CHAPTER 12

COVERT ASPECTS OF SURVEILLANCE AND THE ETHICAL ISSUES THEY RAISE

David J. Harper, Darren Ellis and Ian Tucker

ABSTRACT

This chapter focusses on the ethical issues raised by different types of surveillance and the varied ways in which surveillance can be covert. Three case studies are presented which highlight different types of surveillance and different ethical concerns. The first case concerns the use of undercover police to infiltrate political activist groups over a 40-year period in the UK. The second case study examines a joint operation by US and Australian law enforcement agencies: the FBI's operation Trojan Shield and the AFP's Operation Ironside. This involved distributing encrypted phone handsets to serious criminal organisations which included a 'backdoor' secretly sending encrypted copies of all messages to law enforcement. The third case study analyses the use of emotional artificial intelligence systems in educational digital learning platforms for children where technology companies collect, store and use intrusive personal data in an opaque manner. The authors discuss similarities and differences in the ethical questions raised by these cases, for example, the involvement of the state versus private corporations, the kinds of information gathered and how it is used.

Keywords: Ethical issues; undercover police; human rights; encryption; artificial intelligence; educational technology

Ethical Issues in Covert, Security and Surveillance Research
Advances in Research Ethics and Integrity, Volume 8, 177–197

ISSN: 2398-6018/doi:10.1108/S2398-601820210000008013

INTRODUCTION

In this chapter, we focus on the ethical issues raised by different types of surveillance and the varied ways in which surveillance can be covert. Over the last decade, we have examined the social and psychological aspects of a range of surveillance practices and technologies including how the public understand and experience them (Ellis, Harper, & Tucker, 2016; Harper, Ellis, & Tucker, 2014; Harper, Tucker, & Ellis, 2013). We have been struck by the way in which public discourse about the ethics of surveillance is very much shaped by the types of surveillance seizing the popular imagination at the time. In one of our projects, in the Summer of 2010, when Londoners were asked about surveillance, they tended to spontaneously associate it with Closed Circuit Television (CCTV) in public spaces and some needed to be prompted about other, less visible, modes of surveillance. Over a decade later and the public are more aware of the way in which electronic data from digital devices is gathered, stored and used by governments and private corporations because of media reporting about technology companies and about the Edward Snowden National Security Agency (NSA) disclosures. Yet many are still not aware of the myriad ways in which they are surveilled every day and often only a restricted range of issues – privacy, security and convenience – feature in public discourse. However, as Macnish notes in his introduction to this volume, surveillance involves a range of activities, practices and technologies that often engage distinct types of ethical concern. In this chapter, therefore, we examine three contemporary examples of covert forms of surveillance – all involving the gathering, storage and usage of information about people in a covert or hidden manner – both human and technological and involving the state or private corporations. We discuss the specific aspects of these types of surveillance which raise ethical concerns. In the concluding section, we discuss commonalities and differences in the kinds of ethical questions engaged by the case studies and suggest potential avenues worthy of further exploration by researchers and in public debate.

CASE STUDY 1 – COVERT SURVEILLANCE OF ACTIVIST GROUPS BY UNDERCOVER POLICE: THE 'SPYCOPS' SCANDAL

Analogue Surveillance in a Digital World: Covert Surveillance by Human Beings

Technological surveillance might have captured the contemporary popular imagination but surveillance by human beings – the oldest form of surveillance – is still with us. Although endemic in totalitarian societies, human surveillance by the state (as opposed to surveillance by private investigators or security companies) operates at a much smaller scale in Western liberal democracies: in the UK in 2019, there were 3,652 authorisations of 'Covert Human Intelligence Sources' (i.e. informants or undercover officers) and 8,049 authorisations for 'directed surveillance' (i.e. covert surveillance of a person in public by undercover surveillance teams). In contrast, technological surveillance is much more prevalent – for example, in the same period, there were 116,171 authorisations[1] for the use

of communications data by the Metropolitan Police Service Central Intelligence Unit (Investigatory Powers Commissioner's Office, 2020). Yet, although technology-mediated surveillance is much more common, human surveillance can intrude into people's personal lives in a much more invasive and potentially harmful manner since it often involves deceptive relationships and betraying others' trust.

This case study concerns the Special Demonstration Squad (SDS), which ran from 1968–2008, and similar units like the National Public Order Intelligence Unit (NPOIU[2]), established in 1999. In 2015, following a series of revelations and official inquiries, the UK government established a judge-led investigation – the Undercover Policing Inquiry (UCPI[3]) – which began to hear evidence in November 2020.

Issues Raised During the UCPI

The SDS was established in 1968 within the London Metropolitan Police's Special Branch,[4] the policing body responsible for national security and terrorism and liaising with the Security Service (MI5). SDS officers often adopted cover identities by assuming the name of a real person who had died as a child.[5] They would change their appearance to blend in with activists, had vehicles and apartments in their cover names and would attend meetings, befriend activists and live their lives using these cover identities. In contrast to undercover police investigating crimes, these infiltrations were unusual in that they often lasted for several years, and officers did not collect evidence for criminal prosecutions. Over 1,000 groups were infiltrated (Evans, 2017). The information collected was quite intrusive. For example, the UCPI heard evidence that undercover officers:

> recorded the political activities of children as well as details of their parents' domestic lives. On one occasion, an undercover officer sent back to his supervisors the babysitting rota that had been organised by leftwing campaigners …. They also recorded the births of campaigners' children and made comments in their reports about the lives of politically active parents, such as the fact they had a child with Down's syndrome …. Some reports recorded deeply personal information, such as leftwing activists experiencing mental illness and depression or having an abortion …. Others recorded the sexuality of activists …. The police spies regularly reported on the bank accounts and jobs of campaigners, along with their home addresses. (Evans, 2021c, 12 May)

SDS officer 'Paul Gray' (HN126,[6] 1977–1982) reported extensively on young people, including children active in Hackney School Kids Against the Nazis, as well as their teachers, sending photographs to his managers (Heaven, 2021). Evans (2020a, 28 October) reports that undercover officers collected information on campaigns about police injustice (e.g. the Stephen Lawrence campaign), caused miscarriages of justice because their presence was withheld from lawyers defending activists (in 26 cases officers had been arrested along with activists) and appear to have shared data with private companies enabling them to 'blacklist' applicants for jobs (see also Lubbers, 2015).

In contrast with technical surveillance, human intelligence can give insight into the plans and intentions of targets, but it generates many ethical dilemmas. In one of the earliest discussions of the use of human intelligence sources within

social movements, Marx (1974) observed that they faced a dilemma: staying on the fringes of the group gathering intelligence passively meant they had much less access to information than if they took on leadership roles. The UCPI has heard how undercover officers often rose to key administrative positions in the groups they infiltrated, passing membership lists to their headquarters who, in turn often passed them onto 'Box 500', the Security Service (MI5). However, as Marx (1974) notes, being a more active and senior member of a group increases the risk that officers significantly affect the direction of the group's activities and raises serious questions about whether they might be viewed as agent provocateurs. Marx (1974) also observes that the importance of the group and the threat is vulnerable to exaggeration:

> Further, wishful thinking, limited exposure, and selective perception may lead the agent to believe a group's own exaggerated estimates of its power and appeal and to confuse vague revolutionary rhetoric with specific plans. (p. 420)

Undercover Surveillance and Human Rights

A key concern for the activists surveilled by these officers is that their human rights were violated. Kate Wilson, an environmental activist who lived with 'Mark Stone' (in reality, NPOIU undercover officer Mark Kennedy) was deceived into a sexual relationship by this undercover police officer (Evans, 2021a, 20 April). In a landmark judgement in 2021 the Investigatory Powers Tribunal[7] upheld Wilson's complaint that several articles of the European Convention on Human Rights had been breached in her case (Wilson, 2021; Wilson v (1) Commissioner of Police of The Metropolis (2) National Police Chiefs' Council (2021, 30 September)). The articles breached were:

- Article 3: which prohibits torture and 'inhuman or degrading treatment or punishment'.
- Article 8: the right to respect for one's private and family life.
- Article 9: the right to freedom of thought, conscience and religion.
- Article 10: the right to freedom of expression.
- Article 11: the right to freedom of assembly and association.
- Article 14: Protection from discrimination

These articles are also relevant to many of the other activists surveilled by these undercover units. Some of the most serious ethical issues concern the way in which many officers invaded activists' personal lives. The UCPI is investigating the work of at least 139 undercover officers from the SDS, NPOIU and other units of whom more than 20 (i.e. over 14%) had sexual relationships with members of the groups under their cover identities (Evans, 2020a, 28 October). Many had long-term intimate relationships with activists, living with them for long periods and four fathered children with activists (Evans, 2021b, 22 April). Undercover officers often feigned mental health problems at the end of their deployment as part of an exit strategy. In 1987, animal activist 'Bob Robinson' suddenly broke contact with a female activist with whom he had had a child two years earlier. In 2012, she discovered that he was an undercover SDS officer

called Bob Lambert. She subsequently received an apology and £425,000 compensation in 2015 after taking legal action alleging assault, negligence, deceit and misconduct by senior officers (Kelly & Casciani, 2014). She said that it was 'like being raped by the state. We feel that we were sexually abused because none of us gave consent' (Lewis, Evans, & Pollak, 2013).

Seven women sued the Metropolitan Police for the emotional trauma caused by such deceptive intimate relationships (some lasting up to nine years) and the subsequent apology from Martin Hewitt, an assistant commissioner at the Metropolitan Police acknowledged that their human rights had been violated:

> some officers, acting undercover whilst seeking to infiltrate protest groups, entered into long-term intimate sexual relationships with women which were abusive, deceitful, manipulative and wrong … these relationships were a violation of the women's human rights, an abuse of police power and caused significant trauma … relationships like these should never have happened. They were wrong and were a gross violation of personal dignity and integrity. (Evans, 2015)

Other Harms of Undercover Surveillance

Undercover work is a common policing tactic when investigating serious organised crime networks and these deployments are recognised as stressful for officers (Curran, 2021) and extreme levels of compartmentalised secrecy mean their families often cannot be told what they are doing and they live with a constant worry about getting 'burned' (exposed) or losing a target (Loftus, Goold, & Mac Giollabhuí, 2016). For those infiltrating activist groups, there are unique challenges for officers – for example, many report being violently assaulted on demonstrations by uniformed police unaware that they were working undercover (see also Marx, 1974). In some cases, officers may experience mental health breakdowns (Casciani, 2015). Their families can experience other harms and three ex-wives of SDS officers said that the deployments had caused their marriages to break down (Evans, 2020b, 4 November). At least 42 dead children's identities were stolen and the police have admitted this caused their families 'hurt and offence' (Evans, 2016).

Infiltration also harms the groups targeted. Marx (1974, p. 428) notes that the discovery of informers or undercover officers can leave groups with 'feelings of demoralization, helplessness, cynicism and immobilizing paranoia, and can serve to disintegrate a movement'. Stephens Griffin's (2020) interviews with activists who had been surveilled revealed that their conceptions of a fixed and stable external reality were fundamentally challenged – as one participant put it 'everyone was questioning everything' (p. 8) with some being diverted from environmental activism. SDS 'Officer A' told a reporter '[i]f the SDS had been in existence at the time of the Suffragettes, their campaigns would never have got off the ground and they would have been quickly forgotten' (Thompson, 2020).

There are important questions then, about balancing the state's obligation to preserve public order and its obligation to protect legitimate debate and to provide the basis for a functioning civil society. How do we weigh up the potential harms of undercover surveillance with its possible benefits? Macnish (2015) has argued that proportionality and the level of intrusiveness are important considerations.

The Proportionality of Political Intelligence Gathering by Undercover Police

Given that the work of units like the SDS involved considerable intrusion into the personal lives of some activists, was it justified by the level of threat and were there no realistic alternatives? The SDS was formed because of rising concern about a wave of protests about the Vietnam War. For example, in a March 1968 demonstration thousands of people marched on the US embassy in London, the police lost control and more than 200 people were arrested (Evans & Lewis, 2013). The police and government were concerned about the threat of revolution posed by those it saw as subversive, especially those in anarchist and Trotskyist groups. In 1975, the Home Office Minister, Lord Harris of Greenwich, defined subversive activities as those 'which threaten the safety or well-being of the state and which are intended to overthrow or undermine parliamentary democracy by political, industrial or violent means' (Security Service, n.d.).

However, over the 40 years of its existence, there does not appear to have been any detailed and regular threat assessment conducted by the SDS nor any systematic consideration of potential harms and benefits. Moreover, there is evidence of inequity in the types of groups targeted. Although the UCPI have not published a full list of groups targeted, the *Guardian* journalist Rob Evans and the Undercover Research Group have collated a list of 135 organisations (Evans, 2019). As studies in the USA have found (Marx, 1974), the groups targeted were, overwhelmingly, on the political left, suggesting that target selection was inequitable, a key issue in deciding on the ethics of surveillance (Macnish, 2015). Out of the 135 groups infiltrated, only two were right-wing: the British National Party was infiltrated by three SDS officers and Combat-18 by one (Evans, 2019). The National Front, a violent racist group which was very active in the 1970s, does not appear to have been targeted at all.

According to evidence given by HN329, a founding member of the SDS, the unit focussed on 'people who were opposed to the current political situation, or the current government' (Casciani, 2020, 12 November) which seems a broader definition of subversion than that of Lord Harris and appears to simply involve opposition to the government of the day. HN329 went on to say '[i]t may well be that a particular group is completely harmless but we would be asked to find out what their objectives were. A file would then be opened' (Casciani, 2020, 12 November).

However, evidence heard by the UCPI suggests that surveillance of many groups deemed not to pose a threat in terms of serious crime or violence continued. For example, the Anti-apartheid Movement (AAM) was infiltrated by four SDS officers. In an earlier Freedom of Information Act investigation by the BBC, the Metropolitan Police was found to have gathered, between 1969 and 1995, 30 inch-thick files on the AAM. These files included 'reports of demonstrations and pickets' consisting of 'methodical listings of the banners carried and slogans chanted' but 'the documents seen by the BBC contain no evidence of the movement having been involved in anything criminal' (Rosenbaum, 2005). Anti-apartheid activist and ex-government minister Peter Hain argued that '[t]he police, in targeting us, were putting themselves on the wrong side of history'

and he asked why they were not 'targeting the agents of apartheid bombing and killing' (Casciani, 2021a, 30 April). When an SDS officer was asked whether anti-apartheid groups had sought to overthrow democracy, he stated that '[i]t was not all about overthrowing democracy but nuisance – they caused problems and dangers to the public' (Casciani, 2021b, 4 May).

The Socialist Workers Party (SWP) appears to have been a particular focus for the SDS. Although most groups seem to have been infiltrated by one or two SDS officers, the SWP was infiltrated by no fewer than 26 officers between 1970 and 2007 (Evans, 2019). For a small organisation with a membership in the low thousands with relatively little national influence, the proportionality of such surveillance seems questionable. Moreover, the SWP was already under heavy surveillance by the Security Service – Hollingsworth and Fielding (2003) report that MI5 had 25 informers in the organisation over a 30-year period whilst all 12 of its telephone lines were tapped. This level of infiltration of small groups has been seen in the USA too. Garrow (1988) reports that 17% of the Communist Party USA were FBI informants as were 11% of the US SWP even though it only had 480 members.

But, as the barrister for activists argued at the UCPI, the SDS did not appear to conduct any 'regular and thorough risk and threat assessments which fully set out and consider any alleged risk to the public and the state from both public disorder and subversion' (Heaven, 2021, p. 4). Indeed, a witness from the Security Service (MI5) was sanguine about the threat of subversion, noting that:

> It appears … that the Security Service did not consider that subversive organisations posed a particularly high priority threat, and the pressure to investigate these organisations often came from the Prime Minister and Whitehall. (Witness Z, 2021)

However, despite this, the UCPI has heard evidence that the Security Service continued to task SDS officers with gathering information for its files.

'Domestic Extremists' as the New 'Subversives'

In the twenty-first century the term 'subversive' has gone out of fashion and, instead, policy documents now refer to the similarly ambiguous term 'domestic extremism'. Schlembach (2018) observes that some definitions emphasise the risk of violence whilst others refer to 'serious criminal activity', a much broader category if it includes damage to property and public disruption rather than violence towards people. The ambiguity and apparently widespread use of this term is likely to lead to the kinds of problems seen with the similarly ambiguous term 'subversive'.

It is hard to escape the conclusion that these undercover units were used less because of the level of threat posed by activist groups but for pragmatic reasons like the fear of political embarrassment when they cause public disruption or the ease of surveillance by human rather than technological means. Garrow (1988, p. 9), for example, has argued that the FBI made extensive use of informants in political groups because human sources were more efficient than electronic surveillance 'which consumed vast quantities of agent and clerical staff time while gathering, vacuum-cleaner style, far more chaff and trivia than even the FBI wanted'. Even if we accept that the state has a legitimate interest in

surveilling such organisations, it is hard to believe that, in the era of big data and the extensive use of social media by campaign groups, there are not alternative, less intrusive forms of surveillance which would avoid the risk of the kinds of abuses investigated by the UCPI.

We do not know whether there is now more rigorous assessment of the threat posed by groups and whether there are mechanisms for weighing up the potential harms and benefits of such intrusive surveillance. Evidence given to the UCPI suggests there was previously a level of disregard for the range of potential harms which bordered on the reckless. Although there might be a temptation to regard abuses as the result of a small number of 'rotten apples', the number of officers involved suggests that the failings are of a systemic nature. Given that the vast majority of undercover officers involved in sexual relationships with activists were men (as were their managers), some activists have argued that the apparent lack of guidance about sexual relationships with activists indicates the existence of institutional sexism (Evans, 2014).

In contrast to undercover political intelligence gathering, infiltration of organised crime networks by undercover officers attracts more public support. However, here too, innovative policing tactics have raised ethical dilemmas. In the next section, we discuss Operation Trojan Shield, a recent international policing operation where criminal organisations were surveilled via ΛNØM, an apparently encrypted device which, unbeknownst to the criminals, secretly sent copies of messages to the police.

CASE STUDY 2 – ΛNØM AND OPERATION TROJAN SHIELD

ANOM

In 2018, a secure messaging company called Phantom Secure was suspended and shut down as the CEO Vincent Ramos was arrested in Washington. The Canadian company had provided many international criminals, such as high-level drug traffickers and other organised crime groups, with modified secure mobile phones (Federal Bureau of Investigation, 2018). An investigation revealed that they sold the devices exclusively to members of criminal organisations, particularly targeting transnational criminal organisations (Cheviron, 2021). Ramos was asked by the FBI to insert a backdoor into the device so that the criminal communications could be surveilled but he refused. However, with the closure of Phantom Secure, organised crime networks needed secure communications and the fact that its clientele seemed to consist only of criminals meant that law enforcement agencies, assessing that the general public would not be affected, saw an ideal opportunity to target criminal networks.

An international collaboration developed between the San Diego FBI office's Operation Trojan Shield and the Australian Federal Police's (AFP) Operation Ironside to develop a next generation encrypted device and app known as ANOM (often styled as AN0M or ΛNØM).

The FBI worked with a 'Confidential Human Source' (Cheviron, 2020) to develop and distribute the devices in exchange for a reduced sentence, $120,000, and travel expenses of around $60,000. Initially ANOM was beta tested with 50 users in Australia. Cheviron suggests that this trial was a success and enabled the AFP to penetrate two of the most sophisticated criminal networks operating in Australia. Importantly, for the project's ethical viability, he adds that 'according to Australian law enforcement, 100% of Anom users in the test phase used Anom to engage in criminal activity' (Cheviron, 2020, p. 8). In other words, the technology was not being used for anything outside of crime. The operation moved on to the next phase and, by May 2021 there were about 9,000 devices in use. The devices – costing approximately £2,000 for a six-month service plan – sent and received encrypted electronic communications and stored data in encrypted form but had limited functionality. For example, users could not make normal phone calls or surf the internet. However, users were not aware that a master key was built into the device which surreptitiously attached to each message, allowing them to be instantly stored and decrypted by law enforcement. It was widely reported that over 800 people were arrested around the world, $48m in cash and cryptocurrencies and over 32 tonnes of drugs were seized, and more than 100 murder plots were counteracted. Europol reported that over 27 million messages were collected and it is expected that there will be further arrests in the future.

Privacy advocates have welcomed the fact that the operation did not involve inserting backdoors into products used by the general public, but they have also raised concerns. For example, Ashkan Soltani, previously the Chief Technologist of the Federal Trade Commission in the Division of Privacy and Identity Protection, stated that the operation showed that 'You can use good old-fashioned detective work and operations without backdooring protocols and services that consumers widely use' (Murphy, 2021). However, he went on to question the potential for the surveillance of innocent people. How many 'non-targets', he asked, were 'swept up in this operation?' (Murphy, 2021). Cheviron (2020) states that he believes 'that Anom devices are used exclusively to openly discuss criminal schemes or to maintain relationships in furtherance of those schemes' (p. 11). Presently, we can only assume that 'non-targets' were not caught up within the surveillance operation.

Concerns have also been raised about the impact of such operations on the legitimate encryption industry and about the way in which international law enforcement collaborations can enable national laws to be circumvented.

'Laundering' Surveillance

Jennifer Lynch, the Surveillance Litigation Director at the Electronic Frontier Foundation, has stated that US law enforcement was not able to monitor domestic Anom users because this would violate the Fourth Amendment and the Wiretap Act. Therefore, the USA relied upon other countries without these regulations 'to launder its surveillance' (Murphy, 2021). To circumvent US laws, the devices routed BCC encryptions of the messages to an iBot server outside of the USA, where it was decrypted, then re-encrypted with an FBI encryption code

before being decrypted again for viewing (Cheviron, 2020). Around the middle of 2019, the investigators sought a third country to obtain an iBot server of its own because, although Australia's judicial order allowed for the interception of Anom communications, it was unauthorised to share the information with foreign partners (Cheviron, 2020, p. 8, footnote 6). The mass raids and arrests took place on 8 June 2021, the day after the expiration of the court order allowing the third country to supply Anom server data to the FBI and this was probably no coincidence.

Greg Barns SC from the Australian Lawyers Alliance suggested that Australia was likely chosen as a partner in the operation because of its 'very weak privacy protections'. He went on to state:

> Often with these operations you go to the country with the weakest laws, as it were, so that you can obtain more evidence more easily and run less of a risk of evidence being obtained illegally. (Swanston, 2021)

Barns has argued that this is a form of entrapment wherein people are induced into committing a crime – entrapment is allowed in Australia but not in the USA.

Varying legal regimes mean that such international law enforcement collaborations provide potential societal benefits in terms of increased flexibility in mounting operations against well-funded targets but potential societal harms by undermining legal protections within each jurisdiction. This international operation has also reignited the debate about the legitimacy of public access to encryption.

The Rights and Wrongs of Encryption and Decryption

The US Department of Justice has made it clear that a goal of the operation was to target encryption. Randy Grossman, the acting US attorney said:

> Hardened encryption devices usually provide an impenetrable shield against law enforcement surveillance detection. The supreme irony here is that the very devices that these criminals were using to hide from law enforcement were actually beacons for law enforcement. We aim to shatter any confidence in the hardened encrypted device industry with our indictment and announcement that this platform was run by the FBI. (United States Department of Justice, 2021)

Wired reports that the US Department of Justice and other law enforcement agencies have long lobbied for access to 'end-to-end' encrypted data from, for example, social media and other communication platforms (Newman, 2021). Since data are kept scrambled by companies so that they remain undecipherable along their journey across the internet, law enforcement agencies do not have access to their content, a problem they refer to as 'going dark'. However, *Wired* argue that the FBI and, of course other agencies, have had continued success in finding creative ways of developing workarounds by, for example, targeting the devices rather than the encryption protocols themselves.

Some might argue that, given the success of operations like this, backdoors should be built into all apps. For example, in 2019 the UK's Government Communications Headquarters (GCHQ) proposed that communication systems should be designed to include a silent, unseen participant like another member

of the group chat, enabling government agencies to access them. However, there was a storm of reaction against this, not only from human rights groups but also from the Big Tech companies. Indeed, many of these companies introduced end-to-end encryption in the first place because of public reaction to the activities of the US and UK governments. Edward Snowden disclosed that, under the NSA's PRISM programme, technology companies passed internet data to the NSA and that, under the MUSCULAR programme, GCHQ and the NSA had hacked into the main communications links connecting the data centres run by Yahoo! and Google without their knowledge. PRISM threatened public trust in technology companies whereas MUSCULAR threatened the companies' trust in the US and UK governments. End-to-end encryption appeared to them to provide a solution to both problems.

Research suggests that, whilst there is wide public support for overt surveillance like CCTV, there is less support for covert and digital surveillance. The 34th British Social Attitudes (BSA) Survey reported that, although 80% of the public supported the use of video surveillance in public areas, 60% supported the collection of 'information about anyone living in Britain without their knowledge' and only 50% supported the monitoring of emails and other internet activity (Clery, Curtice, & Harding, 2016). Although Operation Trojan Shield will in the future be seen as a very successful method of counteracting serious organised crime, it will also serve to remind us that our online lives are always in danger of being covertly surveilled.

Operation Trojan Shield threw up some unique challenges. For example, the FBI needed to ensure both that the general public was not affected and that the fake encrypted phone company's cover was maintained. Andrew Young, a partner in the Litigation Department in law firm Barnes and Thornburg stated 'We can't just run a good investigation; we have to run a good company' (Cox, 2021). This included ensuring both that the marketing of the company was done correctly, and that the fake company was credible. In order to gain and maintain good customer service and satisfaction they had to provide technical support and deal with hackers. Importantly, they had to make sure that it did not become mainstream – they could not allow it to get into the hands of the public because of the ethical issues related to surveilling non-targets. Hence, distribution needed to happen within the criminal circles. A key unwitting distributor was Hakan Ayik who had long standing connections with Australian biker gangs and was an alleged drug lord. Ayik is currently an international fugitive, wanted not only by the authorities but, presumably, by previous customers who hold him responsible for their predicament (BBC News online, 2021).

Operation Trojan Shield is a good example of surveillance through data and digital technologies. Indeed, the capture, processing and categorisation of data has unsurprisingly become a significant part of surveillance studies and raises significant ethical challenges (Harper et al., 2013; Tucker, 2013; Van Dijck, 2014). Another key area, outside of law enforcement, in which data capture and processing is a growing concern is in relation to children's learning in schools, and the associated role of forms of education technology (so-called 'EdTech'). The use of digital learning platforms, and associated technologies in schools, has risen significantly during the Covid-19 pandemic. However, it is not clear that governance

structures have kept pace with their increased use, or with the new technological developments on the horizon (e.g. use of artificial intelligence, AI). The next section focusses on some of the ethical concerns of EdTech, with a specific focus on the UK context.

CASE STUDY 3 – SURVEILLANCE, EDUCATION AND EMOTIONAL AI

The use of large scale digital learning platforms, such as Google Classroom, has increased significantly over the past decade. Many schools have welcomed the possibility to use platforms that can streamline key learning processes, and often these are free of charge. For instance, Google Classroom allows teachers to set work for children, to mark and feedback, and to communicate updates via Classroom or linked Google platforms, such as via Gmail. The fact that Google's digital learning platform is free to use, makes it an attractive option for many schools, particularly given significant pressure on school budgets in many countries. The use of platforms such as Google Classroom has risen markedly during the Covid-19 pandemic, with registered users rising from 40 to 150 million worldwide during this period (Williamson, 2021). The advantages of using the platform in terms of delivering learning mean that it is likely that many schools will continue to use it after Covid-19 'lockdowns' imposed by many countries, which meant children accessed the learning remotely from home. Furthermore, Google, as the main provider of free digital learning platforms in primary and secondary education has sought to further strengthen its position through integration with other of its products and services, for example, providing low-cost Google Chromebooks to schools, that integrate seamlessly with its education ecosystem; examples include Classroom, Meet and Gmail.

Concerns have been raised about the increased presence of large data companies in education – with reference to children's privacy, and the extent of data generation from children's learning activity. For instance, the Electronic Frontier Foundation filed an official complaint with the Federal Trade Commission about data mining of children's personal information by Google's Workspace for Education (Williamson, 2021). Google's reply to such concerns is to stress the robustness of its privacy policy, in terms of not sharing personalised data. However, what is missing is transparency regarding how Google uses the data. Concerns have been raised that education technologies effectively become surveillance technologies because of the mass data processing involved in Edtech (Williamson, Potter, & Eynon, 2019). And furthermore, that the growing presence of education technologies in public education systems 'intensifies and normalises the surveillance of students' (Manolev, Sullivan, & Slee, 2019). We argue that the surveillance elements of education technologies are, in essence, covert, because (a) such technologies are not 'surveillance by design' and (b) children are highly unlikely to recognise them as forms of surveillance.

Governance of Education Technology in Schools

Children are, by definition, classed as a vulnerable group, and yet there is significant opacity regarding the governance of the use of education-focussed technologies such as Google Classroom in UK schools. This point is a key message from a recent Digital Futures Commission report (Day, 2021), which undertook a detailed analysis of the data-related legislation, and associated governance processes (at government and school level), in relation to the use of what they refer to as 'EdTech'. Whilst there are clear legislative frameworks for data processing, such as GDPR, there is no specific legislation focussing on the use of EdTech in schools, which given that its use, and therefore the role of the private sector, has increased significantly in recent years, is somewhat of a surprise. This lack of a legislative framework creates a governance vacuum, as schools and local education authorities (LEAs) do not have clear legislation upon which to develop and implement their local governance practices. The current system also places significant responsibility on schools to manage governance, as policies allow and encourage schools to identify their own EdTech systems, meaning that different schools can use different platforms (although the 'free to use' policies of big players such as Google Classroom means that certain platforms are coming to dominate).

The fact that legislation lags behind the data generating and processing practices of EdTech makes it difficult to identify the entirety of the ethical concerns in relation to children's data in schools. With children having to attend school by law (unless they have a home-schooling agreement with their LEA), they have no choice but to engage with any EdTech used by their school. This makes the use of EdTech such an important ethical issue, because children cannot avoid it. The opacity regarding the governance of data processing activity means that forms of covert surveillance emerge. For instance, does a child understand that if they opt-in to an associated product/service provided by their EdTech provider, they could be consenting to the company to use their data for marketing purposes – and that such activity involves a direct contract between child and digital platform, outside of any school policy (Day, 2021)?

AI and EdTech

Concerns about the potential for surveillance of children's learning are broadening in relation to new developments involving the use of forms of AI in digital learning platforms. This step potentially signifies a move towards automated forms of learning, whereby children can ask an AI-driven conversational agent questions related to learning. Google CEO, Sundar Pichai, recently announced its foray in this area, an AI-driven system called LaMDA (Language Model for Dialogue Applications), which is a natural language processor-based conversational agent that children can ask questions of and subsequently receive responses in a conversational format (Williamson, 2021). We know that such systems rely on 'learning' from the data gathered from previous interactions, so will involve mass aggregation of data related to children's learning, and as such, involve widespread surveillance of engagement with digital learning platforms.

Given the fact that AI and data mining are dependent on having large amounts of data, there is significant incentive to expand aggressively into new domains like education. In addition to major technologies and data companies such as Google moving into large scale data mining in education, there are also smaller technology firms drawn to education and the development of AI-driven tools to capture and categorise children's learning.

One example is the use of AI-based emotion detection systems, for example, http://www.4littletrees.com/ which has been used in secondary education in Hong Kong (Murgia, 2021). 4 Little Trees is an AI-driven system that is designed to identify and monitor children's emotional responses and activity during online lessons. The aim is to provide feedback to teacher and schools about when students lose attention, and whether this informs as to the effectiveness of teaching practices and allow for teachers to respond to children's learning in 'real time': for example, if 4 Little Trees suggests a child is losing attention a teacher can ask a question to that child to re-engage them. 4 Little Trees is based on facial recognition systems that have been used by law enforcement and border control agencies in recent years. 4 Little Trees extends the 'recognition' capabilities of such systems through claiming to be able to identify not the person's identity, but their emotions, feelings, sentiments. The growth of emotion-related facial recognition systems, which have been named 'emotional-AI' has been significant in recent years (McStay, 2018, 2020). The attraction to advertisers of being able to identify individuals' emotional responses to adverts is a major one and is driving the industry. Its use in education is at the embryonic stage, but there is no reason to think that education will be naturally immune to the desire and push to automate that AI-driven systems offer.

There are important points to note regarding emotion-AI systems such as 4 Little Trees. Firstly, that the data collected from children are of an intrusive nature (e.g. emotional state, videos of children in their homes and so on). Secondly, it is not entirely transparent how the data will be used, both by the private sector (i.e. 4 Little Tress) and by schools. Whilst 4 Little Trees states that data collected by authority figures (i.e. teachers) will be used to make decisions about children's engagement with learning, it is not clear how it might be used in the future. Finally, the universal model of emotion that such technologies are developed from (i.e. that a core set of emotions exist with largely universal modes of expression) has been extensively critiqued (Barrett, 2018; Barrett, Adolphs, Marsella, Martinez, & Pollak, 2019; Ellis & Tucker, 2020). The implication of these critiques is that the categorisation of the emotional states of children cannot reliably be taken as accurate. If we cannot rely on interpretations of systems such as 4 Little Trees, it is problematic to base elements of children's education on them. An expression of inattention could relate to a child reflecting on a problem relating to their learning, rather than inattention per se. Furthermore, if a child is deemed to be inattentive and unengaged, despite previous warnings, would this lead to punishments?

The real time monitoring, tracking and categorising of children's facial expressions during online learning is an example of an emerging form of surveillance. Whilst it resonates with traditional notions of top-down power, in the form of

powerful organisations (such as technology companies and schools) initiating and undertaking the surveillance, its operation is closer to what Isin and Ruppert (2020) refer to as *sensory power,* which involves 'data that tracks and traces people in their movements, sentiments, needs and desires' (p. 2). In the case of 4 Little Trees, it is the tracking and categorising of facial expressions in terms of emotion, mood and attention. Isin and Ruppert claim sensory power is a new form of power that is distinguished from traditional notions of sovereign, disciplinary and regulatory power. Data tracking technologies such as emotion-AI systems have made possible more sophisticated forms of surveillance in terms of focussing down on specific psycho-physiological activity, such as with micro-facial expressions. Others forms of tracking have also emerged, such as fitness trackers that can capture and categorise heart rate, skin conductance and so on.

The ethical challenges of EdTech are only going to continue to grow as with increased use of AI in digital learning platforms. To date, much of the data under focus has involved things such as children's IP addresses, time spent engaging with platforms, wider patterns of use and such like. The advent of tools such as 4 Little Trees adds an additional layer because it generates different kinds of data about children. The processing of descriptive data about patterns of use (such as location, duration) is added to data interpreting and categorising children's faces directly in relation to emotion and attentional state. This is a more sophisticated level of data, which is seen as attractive due to its potential to inform regarding the effectiveness of different forms of online learning. However, its categorising of facial expressions as informing of emotional states, based on problematic emotion science, makes it both intrusive and potentially inaccurate due to not being scientifically valid.

Allowing private companies to develop and use facial recognition technologies in children's learning environments presents major ethical challenges, from concerns regarding data protection through to allowing private companies access to videos of children's engagement in 'real time' learning in their homes. This is an emerging area of concern, for which new forms of governance are required. Whilst the 4 Little Trees system is not currently in use in the UK, it is indicative of one direction that EdTech is taking, and as such it is an important example of the considerations for governance processes. As the Digital Futures Commission Report notes:

> [G]iven the lack of data governance or data analytics expertise in schools, putting the responsibility on schools to negotiate these contracts puts a large amount of power in the hands of EdTech companies to interpret and apply data protection laws in a way that suits their own commercial purposes, without any oversight. (Day, 2021, p. 46)

In relation to the current use of EdTech in UK schools, the system's positioning of responsibility at the level of schools, which can often lack the detailed technical knowledge to map sophisticated data generating and processing practices onto existing governance, is not an optimal strategy to ensure transparent and ethical governance structures. Legislation and governance structures are required to be developed and implemented at the level of government and given the significant increase in the use of EdTech during the Covid-19 pandemic, the need is significant and pressing (Day, 2021).

DISCUSSION

The three case studies we have presented raise some common and some different ethical concerns. All involved the gathering of data on individuals but the nature of the information varied. In the 'spycops' and AI EdTech cases the data were potentially of a very personal nature whereas ΛNØM appeared to gather data mainly about criminal activity. Both the 'spycops' and ΛNØM cases involved intentional deception whereas, in the case of AI EdTech the nature of the data gathering was opaque rather than deceptive. The data in the ΛNØM case were gathered to support criminal prosecutions whereas, in the 'Spycops' and AI EdTech cases the future use of the data, and thus consequences for the individuals, was unclear. Similarly, in the latter two cases, the information was potentially inaccurate. The cases differed also in respect of whether the information was gathered by the state or by private corporations. In the two cases of state surveillance, deception was also involved. Key concerns here include proportionality and whether the targeting was discriminate. In the ΛNØM case, the target group appeared to be clearly defined but, although undercover infiltration might be regarded as proportionate in relation to the threat posed by serious organised crime networks, there are questions about the benefit versus harm calculus. For example, it is unclear whether the operation will have unintended long-term consequences like weakening public trust in commercial encryption products. In the 'spycops' case, there was little evidence of a rigorous threat assessment and deliberation of harms and benefits, the targeting seemed to lack discrimination and there was significant collateral intrusion and breaches of human rights.

In the case of AI EdTech, the involvement of large private corporations gathering data raises some different ethical questions not only about the datafication of children who have not been able to give consent and the commercialisation of education but also about what Zuboff (2019) has termed 'surveillance capitalism'. The motto of surveillance capitalism can be summarised, in Bruce Schneier's (2015) memorable phrase, as '[i]f something is free, you're not the customer; you're the product' (p. 83). It has been argued that many private corporations now hold more personal information on the public than governments. Whilst, in principle, governments can be held accountable by their citizens, corporations are only accountable to their shareholders and the law (which is notoriously weak in this area, especially in the USA). This gives technology companies considerable leeway in how they use data gathered from their users. An investigation by ProPublica (https://www.propublica.org/) revealed that Facebook uses over 52,000 unique attributes – including categories like 'affinity', with different ethnic groups, 'pretending to text in awkward situations' and 'breastfeeding in public' – to classify its users which they market to advertisers (Angwin, Mattu, & Parris, 2016). ProPublica have reported on how some advertisers have used this information in a discriminatory fashion, for instance, only advertising housing to white people. This is an example of how information collected in an opaque fashion can be utilised in a way that users are unaware of and thus this raises concern about how data collected on children might be used in the future.

Our review of these three cases demonstrates that, although covert aspects of surveillance prompt some common ethical concerns (e.g. privacy, lack of transparency, etc.), some questions arise from the specificity of the type of surveillance, who is employing it (e.g. the state or private corporations) and for what purpose. As a result, it is important in public discussion of ethics not to treat surveillance as a set of homogenous practices.

There is clearly a need for a more informed public debate about covert aspects of surveillance and further research is warranted on how the public understand and weigh up competing moral imperatives. For example, in relation to the 'spy-cops' case, what level of surveillance is publicly acceptable to prevent non-violent public disorder by activists compared with, say, people actively engaging in violent acts of terrorism? And, in either case, what degree of certainty do we have in the intelligence gathered? The 34th BSA Survey did not investigate these more intrusive types of surveillance though, interestingly, it found that two-thirds of the population supported the rights of groups to hold demonstrations and 50% supported this right even if the groups wanted to overthrow the government by revolution (Clery et al., 2016).

One of the challenges in public discourse about the ethics of surveillance is that, as we have noted, only a selected number of ethical issues are discussed and often those associated with particular types of surveillance. For example, state surveillance via CCTV and collection of digital communications engages questions of privacy but not the kinds of deception required in undercover operations. As a result, it can be helpful to utilise frameworks which prompt us to consider a broad range of ethical questions. One such framework is the 'ethical grid' developed by David Seedhouse (2009). Although there is not enough space to discuss the grid in detail, for the present discussion it is sufficient to understand that Seedhouse views good ethical decision-making as involving four different 'layers': a concern for individuals (which broadly engages concerns about human rights like respecting and creating autonomy, respecting persons equally; and serving needs first); a deontological layer (concerning moral duties like telling the truth, minimising harm, keeping promises and seeking to do the most positive good); a consequentialist layer (concerning the consequences of actions like what would deliver the most beneficial outcome for oneself, the individual, a particular group and/or society); and a layer of external considerations (such as laws, codes of practice, risks, the wishes of others, resources available, the effectiveness and efficiency of action, disputed facts and the degree of certainty of the evidence on which action is taken).

Since Seedhouse developed the ethical grid for use by healthcare professionals, it requires adaptation when considering the covert aspects of surveillance. But the notion that ethical decision-making requires attending to human rights, moral duties and the consequences of actions as well as a range of external considerations is a useful one and could help to guide future discussions. For example, there are obviously tensions within and between human rights and deontological and consequentialist concerns. We might wish to create and respect autonomy and equality for children, but society is prepared to accept restrictions on the autonomy of members of organised crime networks to minimise the harms caused by

serious crime. External considerations are also important – for example, what degree of certainty do we have that the information gathered (such as in relation to children's emotional state) is accurate? Hopefully the use of such frameworks might lead researchers to address a broader set of ethical questions and might inform a more comprehensive public debate. Given the secrecy and lack of transparency inherent in covert surveillance, such public debate is important.

NOTES

1. Some of these authorisations may be 'thematic'– that is, covering organisations.
2. This unit was subsumed into different organisations: the National Domestic Extremism Unit (2011–2013) and the National Domestic Extremism and Disorder Intelligence Unit (2013–2016). Domestic extremism now seems to be managed, along with national counter terrorism, by the National Police Chiefs' Council's Counter Terrorism Coordination Committee through the National Counter Terrorism Policing Headquarters.
3. The inquiry's extensive website (https://www.ucpi.org.uk/) provides access to hearing transcripts and evidential documents (over 1,000 at the time of writing). When hearings are being held summaries of each day's evidence can also be found on an activist website: http://campaignopposingpolicesurveillance.com/.
4. In 2006, the Metropolitan Police's Special Branch was subsumed under Counter Terrorism Command (SO15).
5. This tactic was popularised by Frederick Forsyth's 1971 novel *The Day of the Jackal*.
6. Names in inverted commas are cover identities rather than officers' real names. In the UCPI many officers are referred to by a code beginning with the letters 'HN'.
7. The Investigatory Powers Tribunal was established by the Regulation of Investigatory Powers Act 2000 in order to deal with complaints about their use.

REFERENCES

Angwin, K., Mattu, S. & Parris Jr., T. (2016, 27 December). Facebook doesn't tell users everything it really knows about them. Retrieved from https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them

Barrett, L. F. (2018). *How emotions are made: The secret life of the brain*. London: PAN Books.

Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. *Psychological Science in the Public Interest*, *20*(1), 1–68. https://doi.org/10.1177/1529100619832930

BBC News Online. (2021). Hakan Ayik: The man who accidentally helped FBI get in criminals' pockets. *BBC News Online*. Retrieved from https://www.bbc.co.uk/news/world-57397779

Casciani, D. (2015). Undercover policing inquiry: Why it matters. BBC News Online. Retrieved from https://www.bbc.co.uk/news/uk-33682769

Casciani, D. (2020, 12 November). Undercover officer targeted 'anti-establishment' left. BBC News online. Retrieved from https://www.bbc.co.uk/news/uk-54924071

Casciani, D. (2021, 30 April). Undercover police on wrong side of history, says ex-cabinet minister Lord Hain. BBC News Online. Retrieved from https://www.bbc.co.uk/news/uk-56948404

Casciani, D. (2021, 4 May). Undercover policing: Officer defends spying on anti-apartheid movement. BBC News Online. Retrieved from https://www.bbc.co.uk/news/uk-56988040

Cheviron, N. (2021). Affidavit in support of application for search warrant. Case 3:21-mj-01948-MSB Document 1 Filed 05/18/21 PageID.45 Page 2 of 33. Retrieved from https://web.archive.org/web/20210609190720/https://www.justice.gov/usao-sdca/press-release/file/1402426/download

Clery, E., Curtice, J., & Harding R. (2016). *British social attitudes: The 34th report*. London: NatCen Social Research. Retrieved from www.bsa.natcen.ac.uk

Cox, J. (2021, 10 June). 'We have to run a good company': How the FBI sold its encryption honeypot. *Vice*. Retrieved from https://www.vice.com/en/article/m7e733/anom-fbi-andrew-young-encryption-honeypot

Curran, L. S. (2021). An exploration of well-being in former covert and undercover police officers. *Journal of Police and Criminal Psychology*, *36*, 256–267. https://doi.org/10.1007/s11896-020-09406-x

Day, E. (2021). *Governance of data for children's learning in UK state schools*. Digital Futures Commission, 5Rights Foundation. Retrieved from https://digitalfuturescommission.org.uk/wp-content/uploads/2021/06/Governance-of-data-for-children-learning-Final.pdf

Ellis, D., Harper, D. & Tucker, I. (2016). The psychology of surveillance: Experiencing the 'Surveillance Society'. *The Psychologist*. 29 (September), 682–685. Retrieved from https://thepsychologist.bps.org.uk/volume-29/september/experiencing-surveillance-society

Ellis, D., & Tucker, I. (2020). *Emotion in the digital age: Technologies, data and psychosocial life*. London, UK: Routledge.

Evans, R. (2014). Police spies still get free rein to have sexual liaisons, say women suing Met. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2014/mar/28/police-spies-sexual-liaisons-women-suing-met

Evans, R. (2015). Police apologise to women who had relationships with undercover officers. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2015/nov/20/met-police-apologise-women-had-relationships-with-undercover-officers

Evans, R. (2016). Met to apologise to woman after admitting officer stole dead son's identity. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2016/dec/15/met-police-barbara-shaw-rod-richardson-anti-capitalist

Evans, R. (2017). Undercover police spied on more than 1,000 political groups in UK. *The Guardian*. Retrieved from https://amp.theguardian.com/uk-news/2017/jul/27/undercover-police-spied-on-more-than-1000-political-groups-in-uk

Evans, R. (2019). UK political groups spied on by undercover police – search the list. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/ng-interactive/2018/oct/15/uk-political-groups-spied-on-undercover-police-list

Evans, R. (2020, 28 October). Secrets and lies: Untangling the UK 'spy cops' scandal. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2020/oct/28/secrets-and-lies-untangling-the-uk-spy-cops-scandal

Evans, R. (2020, 4 November). Ex-wives of undercover police tell of marriages 'based on lies'. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2020/nov/04/ex-wives-undercover-police-inquiry-marriages-based-lies

Evans, R. (2021, 20 April). Police spy's bosses knew activist was being duped into sexual relationship, court told. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2021/apr/20/police-spys-bosses-knew-activist-was-being-duped-into-sexual-relationship-court-told

Evans, R. (2021, 22 April). Fourth officer allegedly fathered child after meeting woman undercover. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2021/apr/22/fourth-officer-allegedly-fathered-child-after-meeting-woman-undercover

Evans, R. (2021, 12 May). Undercover police frequently spied on children, inquiry hears. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2021/may/12/undercover-police-frequently-spied-on-children-inquiry-hears

Evans, R. & Lewis, P. (2013). *Undercover: The true story of Britain's secret police*. London, UK: Guardian/Faber & Faber.

Federal Bureau of Investigation (2018, 16 March). International criminal communication service dismantled phantom secure helped drug traffickers, organized crime worldwide. Retrieved from https://www.fbi.gov/news/stories/phantom-secure-takedown-031618

Garrow, D. J. (1988). FBI political harassment and FBI historiography: Analyzing informants and measuring the effects. *The Public Historian*, *10*(4), 5–18. https://doi.org/10.2307/3377831

Harper, D. J., Ellis, D. & Tucker, I. (2014). Surveillance. In T. Teo (ed) *Encyclopedia of critical psychology* (pp. 1887–1892). New York: Springer. https://doi.org/10.1007/978-1-4614-5583-7_305

Harper, D., Tucker, I. & Ellis, D. (2013). Surveillance and subjectivity: Everyday experiences of surveillance practices. In K.S. Ball & L. Snider (eds) *The surveillance-industrial complex: A political economy of surveillance* (pp.175–190). London, UK: Routledge.

Heaven, K. (2021, 15 April). Opening statement for tranche one phase two on behalf of the co-operating group of co-operating non-state, non-police core participants. (2021). Undercover Policing Inquiry. Retrieved from https://www.ucpi.org.uk/publications/opening-statement-from-richard-chessum-and-mary-for-tranche-1-phase-2/

Hollingsworth, M. & Fielding, N. (2003). *Defending the realm: Inside MI5 and the war on terrorism*. New edition. London, UK: André Deutsch.

Investigatory Powers Commissioner's Office (2020). *Annual Report of the Investigatory Powers Commissioner 2019* (HC 1039). London: Author. Retrieved from https://hansard.parliament.uk/commons/2020-12-15/debates/20121549000015/InvestigatoryPowersCommissionerAnnualReport2019

Isin, E., & Ruppert, E. (2020). The birth of sensory power: How a pandemic made it visible?. *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720969208

Kelly, J. & Casciani, D. (2014, 24 October). Met pays £425,000 to mother of undercover policeman's child. BBC News online. Retrieved from https://www.bbc.co.uk/news/uk-29743646

Lewis, P., Evans, R. & Pollak, S. (2013, 24 June). Trauma of spy's girlfriend: 'like being raped by the state'. *The Guardian*. Retrieved from https://www.theguardian.com/uk/2013/jun/24/undercover-police-spy-girlfriend-child

Loftus, B., Goold, B. & Mac Giollabhuí, S. (2016). From a visible spectacle to an invisible presence: The working culture of covert policing, *British Journal of Criminology*, *56*(4), 629–645. https://doi.org/10.1093/bjc/azv076

Lubbers, E. (2015). Undercover research: Corporate and police spying on activists. An introduction to activist intelligence as a new field of surveillance. *Surveillance & Society*, *13*(3/4), 338–353. https://doi.org/10.24908/ss.v13i3/4.5371

McStay, A. (2018). *Emotional AI: The rise of empathic media*. London, UK: SAGE Publications.

McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data & Society*, *7*(1), 205395172090438. https://doi.org/10.1177/2053951720904386

Macnish, K.N.J. (2015). An eye for an eye: Proportionality and surveillance. *Ethical Theory and Moral Practice*, *18*(3), 529–548. https://doi.org/10.1007/s10677-014-9537-5

Manolev, J., Sullivan, A., & Slee, R. (2019). The datafication of discipline: ClassDojo, surveillance and a performative classroom culture. *Learning, Media and Technology*, *44*(1), 36–51. https://doi.org/10.1080/17439884.2018.1558237

Marx, G. T. (1974). Thoughts on a neglected category of social movement participant: The agent provocateur and the informant. *American Journal of Sociology*, *80*(2), 402–442. https://doi.org/10.1086/225807

Murgia, M. (2021, 12 May). Emotion recognition: Can AI detect human feelings from a face? *Financial Times.* Retrieved from https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452?shareType=nongift

Murphy, H. (2021, 9 June). How the FBI's Trojan Shield operation exposed a criminal underworld. *Financial Times*. Retrieved from https://www.ft.com/content/65ed6eb5-4968-4636-99bc-27a516d089dd

Newman, L. (2021, 11 June). The FBI's Anom stunt rattles the encryption debate. *Wired*. Retrieved from https://www.wired.com/story/fbi-anom-phone-network-encryption-debate/

Rosenbaum, M. (2005). Tracking the anti-apartheid groups. BBC News online. Retrieved from http://news.bbc.co.uk/1/hi/uk_politics/4285964.stm

Schlembach, R. (2018). Undercover policing and the spectre of 'domestic extremism': the covert surveillance of environmental activism in Britain. *Social Movement Studies*, *17*(5), 491–506. https://doi.org/10.1080/14742837.2018.1480934

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. New York, US: W.W. Norton.

Security Service (undated). FAQs about MI5: Does MI5 investigate trade unions and pressure groups? Retrieved from https://www.mi5.gov.uk/faq/what-is-the-difference-between-mi5-and-mi6-sis

Seedhouse, D. (2009). *Ethics: The heart of health care*. Third edition. Chichester, UK: Wiley.

Stephens Griffin, N. (2020). 'Everyone was questioning everything': Understanding the derailing impact of undercover policing on the lives of UK environmentalists. *Social Movement Studies*, 1–19. Advance online publication. https://doi.org/10.1080/14742837.2020.1770073

Swanston, T. (2021, 9 June). Australia's 'very weak' privacy protection may be behind key role in global operation against organised crime. ABC News. Retrieved from https://www.abc.net.au/news/2021-06-10/nsw-operation-ironside-privacy-in-wake-of-afp-raids/100202924

Thompson, T. (2010, 14 March). Inside the lonely and violent world of the Yard's elite undercover unit. *The Guardian.* Retrieved from https://www.theguardian.com/uk/2010/mar/14/undercover-police-far-left-secret

Tucker, I. (2013). Bodies and surveillance: Simondon, information and affect. *Distinktion: Scandinavian Journal of Social Theory*, *14*(1), 37–41. https://doi.org/10.1080/1600910X.2013.766225

United States Department of Justice (2021, 8 June). FBI's encrypted phone platform infiltrated hundreds of criminal syndicates; Result is massive worldwide takedown. Retrieved from https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Williamson, B., Potter, J., & Eynon, R. (2019). New research problems and agendas in learning, media and technology: The editors' wishlist. *Learning, Media and Technology*, *44*(2), 87–91. https://doi.org/10.1080/17439884.2019.1614953

Williamson, B., (2021, May 28). *Google's plans to bring AI to education make its dominance in classrooms more alarming*. Fast Company. Retrieved from https://www.fastcompany.com/90641049/google-education-classroom-ai

Wilson, K. (2021). Kate Wilson: After spy cops case the Met is beyond redemption. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2021/sep/30/kate-wilson-after-spy-cops-case-the-met-is-beyond-redemption

Wilson v (1) Commissioner of Police of The Metropolis (2) National Police Chiefs' Council (2021, 30 September). IPT/11/167/H. Retrieved from https://www.ipt-uk.com/judgments.asp?id=61

Witness, Z. (2021, 22 March). First witness statement of Security Service Witness Z. Undercover Policing Inquiry. Retrieved from https://www.ucpi.org.uk/publications/first-witness-statement-of-security-service-witness-z/

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, US: Public Affairs.