Tracking People Network

Briefing Paper 2

The Ethics of Tracking People

Anthea Hucklesby (University of Leeds, UK) and Kevin Macnish (University of Twente, The Netherlands)

Introduction

The ability to track the movements of individuals has become ubiquitous in modern societies via the use of smartphones which all have embedded GPS technology. Apps also exist which are designed specifically to enable individuals to track others – for example, many parents use apps to keep an 'eye' on their children. Whilst these uses of tracking technologies raise their own ethical issues, wearable tracking devices, which are designed specifically to be difficult to remove, heighten ethical concerns because they potentially, or actually do, involve an element of coercion. Wearers might lack capacity to consent to wearing the devices in the case of individuals with dementia or children in care or may be required to wear them as part of a court order (suspects/defendants/offenders) or because they are seeking asylum (immigration). There has been little debate about the ethical issues arising from the use of these difficult to remove devices despite their increasing use, both in terms of the number of domains in which they are deployed and the number of individuals subject to them. This paper summarises the main ethical issues connected with difficult to remove human tracking technologies.

Informed consent

Informed consent is an important ethical standard which requires individuals to give their permission *voluntarily* to something, having received all the pertinent information so that they have a clear understanding of the relevant facts and potential risks, implications and consequences. Legal definitions of consent require individuals to have choice *and* have the freedom and capacity to make that choice. The concern is that wearers are vulnerable to coercion and exploitation, even when nominal consent is provided.

Many potential wearers of difficult to remove devices are not in a position to give their informed consent. People with dementia or children and young people may lack capacity and defendants/offenders face tough, not free, choices – wearing a device or going to prison for instance. Assessments of whether devices should be used in these circumstances require weighing up the risks and the benefits to wearers and others, whether that is specific individuals (relatives or victims), organisations (the police) or the public at large. The dilemma is that these groups often have competing interests and difficult decisions need to be made about whose interests take priority.

Purpose and success

It cannot be ethical to require individuals to wear devices that do not do the job they are designed to do and/or which have insufficient resources to provide the necessary support or react when things go wrong. A clear purpose(s) must be articulated for success to be measured. These stated purposes most often relate to the prevention of harm to wearers and/or others. For instance, the purpose of devices worn by individuals with dementia is to provide alerts when they go 'wandering' beyond set limits and to assist with locating them. In theory this prevents them from going missing for long periods and potentially being harmed as a result. There are a number of pre-conditions to success: i) the devices must work; ii) the devices must stay in place; and iii) any alerts must be identified and acted upon within a reasonable timeframe. Devices are also linked to increased freedom for individuals – whether this is individuals with

Arts & Humanities Research Council

dementia or defendants/offenders who avoid being detained in prison. Rarely do devices have just one purpose – purposes may be complementary or compete with each other. For example, using devices on offenders might *inter alia*: reduce the number of individuals in prison; improve individuals' prospects for rehabilitation; provide reassurance to victims and/or the public; and save money. Not all ascribed purposes may be articulated openly. For instance, devices may be used to collect information on associates of offenders or individuals suspected or convicted of being involved in terrorism.

Different purposes may be assigned by different individuals and/or organisations and they may be viewed as more or less legitimate. For example, a less readily articulated purpose of dementia trackers is to save police resources and bring about financial savings. The police spend considerable time looking for missing persons with dementia taking up their limited resources. As a result, some forces have been proactive in setting up schemes to test out the technologies (BBC, 2013) whilst others are using nudging tactics (McAlees, 2018).

The rationale for using devices for those individuals seeking asylum is also linked to resources as well as surveillance – it should be easier for authorities to locate them. The potential pitfall, which this example clearly illustrates, is that wearers need to have a reason to comply and not to remove the devices. Compliance is complex but some applications more readily lend themselves to one or more of these mechanisms: i) deterrence - the threat of more severe punishment in the case of offenders; ii) legitimacy - the state/relative has a right to require individuals to wear devices; iii) instrumental – it has positive outcomes for wearers or their significant others. The legitimacy of some purposes may be questionable: for example, finding out more information about the networks that asylum seekers use whilst awaiting decisions or deportation or relatives using trackers to control or 'stalk' wearers. The potential for harm to come to wearers is ever present – individuals with dementia may be exploited by relatives and offenders may be more easily locatable by associates who wish to harm them.

It is also unethical to provide false reassurance to individuals and the public about the efficacy of the devices. This has been a particular problem in criminal justice where tracking technologies have been referred to using terminology such as 'electronic ball and chain' or 'prison without bars' which gives the misleading impression that the devices incapacitate offenders. Similarly, devices sold as preventing individuals with dementia 'wandering' would create unrealistic expectations.

By focusing on measuring success, unforeseen effects of devices can be missed. Just because devices seem more humane and/or less intrusive it does not follow that they are better or more ethical (Bülow, 2014). Furthermore, these types of justifications can be insensitive to individuals and their needs because they focus on quantifiable outcomes. In all domains personal motivations and narratives should be considered.

Privacy

Privacy involves having control over what others know about you. Individuals make choices about what they do and what information they release about themselves. Privacy issues are pertinent to debates about their use because tracking devices collect data which has the potential to make third parties aware of information which normally would be unavailable, and potentially sensitive. For example, tracking data may show that an individual is spending long periods in an unusual location leading to questions about what they are doing there – it may be something unlawful but it may also be legitimate but private.

There are, of course, limits to privacy usually on the grounds of national security or the safety of the public but these are not uncontested concepts in themselves. They are vague and open to interpretation and grounds for making such assessments are often not transparent and/or in the public domain.

Privacy is also relative. Individuals confined to institutions such as prisons might have little privacy and view the additional privacy afforded to them in the community with a tracking device as preferable. However, just because one solution is preferable to another, it does not follow that either are justified *in toto*. It is still not known what harms might arise from depriving individuals of their privacy over time and it would likely be unethical to find this out. Nonetheless, it is possible that it has significant impact on relationships with others, individual autonomy and freedom of movement.

Chilling effects

Wearing tracking devices may deter individuals from activities and these are called chilling effects. Chilling effects are one of the legitimate purposes of deploying devices in some circumstances, for instance to deter offenders from going to particular places or associating with particular individuals. In other circumstances deterrence is not ethically legitimate and would likely be counterproductive. For example, when it prevents individuals with dementia from going to their local shop or to keep fit or art classes or when offenders cannot fully engage with potential pathways to rehabilitation. As the examples provided illustrate, chilling effects might be part of

the purpose of wearing devices or they may be unintended consequences. It is, therefore, vital that potential chilling effects form part of assessments of whether tracking devices should be deployed in particular circumstances.

Stigmatisation

Difficult to remove tracking devices are worn either around the ankle or wrist and come in various different sizes and configurations. Generally, devices used in criminal justice, immigration and terrorism domains are larger and more prominent than those in health and social care because the requirements need more battery power and because, in the case of criminal justice, the device is, arguably, part of the punishment. All devices may be visible and may be viewed as stigmatising by wearers. Fear of stigma as well as actually being stigmatised may impact upon individuals' feelings of well-being and their behaviour. For example, wearers may stop wearing particular clothes or going out or doing activities such a swimming for fear of the devices being seen. They may also avoid seeing certain people and explaining the presence of the devices to their children may be particularly challenging. Stigma by association may also be a consideration which may lead to others not wanting to be associated with wearers, potentially putting strain on positive and/or less constructive relationships.

A particular challenge when devices are used across domains is that their purpose may be mistaken because many of the devices look similar to the untrained eye. This may lead to one group of wearers (those with dementia) being mistaken for another group of wearers (offenders) or one group of offenders (shoplifters) being mistaken for another (sex offenders). Stigma then is as much about the reactions of the wider public to the wearing of devices as to the wearers.

Pinning down responsibility

Devices provide information that there is a potential problem which needs to be looked into and/or dealt with. Therefore adequate mechanisms need to be in place to react to alerts to avoid harm to wearers and/or others. An important ethical issue is who should be responsible for taking action and who takes responsibility when things go wrong. In the case of offenders these issues are relatively straightforward but they are less clear cut with dementia use – when individuals go missing who is responsible: the private companies providing the devices and support; the relative; the police or social services? Is it ethical to require relatives to make long trips to investigate the well-being of loved ones rather than involve public services? In the case of offenders, to what extent should families and friends be involved in offenders' punishment, provide housing and assist offenders to comply with their orders (Hucklesby, 2009).

The growing use of tracking devices raises the likelihood that services may have to prioritise cases they react to in future because there will be insufficient resources to deal with them. This is likely to lead to dilemmas such as whether the police should prioritise cases involving an individual with dementia, a woman at imminent risk of domestic abuse or apprehending an offender who has entered an exclusion zone?

Accounting for difference

It has been noted already that the devices used in different domains are similar. Equipment providers often supply more than one market, most commonly the offender/immigration markets but a few cross over between care and control functions. Whilst the capabilities of the technologies allow for the equipment to operate in different domains, it does not follow that this is desirable or ethical. The uses to which the equipment is put differ markedly and a 'one size fits all strategy' may not be appropriate. Similarly, wearers within domains differ and these differences should be considered. For example, all devices used in criminal justice are grey which are much more prominent on black than white skin, potentially producing different levels of stigma. Similarly, all devices are designed for men when a significant number of wearers are women, especially outside of criminal justice.

Equality of access is a key ethical issue in some domains, mostly notably care, where trackers and 24/7 support normally need to be purchased directly from commercial providers. Such resources are beyond the means of some resulting in inequitable access.

Ownership of tracking data

Tracking devices collect a large amount of data on individuals' movements. Data collected via Global Positioning Schemes (GPS) provide relatively accurate pictures of individuals' movements. There are various ways in which these data can be used. For instance, they can be checked against crime data and known locations, traced on Google maps and heat maps can be produced showing how long individuals spend in particular locations. Who owns, controls and has access to these data raise important ethical questions. Potential candidates include: individuals generating the data; individuals' carers or guardians; or companies/agencies operating the devices, collecting the data, or paying for the service. A general rule may be that the individuals or organisations paying for the service have the right to control the data generated by it. But this may mean that police forces, rather than carers,

have control over the data generated by individuals with dementia if they pay for the schemes. Data ownership is also complicated by the involvement of private firms – all devices rely on equipment providers' systems and data are collated and stored on their servers, irrespective of whether the purchasers are individuals or public sector organisations, or who legally or contractually 'owns' the data – it always relies on the private companies to facilitate access.

False positives and automation bias

Although tracking devices collect data 24/7 they usually work on a system of alerts. In the case of location tracking devices, alerts occur when wearers go somewhere they are not supposed to go, for example an exclusion zone or when they leave somewhere, for instance, their home or area to which they are confined. These systems are fully automated and the data produced are likely to be viewed as irrefutable. As a result, there is a strong tendency, even among trained individuals, to override their intuitions in preference for outputs from the system, even when there is clear evidence to the contrary. For example, when drivers drive their cars into rivers while following SatNavs (Pritchard, 2017).

It is important to be mindful of the pitfalls of automation bias particularly when the consequences may be significant, for example being returned to prison to complete a sentence or relatives travelling long distances because their relative has been wrongly identified as missing. Automation bias can be mitigated through training, but recognising that technologies are not infallible and do not provide the context to an event must always be considered.

The alerts which are received may not be accurate and create false positives, i.e. that a prohibited event has occurred when in fact it has not, or false negatives i.e. failing to pick up an event. Whilst the technology of tracking devices is considered to work well in most cases, problems still exist. This might be because of problems with the technology. For example, it is well known that GPS does not work inside buildings but also that there is a problem of drift i.e. an individual's position is given as somewhere different to where they actually are (Kemp, 2017). Equipment might also be fitted incorrectly and/or the exclusion or inclusion zones set inaccurately. Sometimes those involved in the operation can be corrupt, as in the recent case of monitoring officers fitting tags on offenders which could be easily be removed (BBC, 2017). Finally, data may be wrong, misleading or be interpreted wrongly. Even when the technology works it relies on humans to interpret and act upon it. Both false positives and false negatives can have detrimental effects on wearers and those around them as well as those being protected.

Concluding comments

The use of tracking devices raises considerable ethical issues whichever domain they are deployed in. The major challenge is for ethical debates to keep ahead of technological developments so that ethical issues are considered prior to the widespread adoption of technologies and are only deployed in legitimate circumstances.

References

British Broadcasting Corporation (BBC) (2013) Police use GPS trackers to find people with dementia, BBC News online 30.04.2018 at: https://www.bbc.co.uk/news/av/health-22351445/police-use-gps-trackers-to-find-people-with-dementia [accessed 25.01.2019]

British Broadcasting Corporation (BBC) (2017) 'Electronic tag misuse inquiry leads to 29 people being charged', BBC News online 27.11.2017 at: https://www.bbc.co.uk/news/uk-england-42135107 [accessed 25.01.2019]

Bülow, W. (2014) 'Electronic monitoring of offenders: an ethical review', *Science and Engineering Ethics*, 20: 505–518.

Hucklesby, A. (2009) 'Understanding offenders' compliance: a case study of electronically monitored curfew orders', *Journal of Law and Society*, 36(2): 248-71

Kemp, A. (2017) 'Tracking Technology', Tracking People seminar 15 June 2017, University of Leeds at: http://trackingpeople.leeds.ac.uk/2016/08/tracking-people-technological-and-methodological-challenges/

McAlees, M (2018) 'Police urge families to use GPS tracking to keep people with dementia safe', Carehome.ac.uk, 21.09.18 at: https://www.carehome.co.uk/news/article.cfm/id/1600238/Met-police-urges-public-to-use-GPS [accessed 25.01.18]

Pritchard, H., (2017) 'A BMW driver followed his Sat Nav straight into a river' at: http://www.walesonline.co.uk/news/wales-news/bmw-driver-followed-sat-nav-12564727 [accessed 10.11.18].

This briefing paper is one of a series produced by the Arts and Humanities Research Council (AHRC) funded 'Tracking People' network. This cross-disciplinary network brings together academics, policy makers and practitioners from diverse domains including criminal justice, immigration, mental health, dementia, terrorism and children's services to examine the use of tracking devices (non-removable wearable devices that enable location monitoring or tracking of wearers by third parties).

More information about the network is available at: http://trackingpeople.leeds.ac.uk or contact the Network Chair, Professor Anthea Hucklesby (A.L.Hucklesby@leeds.ac.uk).