicit consent seems to offer imprecise and therefore uncertain grounds for moral justification.

What the images (or recordings) are to be used for and how the information captured by the image (or recordings) will be used runs to the heart of consent: does the image-subject have sufficient information about the use to which the image will be put in order to grant/deny consent on an informed basis? The image subject may have little or no control over how images are initially used and may never be aware of any secondary purpose to which an image might be put. Once the images have been shared beyond the image-taking agency (police CCTV-footage used for reality TV shows for example), the subject has little or no realistic control over how they (or the information the images contain) might be used.

Where the images have been taken by a private individual, the extent to which the subject has control over the subsequent use of the images depends on the subject's relationship with the image-taker and anyone who subsequently holds the images. The subject may not know the image-taker at all. If the image is shared on social-networking media, neither the subject nor the image-taker may have any meaningful relationship with anyone holding the image. The absence of such a relationship means the image-subject has no reasonable means of contacting an image-holder to discover their intentions and either consent or object to them. Distribution of images in a manner that denies the image-subject control over the ways in which an image of them (and the information it contains) is used is a moral harm because the image-subject's autonomy is infringed. To the prima facie moral harm is added the harm of impotent redress.

BWV ethics in practice

BWV technology has changed the camera surveillance dynamic. Does this present new ethical challenges or simply reconfigure current ethical challenges? How might the theoretical issues discussed above play out for real?

The fact that camera surveillance equipment can be easily worn and that improved battery technology enables such equipment to be used for an entire patrol shift, has extended the ways in which police can use camera surveillance.⁹ Private security companies, particularly those providing security at night-time economy venues, similarly are choosing to use BWV.¹⁰ Citizen appetite for the spontaneous capture of images is already apparent from the widespread use of camera phones. Affordable BWV extends this capability. Connectivity with wireless technology extends exponentially the ability to distribute the images taken, either in real time or subsequently.

What are the ethical implications of this changed dynamic? As a tool for social control institutions the claimed benefits of BWV are similar to those claimed for CCTV or still photography surveillance: a deterrent to crime and a means of capturing evidence about crime being committed (thus realizing the purpose of policing in relation to public peace preservation and the investigation of crime). Encounters between police and public can be filmed and this serves both as evidence of what the citizen did and said and of what the police officer did and said. Potentially the record will be more accurate than notes written subsequently; less vulnerable to the interpretation and partial recollection of the note-taker; less open to dispute from the subject of the notes. These are obvious attractions.¹¹ Where the police are investigating a suspected offence and so are enforcing the law, the moral theory of policing provides a basis for justified image-taking even though it causes moral (and actual) harm.

But where BWV makes a significant difference is in empowering individuals to challenge immediately the justification for image-taking. Not only can police officers wearing BWV transmit real-time images of patrol activity to a central receiving station: the individual being imaged can engage in a real-time debate with the image-taker about consenting to be imaged. BWV extends the camera surveillance capability of the police officer. It also extends the range of ethical decisions that the officer will confront during any given policing activity. As well as being confronted with arguments about an individual's consent to being imaged, officer mobility between different categories of public, restricted and private space will require real-time protocol-based decision-making. If, for example, an officer is equipped with BWV which cannot be switched off by the user - in order to preserve the integrity of the accountability function of BWV - will the officer be prohibited from entering certain private spaces because of this?

The citizen engaging with a BWV-equipped police officer will know that they are being filmed if the technology is visible or declared; the citizen can identify the individual agent who is filming and not just the agency; and the citizen will be able immediately to challenge the legitimacy of and authority for the BWV use. Is a citizen entitled to request the camera be deactivated if the encounter is not one in which police are directly enforcing the law?

Suppose the officer is speaking to an individual in order to identify whether that individual is a relevant witness. Is the potential witness, because they are not suspected of anything, entitled to request the officer to stop filming? What might be the counter-claim?

Police recourse to otherwise immoral acts is justifiable to the extent that such conduct realises the fundamental end of policing, namely the protection of other (justifiably enforceable) moral rights.

This justification seems to fit well in circumstances in which a *suspect* is being (covertly) photographed, filmed or recorded, but does it also reasonably accommodate circumstances in which police are talking with an individual who may be a witness but turns out not to be? The appropriate focus is whether the police are justified in causing a moral harm (non-consensual filming constituting an intrusion of privacy) to the potential witness. Being able to identify with filmed images those individuals present in the area but who are not witnesses and so are eliminated from the enquiry may be desirable but is it sufficient to warrant filming such persons against their wishes? In the case of a suspected criminal the moral theory of policing offers justification for continued non-consensual imaging as the circumstances dictate. The argument for extending the moral theory of policing as a basis for justification beyond those directly committing crime is weaker. The officer, in seeking to identify witnesses, can be said to be seeking to realise the fundamental aim of policing by investigating an alleged crime - but where the manner of doing this alienates potential witnesses, even to the extent that an actual witness denies this fact and so withholds help the investigation needs, then the fundamental aim of policing in this circumstance has been frustrated. And if morally harmful police conduct frustrates the fundamental aim of policing then it seems not to be justified by the moral theory of policing.

Is there an alternative interest being protected if the police officer continues to film having been asked not to by the potential witness? Certainly the wider community (of which the potential witness is a member) has a legitimate interest in the police being professional and thorough in their work, and to continue filming despite the citizen's objection would be a means of holding the officer to account for their thoroughness and professionalism (in which case the BWV, although worn by the officer, becomes a tool for the member of the community to whom the officer is speaking). The wider interest of the community can be set alongside the interests of individual victims in the moral theory of policing but in this case the potential witness, as a member of the community, could assert that in their one-on-one encounter, the officer is directly and personally accountable to the potential witness (as a community member) and in such circumstances the potential witness (as a member of the community) has no need of technological assistance in holding the officer to account for their professionalism during the encounter. Indeed, accountability as a requirement on being granted discretionary use of coercive powers grounds a line of argument that a police officer should keep the BWV switched on at all times even if both the officer and the person being spoken to would prefer it to be switched off.

Supposing the roles were reversed: a citizen with BWV encounters a police officer not so equipped. Is the officer entitled to ask the citizen to stop filming? A police officer, when acting as such

(particularly when in uniform) has a weaker claim to privacy and autonomy in these circumstances. The officer is accountable to the community. If the citizen keeps the BWV activated whilst engaging with the officer, the officer – precisely because he or she is an officer - can have no sustainable objection to being recorded. Police officers should not attempt to remove, cover or disguise otherwise visible forms of identification such as a name badge or a shoulder number in order to evade accountability mechanisms. In the event that the citizen records behaviour on the part of the officer about which the citizen wishes to complain, once again the use to which the image (and information contained therein) will be put becomes relevant. Sending the image(s) to the officer's senior managers will result in a moral harm to the officer if admonished or punished for unprofessional or criminal conduct but that harm is justified by the weightier claim the community has to an effective and professional police service. But the citizen will have no reasonable justification if instead the images are posted on YouTube, the outcome of which may be exposure of the officer's unsatisfactory conduct beyond the community to which the officer is accountable with associated unwarranted humiliation: an unjustifiable moral harm. Only if the citizen could demonstrate that placing the matter in the hands of senior managers would have been to initiate a cover-up would the citizen perhaps then be justified in exposing the images more widely.

So much for BWV surveillance as a mechanism of social control: within the construction of surveillance as a way of seeing, BWV-equipped individuals pass through public spaces filming their lives; perhaps sharing the images online with a virtual community whose members the image-taker may not know or even know of. There seems to be little authority or moral justification for such individuals to continue filming others who object to being imaged - except where this can be demonstrated to be in the wider public interest.

In this construction of surveillance there is more than one way of seeing. Individual contributors to the blogosphere are but one range of actors. The Australian National VET E-learning Strategy envisages technology-assisted first-person documentation in the classroom.¹² To the generation who have known nothing but a digital environment populated with mobile media, using BWV in schools and colleges may seem uncontroversial. But the complexity of camera surveillance ethics in the public space points to the likelihood of complex ethical considerations in the educational space, particularly given the technological ease with which images can pass beyond the control of the person being imaged.

As a footnote to the distinction between the two constructions of surveillance, there exists an interesting possibility in which agents acting within the construction of surveillance as social control use surveillance as a way of seeing: specifically if police officers who are not officially equipped with

BWV in furtherance of their duties nevertheless equip themselves with BWV and use the images privately within social networking media and the blogosphere. Intuitively this seems to give rise to a number of objections based on the abuse of police authority inherent in such a scenario.

Conclusion

Non-consensual taking of an individual's image is a moral harm because it infringes individual privacy. Other than in circumstances where religious or cultural beliefs are profoundly offended by image-taking, in itself it is a moral harm unlikely to have significant actual harmful consequences. A more significant moral harm comes with the second element of the intrusion, the infringement of autonomy and the use of information from such images by third parties. Greater moral harm (and potentially significant actual harm) occurs when the image-subject not only has no control over how the images and information are used but also is directly or indirectly harmed by their subsequent use. The moral theory of policing provides an account in which lawful, proportionate and necessary non-consensual image-taking leading to subsequent moral and actual harm (e.g. conviction and punishment) can be morally justified in certain circumstances.

Taking official use of surveillance and CCTV as its initial context, this article has considered ethical aspects of non-consensual image-taking. Official use of BWV can be accommodated within the same moral conversation. But private citizen use of BWV for surveillant seeing changes the moral dynamic through promiscuous image-sharing and the absence of effective redress mechanisms for image-subjects.

The ethical concerns raised by CCTV camera surveillance and by covert investigation surveillance have begun to be addressed with a number of protections: for example, prior use-authorization regimes; data protection legislation; automatic periodic deletion; subject access protocols; and privacy-protection software.[7] Within the paradigm of public sector accountability, together with Von Hirsch's framework for ethical routine surveillance of public areas, such measures bring ethics-based regulation to official use of camera surveillance: a regime which can incorporate official use of BWV. In this sense BWV is merely a different manifestation of how State and citizen interact. The basic principle is the same as in other forms of interaction: regulating use of State power in relation to a citizen in order to prevent (or else remedy) abuse of that power.

The use of BWV technology by private citizens to capture information about other private citizens empowers the user to the extent that the user acquires usable information about another person,

thus creating an asymmetrical power relationship. The ethics of surveillance as social control have been widely considered and sousveillance can be accommodated within that ethical account. But such an account is found wanting in connection with citizen use of BWV surveillance because there is no obvious morally-justifiable counter-weight to the prima facie moral harms engaged.

The digital environment is redefining social interaction and creating a need for new ethical accounts.[3] Superficially empowered through social networking, individuals have in fact lost the last vestiges of control over how they manage information about self to present a desired public personality. Communications technology not facilitates interaction between people: it can also neutralize social inhibitions if the user perceives their interaction to be primarily with the technology rather than with the recipient of the message: hence the concept of 'netiquette' establishing conventions about acceptable ways of expressing self in email. For similar reasons, general recognition and understanding of what is acceptable and unacceptable in relation to private use of BWV technology is required. Because the immediate outcome of such use is the acquisition of information about others, the onus of ethical responsibility lies firmly with the users of images and recordings made with BWV technology when surveillance is used as a means of private seeing for the purpose of public sharing.

References

- [1] C. Burt, 'Privacy as security: comparative developments in Canada, the UK and the USA' in A. Doyle, R. Lippert and D. Lyon (eds) *Eyes Everywhere: The Global Growth of Camera Surveillance*. Abingdon: Routledge, 2012, 354-369.
- [2] K. Michael, 'For now we see through a glass, darkly' *IEEE Technology and Society Magazine*, 4-5, Winter 2013.
- [3] K. Michael, 'No limits to watching?', *Communications of the ACM*, 56(11), 26-28, November 2013.
- [4] S. Miller and J. Blackler, *Ethical Issues in Policing*. Aldershot: Ashgate, 2005, 26
- [5] J. Rachels, 'Why privacy is important', *Philosophy and Public Affairs* 4(4) 323-333, (1975), 326.
- [6] P. Roberts, 'Privacy, autonomy and criminal justice rights: philosophical preliminaries' in P. Alldridge and C. Brants (eds) *Personal Autonomy, the Private Sphere and the Criminal Law*. Oxford: Hart Publishing, 2001, 49-78, 58.
- [7] A. Senior, 'Privacy protection in a video surveillance system' in A. Senior (ed) *Protecting Privacy in Video Surveillance*. London: Springer-Verlag, 2009, 35-47.
- [8] S. Sontag, *On Photography*. London: Penguin Books, 1979
- [9] A. von Hirsch, 'The ethics of public television surveillance', in A. von Hirsch, D. Garland and A. Wakefield (eds), *Ethical and Social Perspectives on Situational Crime Prevention*. Oxford: Hart Publishing, 2000, 59-76, 64.

¹ I am grateful to Seth Lazar, School of Philosophy, The Australian National University, and to two anonymous peer reviewers for comments on early drafts of this paper.

² Such an act is not necessarily a legal wrong: in many jurisdictions there is no legal right to privacy. A moral right to privacy can exist even though it is not reinforced with a legal right.

³ Susan Sontag (1979:21) discusses the enrolment of photography into the service of institutions of social control. (There may, of course, be many occasions when an individual wants to be photographed in which case no moral harm arises if the image is put solely to the purpose intended by the image-subject.)

⁴ Burt, 'Privacy as security', 362-3: "As a practical matter, one's presence in, or use of, a public resource or facility is itself an act of revelation ...".

⁵ Where employer surveillance is for performance management purposes then the benefit may be less widely distributed, accruing only to the employer's and perhaps share-holders' profit rather than the health and safety of colleagues and perhaps the wider community. In such circumstances the justification claim for workplace surveillance seems weaker than a justification founded upon worker safety.

⁶ Such monitoring can identify persons excluded from the entitlement to be at large in a given public place through a court-imposed movement restriction for instance.

⁷ It is momentarily intruded upon each time I look at the photograph subsequently, but again to no significant adverse consequence if I do nothing with the information in the image other than appreciate its aesthetic value.

⁸ See wearcam.orh/rfd.htm (accessed 17.03.14).

⁹ See for example <http://www.hampshire.police.uk/Internet/advice/Body-Worn+Video+Devices.htm> (accessed 23 February 2012).

¹⁰ See for example http://www.macommercialsecurity.co.uk/body_worn_surveillance_systems.htm (accessed 23 February 2012).

¹¹ Claims that BWV reduces police patrol bureaucracy by negating the need to make contemporaneous written notes (<http://www.hampshire.police.uk/Internet/advice/Body-Worn+Video+Devices.htm> accessed 23 February 2012) fail to take into account the alternative bureaucratic needs that have instead been created: namely, managing the images and the information therein, including being able to retrieve pertinent parts of the video record as required.

¹² See <http://www.flexiblelearning.net.au/> (accessed 28 August 2012).