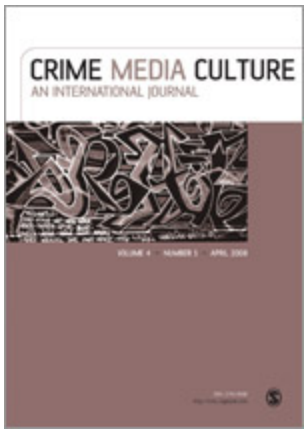

Information security for criminological ethnographers

Journal:	*Crime, Media, Culture*
Manuscript ID	CMC-22-0041.R2
Manuscript Type:	Journal Article
Keywords:	ethnography, methodology, ethics, information security, digital security, surveillance, encryption, privacy, anonymity, threat modelling
Abstract:	Information security refers to 'the practice of defending information from unauthorised access'. Information security practices include everyday activities such as protecting your bank details, or keeping your workplace logins secure. Despite increasingly restrictive approaches to research ethics, academia continues to lag behind journalism when it comes to best practice with regards to information security. This article discusses information security as it pertains to qualitative and especially ethnographic research into crime and deviance. In doing so, the article addresses a gap in the methodological literature by drawing on lessons and real-world examples from journalism, academia and activism, in order to offer guidance for researchers seeking to maintain information security in a digital, networked social world. The article proceeds in three parts. First, the article considers what information researchers might want to protect, who they might want to protect it from, and what the consequences might be if they failed to do so (an exercise known as 'threat modelling'). The different powers, resources and capacities of, and threats posed by, state actors such as the police and intelligence agencies, as well as an array of non-state actors, are considered. Second, the article outlines some general principles of information security and how they might apply to ethnographic research into crime and deviance. Third, the article discusses a range of practical considerations when it comes to using mobile phones (cell phones), social media, passwords and encryption in the course of researching crime and deviance.

Information security for criminological ethnographers

Introduction

Information security refers to 'the practice of defending information from unauthorised access' (Carlo and Kamphuis, 2016: 6). Information security practices include everyday activities such as protecting your bank details or keeping your workplace logins secure. Here, our particular interest is in protecting data acquired in the course of qualitative and especially ethnographic research into crime and deviance. This can include communications with respondents, fieldnotes, recorded interviews and transcripts. These same principles also relate to researchers managing leaked, stolen or illegal secondary data, such as BlueLeaks, a massive leak of U.S. law enforcement data (see Lee, 2020).

Our interest in information security stems from our experience of researching illegal and deviant activities. Kindynis has spent several years undertaking ethnographies of graffiti writers and urban explorers in London (Kindynis, 2017; 2018). Fleetwood spent 16 months in prisons in Ecuador undertaking ethnographic interviews with people convicted of drug trafficking (2014a). She has also interviewed women involved in the street level drug trade (2014b). While we do not claim to always get it right, we hope that sharing what we have learned about information security will prove useful for the reader.

This article addresses a gap in methodological literature. Raymond Lee's (1993, 1995) discussions of sensitive topics and dangerous fieldwork are peerless but outdated. Now several decades old, Lee's discussions are limited to analogue data, discussing notebooks and tape recorders. Universities and government institutions provide guidance on digital data but tend to be preoccupied with data backup and security (see Corti et al., 2019; UK Data Service, 2021), offering almost no discussion relevant to those researching sensitive or illegal activities. For many academics, questions of data security – where they are encountered at all – are often subsumed under the problematic rubric of institutional research ethics. Several commentators have suggested that institutional review of ethics 'has degenerated into risk management' amidst an institutional framework in which the need to defend against litigation and scandal is palpable (Ancrum, 2013: 115; Haggerty 2004). For example, standard guidance from Universities is that research data be stored on University servers or University-owned and secured devices, which may not be appropriate for criminologists. The following discussion of information security in fieldwork on crime and deviance is therefore well overdue.

This article updates Lee's (1993, 1995) advice for researchers reflecting the widespread use of digital and networked devices (such as phones and laptops) in qualitative research in research on crime, deviance or sensitive topics. Academia lags behind journalism in developing best practice regarding information security. The 2013 disclosures by Edward Snowden revealed the unprecedented extent of state surveillance in the digital age. The Centre for Investigative Journalism's *Information Security for Journalists* (2014) offers in-depth technical advice for journalists regarding government interference and is highly relevant for anyone researching state crimes or working with sensitive documents. We can also highly recommend the Electronic Frontier Foundation's (no date) guide, which offers technical guidance on using electronic devices. We draw on these throughout, but readers are encouraged to take this article as a starting point in their reading and to always seek out up to date best practice.

This article sketches out the principles of information security for academic researchers. By 'information security' we mean protecting research material from unauthorised access. There is no 'one size fits all' for all projects and so we intend this article as a resource for academics producing or collecting data on sensitive topics, especially ethnographers of crime and deviance. We hope that this article can help researchers, and especially criminological ethnographers, to make informed decisions about how they can best – in concrete, practical terms – protect themselves and their research participants.

The article is structured as follows. First, we introduce the language of threat assessment, and outline the main state and non-state 'adversaries' and how they might seek to access our data. For criminologists, the state (police, courts and security agencies) are significant adversaries, but non-state actors are also important. Next, we outline some general information security principles for academic researchers, discussing compartmentalisation, obfuscation, 'need-to-know' and de-jeopardising strategies. These are overarching and enduring guidelines that will outlast, for instance, the specifics of how to safely use certain devices and software at any given point in time. Lastly, we discuss the challenges posed by the now ubiquitous use of mobile phones (cell phones) and social media, as well as offering some concrete guidance on passwords and encryption. We conclude by reflecting on the overlap between information security and so-called operational security practices in the real world. Our data does not exist in a vacuum and good information security practice does not begin or end on your laptop or phone screen.

Threat modelling

In thinking about how to keep research data secure, it helps to first ask questions such as *what* information we want to protect, *who* we want to protect it from, *what* are their capabilities, *how likely* it is that we will need to protect it, and what the *consequences* might be if we fail to do so (Electronic Frontier Foundation, no date). This is called 'threat modelling':

> A way of thinking about the sorts of protection you want for your data so you can decide which potential threats you are going to take seriously. It's impossible to protect against every kind of trick or adversary, so you should concentrate on which people might want your data, what they might want from it, and how they might get it. (Electronic Frontier Foundation, no date, np; see also Kazansky, 2021).

Here, we are concerned with both research data and data about our research participants. This might include recordings of interviews, transcripts, text messages, emails, phone call records and more.

In our assessment, the information security threats facing academics broadly fall into two categories: first, the legal and other threats posed by agents of the state and its criminal justice apparatus; and second, the threats posed by various non-state actors. The state has different powers, resources and capacities to other adversaries. Police forces are, for instance, able to access cell site data and call records, which could possibly be used to build a case for legal summons, or as evidence in court. However, in the era of open-source intelligence, private spying and a booming illegal trade in personal data, the distinctions between the capacities of state and non-state actors are becoming increasingly blurred (Higgins, 2021; Meier, 2021). While threats posed by such adversaries are not new, they take on new forms and vectors in a digital, networked social world. Next, we examine some of the main adversaries that criminological researchers might face, the threats they might pose, and how they might seek to access our data.

State actors: Law enforcement and legal threats

For researchers studying crime and deviance, the primary adversary (in information security terms) is likely to be law enforcement seeking to gain access to research material

about our respondents. As Polsky (1967) states, researchers undertaking field research on crime and deviance may sooner or later encounter the police in their fieldwork. Jeff Ferrell (1995) was arrested and tried for graffiti vandalism, reflecting his commitment to active participant observation. Rizwaan Sabir (a PhD student at the University of Nottingham researching the evolution of global militant Islam) was held in police custody for a week before being released without charge, after downloading an Al Qaeda training manual and emailing it to a fellow student (BBC News, 2011).

It is worth stating at the outset that, at least in the British context, academic researchers have none of the protections afforded to journalists or their sources, although at the time of writing, these protections are under renewed threat (Campbell and Campbell, 2021). In the USA, researchers receiving National Institute of Justice funding can apply for a 'Privacy Certificate' offering legal protections of confidentiality (see National Institute for Justice, 2007). Nonetheless, such certificates do not provide absolute guarantees (however, see Beskow et al., 2008).[1]

Police

Researchers studying street drug markets report being questioned, harassed, and arrested by police (Bourgois, 2003: 30; Ancrum, 2013; Ferrell, 1995). Likewise, those researching protests or social movements may come into contact with police (i.e. Scarce, 1994). Being questioned by the police or even arrested may be no bad thing given that researchers are often suspected of working for the police (Lee, 1995; Bourgeois, 2003). Williams et al. (in Lee, 1995: 47) suggest that it is better to get arrested with respondents, only identifying yourself at the booking process. Since one hazard of getting arrested is that police may learn about sensitive research, it may be better not to identify oneself as a researcher. In Kindynis' experience, telling arresting officers that you are studying a PhD in criminology - and perhaps implying in their mind that you think you know more than they do about police work - is unlikely to do one any favours. In 2022, London Metropolitan Police settled with Koshka Duff after she was strip searched after she gave a 'know your rights' card to a teenager who was being stopped and searched by the police (BBC News 2022).

It is good practice for researchers to obtain the contact details of a relevant criminal

[1] Beskow et al. (2008) describe how, in one case, the judge ruled that attorneys (but no one else in court) could see research data relating to the case. This amounted to a limited breach of confidentiality.

defence specialist and should they be arrested and interviewed by the police, seek legal advice. Researchers should give “no comment” in interviews to avoid inadvertently incriminating themselves or participants (in England and Wales see Legal Defence & Monitoring Group, 2014). There are exceptions to this rule. For example, those detained under Schedule 7 of the 20002 Terrorism Act are prohibited from remaining silent or answering “no comment” (and it is a criminal offence to do so). Whilst this might run contrary to academic verbosity, researchers should avoid giving police reason to believe that they are in possession of material relevant to a criminal case, enabling police to initiate proceedings to access research data. Likewise, should you be arrested, police may request the passcode to access your phone. In England and Wales you can refuse, compelling police to seek a warrant from a judge (Wellsburcombe solicitors, no date). Nonetheless, new technologies increasingly mean that police can download the contents of digital devices, even without your permission (more on this below).

Court summons and subpoena

Police and courts can apply for access to researcher’s data and have done so in the UK, Canada and the USA (Elliott and Fleetwood, 2017; Dekeyser and Garrett, 2018; Trace 1993). For example, Rik Scarce (1994) spent 159 days in prison after refusing to identify his respondents (animal rights activists). Scott Demuth was charged with contempt of court and then a terrorism charge after refusing to identify his research respondents who were animal rights activists (Fillion 2009, see also Dekeyser and Garrett, 2018: 414). Recently, the USA’s Department of Justice threatened to deploy a subpoena regarding researchers studying elections in Bolivia (Klippenstein and Grim, 2021). International treaties mean that foreign governments can formally request access to research data (Coomber, 2002a). Researchers at the University of Boston have been embroiled in legal proceedings relating to a request by the UK government to access oral history interviews with former Irish Republican Army and Ulster Volunteer Force members for nearly a decade (Breen-Smyth 2020).

In England and Wales, confidentiality is not enshrined in legislation but rather in common law (Corti et al., 2019, p.112). Researchers can be legally obliged to disclose information about respondents, or make available research data (Coomber, 2002b; British Society of Criminology, 2015) but usually only under limited and specific circumstances (Elliot and Fleetwood, 2017). Nonetheless, this represents a major threat in terms of the security of our data.

The case of Bradley Garrett, a geographer researching urban exploration, offers a

recent example of the considerable extent to which the state can intervene regarding researchers' data (and may help us identify how researchers might take steps to limit such risks). Garrett employed participant observation methods in his PhD on 'place hacking'. In 2012, as he travelled to the UK, Garrett was arrested by British Transport Police (BTP) to 'collect evidence for an investigation regarding criminal damage, burglary and assisting and encouraging an offence' (Garrett, 2013: 228). In England and Wales, to legally access researchers' data, police must apply to a court for a warrant (Elliott and Fleetwood 2017: 6-8). The court would have to be persuaded that there was material likely to be of interest to an ongoing investigation or criminal trial (Elliott and Fleetwood 2017: 5). Garrett's PhD thesis – replete with richly descriptive ethnographic vignettes (and photographs!) of Garrett and his participants' lawbreaking at a number of named and easily identifiable locations; and using aliases that were easily connected to individuals' real names and addresses – was likely used to apply for a warrant. Indeed, it would later become "Exhibit A" in a conspiracy case brought by BTP against the geographer and his research participants. In his book, Garrett recalls a police officer reading him sections of his thesis while he was in police custody, describing the content as 'very condemning' (2013: 229). Police also asked about his social media, having identified his online pseudonym and social media accounts. Following his arrest, Garrett wrote an ill-advised blog post styled as 'an Open Letter to the BTP', thumbing his nose at the Transport Police and invoicing them "for the work we have done exposing your network's security flaws" (Garrett, 2011). While not illegal, we do not recommend bragging about lawbreaking or taunting the authorities in public fora.

While Garrett was in custody in 2012, police raided his flat confiscating data-holding devices including laptops, notebooks, hard-drives, phones and camera equipment (2013: 229). Although Garrett describes refusing to give his passcode for his phone, courts have legal powers (Schedule 1 PACE; Regulation of Investigatory Powers Act 2000) to demand that data be provided to the court in a legible form, i.e. decrypted. Failure to do so could result in being in contempt of court (Elliott and Fleetwood, 2017: 7). Garrett's legal representatives argued that research data comprise 'special procedure material' and should be treated as confidential but this was not successful (see Elliott and Fleetwood 2017: 7). A witness summons (or in the USA a court subpoena) can also require a researcher to appear in court to answer questions. Failure to appear could result in a prison sentence of up to 3 months for contempt of court (Elliott and Fleetwood 2017: 8).

State security and surveillance

More rarely (to the best of our knowledge), state security agencies have accessed

researchers' data. During the cold war, anthropologists conducting research in Central America were a source of information for the Central Intelligence Agency (Lee, 1995: 36-37). Some were approached directly, but others were unwittingly involved (ibid). More recently, Matthew Hedges, a PhD student at Durham University, was detained for 6 months in the United Arab Emirates (UAE) on charges of spying, later downgraded to charges of handling sensitive information (BBC News, 2021). The UAE attorney general cited evidence from his electronic devices, as well as evidence from UAE intelligence and security forces (Emirates Centre for Human Rights, 2018).

Noting above that researchers like Garrett and Sabir were arrested as they arrived in the UK, researchers should consider border crossing a particular threat. Researchers crossing the US border can note that border agents can legally conduct searches of devices such as phones, laptops and hard drives (Bandari, Wessler and Yachot 2018). The Electronic Frontier Foundation's Surveillance Self Defense (no date) offers a comprehensive guide to data security at the US border. Sensible suggestions include reducing the amount of data you are carrying, backing up elsewhere in case devices are seized and uninstalling sensitive apps (i.e. messaging).

The border is also a key site of state power over academics, and we note the recent development of algorithmic surveillance. Eyal Weizman - an academic at Goldsmiths, University of London, was denied entry to the USA where he was due to give a talk. In a statement, Weizman explains:

> I went to the U.S. Embassy in London to apply for a visa. In my interview the officer informed me that *my authorization to travel had been revoked because the "algorithm" had identified a security threat.* He said he did not know what had triggered the algorithm but suggested that it could be something I was involved in, people I am or was in contact with, places to which I had travelled (had I recently been in Syria, Iran, Iraq, Yemen, or Somalia or met their nationals?), hotels at which I stayed, or a certain pattern of relations among these things. I was asked to supply the Embassy with additional information, including fifteen years of travel history, in particular where I had gone and who had paid for it. The officer said that Homeland Security's investigators could assess my case more promptly if I supplied the names of anyone in my network whom I believed might have triggered the algorithm. I declined to provide this information. (2020, our emphasis).

Weizman's rejection at the US border serves as a stark reminder that – even without being conscious of it – we generate a digital footprint that can be and is used for state surveillance. The introduction of algorithmic, automated surveillance presents a novel threat that readers should be conscious of. Nonetheless, noting Weizman's experience, it may be nearly impossible to anticipate or mitigate such algorithmic profiling.

Non-state actors

In addition to the legal threats posed by state actors, various non-state groups – from fascists, “anti-vaxxers” and so-called “men’s rights activists” to climate change deniers and “anti-woke” culture warriors – now also target researchers and their respondents for intimidation and discreditment. While such groups can rarely match the technological capacities or material resources wielded by the state and its security agencies, the risk of crowd-sourced targeted harassment should nonetheless be taken seriously. Instances of such harassment are on the rise internationally and range from online threats and hacking to “doxxing” (maliciously disclosing private information such as the target’s home address on public forums) and organised campaigns to discredit researchers’ work (Greyson et al., 2019). ‘More severe forms of harassment may pose physical danger to the researcher and their loved ones’ and ultimately, ‘fear of harassment may have a chilling effect’ on research (Marwick et al., 2016: 2).

Far-right activists in the Netherlands have recently visited the homes of several high-profile left-wing writers and left threatening messages (DutchNews.nl, 2021). Some academics and public health officials in Sweden have either stopped research or have needed police protection because of threats made by “anti-vaxx” conspiracists during the Covid-19 pandemic (Matthews, 2021). A British academic whose research explores the victim-blaming of women was recently subjected to thousands of coordinated abusive messages, including rape and death threats, from those aligned with the so-called "alt-right", "men’s rights activists", and "incels" (involuntary celibates), culminating in her personal computer being hacked (Flood, 2020). Likewise, racialised scholars report racist trolling and abuse online (Grundy, 2017). Such sexist and racist harassment is by no means a novel hazard (see Green et al. 1993; Sharp et al. 2006), however, it assumes new forms in our networked information society, where intimate personal details can be obtained and wielded at the touch of a button with devastating consequences (Greyson et al., 2019).

Security principles

Above we have outlined the main potential adversaries relevant to criminological research. Of course, not all the above will be relevant for each project. Next, in a threat assessment, it would be usual to consider the risk of an adversary trying to access our data. On the one hand, the risks seem low (only rarely do state or non-state actors access our data), but the

consequences for our respondents are potentially catastrophic. With this in mind, researchers can draw on information security principles to develop a security plan.

Compartmentalisation

Compartmentalisation is a general principle meaning keeping things separate to limit vulnerabilities to accidental loss, or threats from adversaries. First, **consider how much research data you need to carry with you**. During fieldwork, it may be sensible to keep only material from that particular day, archiving the remainder somewhere more secure to mitigate the threat from respondents, or other adversaries in the field (Sluka 1995: 286). This applies to digital material as much as paper records. However, keep in mind that devices such as mobile phones can also contain data about our research – i.e. phone call records, messaging and so on. Even if data was taken by an adversary, the minimum would be lost/disclosed. Fleetwood had her laptop stolen on a work trip which happened to have some research data on it. Fortunately documents and the laptop were password protected and anonymised (more below) reducing the likelihood of a data breach. Better practice would have been to keep research data separate from day-to-day business (for example on a password protected USB stick).

Second, **consider where to securely store research data.** Sluka (1995) who researched Irish paramilitary supporters, kept interview tapes in a hiding place away from his home. However, we would suggest that very sensitive data (i.e. interview recordings, contact details) that could identify participants should ideally be kept within sight until they can have been encrypted/de-identified (Carlo and Kamphuis, 2016: 17; see below). While transcriptions offer plausible deniability, recordings often identify respondents. Sluka recommends keeping fieldnotes under lock and key in a secure location away from the field (1995: 286). University offices are an obvious place, but not the most secure since University webpages routinely list our offices and lax campus security could make them an easy target. Adler and Adler (1993: 39), in their research on international cocaine traffickers, moved tapes between friends' homes.

This same principle can be applied when storing data electronically. For example, journalists working on the Panama papers used "air-gapped"[2] laptops (in this case, from

[2] A computer or network that is physically isolated from all other networks, including the Internet, is said to be "air-gapped" (Electronic Frontier Foundation, no date). This may be achieved by removing or disabling Wi-Fi or hardware connections – although in some instances it may be difficult to physically remove e.g. Wi-Fi components. Air gaps can be "jumped" by highly sophisticated adversaries so do not completely guarantee security (see Guri, 2021).

which Wi-Fi hardware had been physically removed), mitigating the risk of unauthorised access through the Internet (Carlo and Kamphuis 2014). Carlo and Kamphuis (2014, 2016) recommend that journalists use separate devices for personal and research uses, limiting the potential for accidental loss. Further, if a device is compromised, only a portion of data may lost/disclosed. Likewise, storing interviews separately to consent forms makes it much harder for an adversary to deduce respondents' identity. As we discuss further below, researchers can 'offload' data from devices storing it on e.g. external hard drives or USB sticks (which are also effectively air-gapped until they are connected to a networked device).

Universities tend to recommend storing research data on their own servers to guard against loss of an individual laptop (for example Corti et al., 2019; UK Data Service, 2021). While this might be suitable for some projects (or for anonymised, de-jeopardised data – more below), researchers identifying police/courts as potential adversaries may wish to store data off University servers. As we note below, online data is much harder to securely destroy and this may be relevant for some research projects. Furthermore, Universities may be less resistant to complying with law enforcement requests for research data. Much better is to securely backup data externally on a hard drive, USB stick or other media (these can be easily destroyed and you can have several as backup in different locations). Basic practical considerations for securing laptops and phones (i.e. encryption and passwords) are considered below.

Lastly, researchers have been known to simply misplace or even lose data (we are only human and accidents do happen). This is probably more likely than an adversary seeking out our data. Sluka (1995) describes one researcher accidentally leaving field notes behind at a respondents' house after a night of drinking while undertaking research. Taking the above steps would certainly limit the amount of data lost or disclosed, and the potential for someone finding it to be able to access it.

Need-to-know

An important rule for qualitative researchers of crime and deviance is to be selective in the information sought out and collected. As the University of Sheffield suggest, researchers:

> have a responsibility to themselves and their research collaborators, to avoid, where possible - and it may not always be possible - acquiring information that is likely to prove dangerous, compromising or otherwise problematic. In observing the above responsibilities, caution is particularly indicated with respect to what is recorded audio-visually, digitally and in writing. (2020: 3)

Consider carefully how much data you really need to collect or record. Researchers can avoid collecting personal data – this is identifying data, or data that relates to an identified or identifiable person (Corti et al., 2019: 113). This might include a person's full name, address, etc.[3] Most ethnographic research on deviant or criminal activity does not require recording surnames or addresses of respondents. While personal information is commonly collected on information/consent sheets and in receipts for any honorariums for taking part in research, Coomber argues that: 'Individuals committing acts of illegality shouldn't be asked to sign a declaration to that effect' (2002a, para 1.2). We tend not to use consent forms reflecting his advice. When researching women who sold heroin and crack cocaine, Fleetwood brought information sheets to her fieldwork, but not consent forms. Respondents insisted that researchers took information sheets away so they would not be seen by children or family. On the same project, University administrators agreed that respondents' signatures were not required to confirm receipt of honorariums ensuring that no identifying material was collected.

Researchers might also consider the kinds of information they seek out, and how they record it. Jeffrey Sluka, researching paramilitaries during the troubles in Northern Ireland "chose not to ask about some things such as weapons, finance and planned military operations, which I felt were unnecessary and potentially dangerous to both me and to other research participants" (1995: 279). Likewise, when he recorded interviews, Sluka 'tried to ensure that there was nothing on them that would directly identify an individual, particularly the interviewee' (1995: 282). When interviewing graffiti writers, Kindynis asked respondents to avoid discussing specific locations that might implicate them in particular instances of criminal damage. Some things are best committed to memory. We would suggest that it is perfectly possible to avoid ever committing respondents' real names to paper (and certainly not connected to their pseudonyms).

Researchers can also give thought to what is known publicly about them and their research. It can be a good general principle to limit who knows about sensitive or illegal

[3] Personal data is also covered by legal duties to comply with the Data Protection Act.

research. For example, Adler and Adler (1993: 39) did not publicly speak about their research on drug trafficking while they were undertaking fieldwork, delaying publication of articles until they had exited their fieldwork site. Jeffrey Sluka limited knowledge of his research on IRA supporters in Belfast to participants and a couple of trusted friends (1995). He was careful not to be seen with paramilitaries in order to avoid arousing suspicion from security agencies or the British Army, and was involved in two other academic research projects to give cover for his presence in the area.

In a contemporary context, researchers would do well to keep track of their online profile and that of their research project. After posting online about her project walking railway along lines near San Francisco, Naomi Adiv was visited by police at her University and told to halt her project (Garrett, 2013: 231). Without getting into a debate about covert research, we can note that we are more traceable than ever before. Facial recognition search engines can be used to identify people based on their photograph alone, presenting a real challenge for those wishing to undertake covert research. As Sluka writes: 'Being dishonest is more dangerous than being honest, because it creates the possibility of being caught out in a lie' (1995: 284-285). Researchers of crime report being accused of being a spy, or police (Lee, 1995; Sluka, 1995), and it may be useful to demonstrate one's academic credentials. Nonetheless, as we note above, researchers' online profiles may also make us vulnerable to being doxxed.

Obfuscation and dejeopardizing techniques

We have hopefully impressed on the reader that certain categories of information simply should not be recorded at all. However, it is the researcher's job to collect data. No matter how cautious, it is still possible that some of the information researchers record could prove useful to, for instance, law enforcement who are keen to develop a fuller picture of the inner workings of some movement, subculture or scene. We propose that researchers can further protect their respondents specifically, and more generally "the field" wherein their research takes place, by 'disutilising' their data (Lee, 1995: 37) as well as obfuscation, or what Lee terms 'dejeopardizing techniques' (1993: 82).

'Disutilisation' means minimising the potential usefulness of research for intelligence or law enforcement purposes (Lee, 1995:37), specifically by reducing its relevance, credibility and visibility. The kinds of information that researchers seek out is often quite distinct from the kinds of precise information likely to be useful in a criminal investigation or trial, and researchers can work in that gap. Again, the University of Sheffield are informative:

> Unless a researcher has actually seen an offence being committed, or can offer other hard proof of criminality - such as knowledge of the location of proscribed drugs, illegal weapons or stolen goods, for example - then most information that is garnered as research data would probably fall into the category of hearsay, if tested in court. (2020: 2).

With this in mind, we can focus on scholarly questions (not law enforcement questions), and aim to develop theoretical generalisations, rather than recording highly accurate, comprehensive and up to date information. As Van Maanen states: 'fieldnotes are gnomic, shorthand reconstructions of events, observations, and conversations that took place in the field. They are composed well after the fact as inexact notes to oneself and represent simply one of many levels of textualization set off by experience' (1988: 223). We might hope that fieldnotes would be of limited use in developing a legal case against our respondents. But we can also take steps to de-jeopardise or disutilise research data.

It is standard practice to anonymise our respondents in published or public data, but we **suggest anonymising data as early as possible** even in data collection.[4] Before commencing an interview, we can remind interviewees to avoid stating their full name, dates, particular places etc. Fieldnotes can use pseudonyms and include aide memoires for moments that might not bear recording. Transcription offers a further opportunity to redact identifying details. Whilst doing so may risk losing some of the fine-grained detail of ethnographic description, that may be the cost of prioritising our respondents' safety. Doing all of the above increases the chances that our data – should it ever see the inside a court room – might be dismissed as 'hearsay'.

Publications can protect respondents through obfuscation. Noting that police officers drew on Garrett's thesis to gather information, Kindynis made use of "composite characters" when recording and writing up his research on graffiti writers. Field notes and interview excerpts were assigned to different pseudonyms (i.e. compartmentalisation). In this way the published research was made less useful to law enforcement, while retaining its sociological "truth". Corti et al. suggest discussing with respondents whether data might be sensitive (2019: 28). Sluka's paramilitary respondents checked his final manuscript for

[4] Corti et al. (2019 p.123) recommend keeping a version of data which is not anonymised - the anonymised version is for archiving with UK data service). For sensitive research it might be better to keep all data pseudonymised and without sensitive information.

problematic material (1995). Whilst our respondents might have situated knowledge about threats to our data that we should consider, ultimately the responsibility remains with the researcher.

Obfuscation and de-jeopardising techniques might extend to authorship itself: one major step that researchers at risk of targeted harassment – e.g. those researching the far right – can take in order to ensure their safety is the creation of fictional personas, aliases or pseudonyms for use when engaging in public-facing activities. Indeed, this is now considered 'best practice' by a growing number of researchers (Massanari, 2018; Marwick et al., 2016). Doing so may also enable a researcher to publish key information to the public, saving theoretical sophistication for a later date. The brilliant participant observation *A Glasgow Gang Observed* (2013) was published pseudonymously by "James Patrick" (an anagram of the Glasgow neighbourhood Partick). Glasgow University was initially hesitant to accept his thesis, but with the help of a solicitor, Patrick argued that his thesis was neither libellous nor likely to present legal difficulties (2013). Nonetheless, his Department restricted access to his thesis and Patrick delayed publication for five years, enabling his respondents to move on from adolescence to early adulthood. Interestingly, few respondents wanted anonymity by that point (some requested colour photographs of themselves be printed – he declined). Those with experience of researching sensitive topics agree that some findings may not be publishable (Sluka 1995: 286) at least not in the short term (Adler 1993; Lee 1995). Patricia Adler did not even speak of her fieldwork publicly at the time and delayed publication of her book for several years (1983). Waiting until institutions close and people move on can mitigate the risk to respondents. Fleetwood delayed publishing on her field site until it had been closed. Lee summarises the problem: 'when they write up their research, researchers must walk a tightrope, careful neither to conceal too much, nor disclose too little' (Lee, 1993: 206). This balance will be different for each project.

Destroying or archiving fieldnotes and data

Alice Goffman deleted her fieldnotes and other data to protect her respondents but was criticised for doing so. Singal (2015) accused Goffman of falsifying aspects of her study, although she subsequently clarified that details were changed to appropriately anonymise her subjects (Neyfakh, 2015). While critics such as Singal seem to apply stringent, journalistic standards of transparency and fact-checking, such standards may be in tension with academic, ethical responsibilities to protect our subjects – often through anonymisation. For some projects, we think it may be appropriate to destroy fieldnotes.

However, a useful general principle is to **reflect on which data needs to be kept and why**. For legally sensitive research, interview recordings are best transcribed and destroyed as quickly as possible. As we describe above, this allows sensitive materials to be redacted to 'disutilise' the data (Lee, 1995: 37).

Destroying data is a technical process. The UK government standard for shredding confidential material on paper (DIN4) is pieces of 15x2mm (Corti et al., 2019: 96). Physical destruction is recommended for USB drives (ibid). Most universities have a facility for securely shredding paper and destroying technology. Data on hard drives can be overwritten to properly erase it, and a range of software is available to do this (Carlo and Kamphuis 2016; Corti et al., 2019: 96).

The main funding bodies in the UK ask for data to be archived, although this does not apply to PhD students (Corti et al., 2019: 124). Any material archived should be thoroughly anonymised, removing any identifying materials (ibid). Material archived with the UK data service is not in the public domain, however. Researchers can embargo data, and can also restrict who can access that data, including maintaining control over access (Corti et al., 2019: 124). Nonetheless, researchers should consider carefully whether legally sensitive data should be archived at all. Once data is lodged with a third party, it could be harder to resist attempts to seize data under legal procedures (described above).

In the UK, PhD theses are routinely archived and made publicly available through the British Library's ethos site (e-theses online search). Rapid, open-access publication is laudable. Nonetheless, in the case of legally or otherwise sensitive research, publication can be delayed by requesting an embargo which effectively restricts access for a period of time – much like Patrick's department did in the 1970s. We both placed our theses under embargo for several years. In Fleetwood's case, it became apparent that some respondents had been under state surveillance.[5] Embargo may not stand up to legal challenges, but it certainly makes research material harder to access and allows the researcher to contest legal attempts to access data.

Good information security practice for researchers

Above we drew on information security principles (compartmentalisation, need-to-know, obfuscation and de-jeopardisation techniques and destroying data) to develop some basic guidelines for researchers. Researchers can consider:

[5] One appeared as a 'case study' in an annual report of a policing organisation.

- how much data they need to collect (be mindful that electronic devices collect data in call records, messages etc.);
- compartmentalising data, and carrying around as little data as possible;
- anonymising or dis-utilising data an early stage;
- reflecting on which data needs to be kept and why;
- storing data securely.

This brief final section offers some notes on good information security practice for researchers regarding digital devices and social media. We intend this section as a starting point and readers are advised to seek out up-to-date guides online (i.e. Electronic Frontier Foundation, no date; Carlo and Kamphuis 2016; Geijer, 2022).

Mobile Phones (Cell Phones)

- Have a separate phone for research projects.
- Switch off the cloud and location services.
- Use secure messaging apps.

We use mobile phones routinely to communicate with respondents. Mobile phones can be a useful resource for fieldworker safety (Lee 1995: 63) but, in terms of information security, they present a range of issues.

A street campaign waged by an obscure, British artistic collective affixed stickers to London telephone boxes throughout the mid-1980s. The stickers read: “ASSUME THIS PHONE IS TAPPED”. Following the global surveillance disclosures made by former National Security Agency contractor Edward Snowden in 2013 (see, for example, Greenwald, 2013; Greenwald and MacAskill, 2013), and the 2021 Pegasus spyware revelations (Kirchgaessner et al., 2021; Priest et al., 2021), we no longer need assume. We now know that phones belonging to academics (al-Rasheed, 2021), activists and journalists have been targeted by spyware at the behest of autocratic regimes such as Saudi Arabia, as well as by non-state actors including the Mexican cartels (Lakhani, 2021). A successful infection by the spyware in question, Pegasus, developed by NSO Group, enables the user to remotely access everything on the target’s device, including contacts, chat messages, and precise location; and to activate the device’s cameras and microphones (Lakhani, 2021; Pegg and Cutler, 2021). There is a maxim in activist circles that one should “never say anything on the phone that you would not say in a court of law.”

A growing number of local police forces in the US and the UK are using mobile phone “extraction” tools such as Cellebrite’s GrayKey, enabling them to break passcodes and extract, store and analyse all of the content from people’s smartphones (Privacy International, 2018). The legal basis for this kind of "digital stop and search" is far from clear (Privacy International, 2018).

What is to be done? First, compartmentalise. **Have a separate phone for work and personal life** (Carlo and Kamphuis 2016). For extremely sensitive projects, this could even be a ‘burner’ phone (a cheap, and if needs be, disposable phone that is not registered to your address, is topped up using cash, and is unconnected to your identity). Be aware that cell phone networks track and log devices current and past locations which can be used to identify users (Electronic Frontier Foundation, no date). So, there is no point having a burner phone if you use it at home or work. When not in use, switch it off and remove the battery. A biscuit tin can function as a faraday cage, stopping remote access (even while switched off, phones still emit signals) (Carlo and Kamphuis 2016). Consider turning off cloud storage. As the saying goes, “the cloud is just someone else’s computer”. Is that someone else sufficiently motivated to protect your data? Consider disabling location services, Bluetooth, Wi-Fi, and NFC capabilities on burner phones to reduce the risk of signal interception (remotely) or device intrusion (if the device falls into the hands of, for example, law enforcement). These capacities represent potential vulnerabilities to be exploited in accessing your phone, and collect data that could unintentionally reveal information useful to adversaries were it to be accessed.

Avoid using SMS messages to communicate with respondents (Carlo and Kamphuis 2016). Your network provider can read the contents of any SMS messages you send and receive. Records of messages and their associated metadata are retained and can be subject to a warrant or subpoena in legal proceedings. Messages sent using apps like Signal are “end-to-end” encrypted, meaning that only the sender and receiver can read them. This protects messages from being intercepted in transit, but not if either party’s device is compromised (for instance, if seized by police or infected by spyware). Be aware that your phone number is shown to recipients, which could be used to identify you if it is publicly connected to your identity.

Whilst mobile phones can be used to record interviews, it is much better to use a digital recorder as it is effectively air-gapped, and it is much easier to destroy removable memory cards and overwrite data. AUTHOR 2 recommends using tapes for recording interviews – they are hard to duplicate, inaccessible via the internet, and can be easily destroyed (yes, they are still available to buy).

Social media

- Communications via social media are not secure;
- Think about what social media reveals about you.

Today, almost every aspect of social life is mediated by the Internet, especially though social media platforms such as Facebook, Twitter, Instagram and TikTok. Online and offline social worlds are increasingly and inextricably enmeshed (Potter 2017). Criminologists have engaged with the implications of such developments for our understanding of issues including surveillance and social control, social harm and victimisation (see, for example, Yar, 2012; Vitis and Gilmour, 2017; Wood, 2018; Williams and Burnap, 2016). There have also been several innovative methodological developments – in the field of digital ethnography (Coleman, 2014; Hine, 2015; see, for example, Wood, 2018; Anderdal Bakken and Kirstine Harder, 2022), as well as new forms of data collection and analysis (Gray and Benning, 2019; Ilan, 2020), and open-source investigative methods (Deutch and Habal, 2018; Weizman, 2019). Furthermore, it is undoubtedly the case that social media present unique opportunities for gaining access to prospective participants as well as disseminating research findings. However, the information security implications of social media for criminological researchers are less frequently considered.

Social media is an information security minefield, and we strongly recommend against communicating with participants using social media, and against any other casual use of social media in the course of sensitive research. Social media companies collect, analyse and share vast amounts of data on their users with advertisers, other tech companies, governments and law enforcement agencies. Concentration of ownership (for instance, Meta, the parent company of Facebook, also owns WhatsApp and Instagram) allows for the combination of users' data from different apps or platforms. Many social media companies proactively work with police. To give just one example, Project Alpha, the unit within the Metropolitan Police tasked with monitoring "gang related" social media activity, 'works collaboratively with Social Media platforms to identify and remove harmful content' (Mayor of London, 2021). Social media platforms' privacy settings give a false sense of security, since "private" posts, while perhaps not publicly searchable or viewable by other users are nevertheless accessible to the social media platforms, their staff, and any law enforcement agencies they choose to share it with. According to a legal complaint

recently filed in the US, Facebook's owner Meta has been accused of secretly keeping users' "deleted" messages and sharing them with police (Martin, 2022).

In addition to the kind of formal data sharing arrangements discussed above, the authorities and non-state actors alike are often able to glean a surprising amount of information from social media without the need for any kind of special access. Seemingly innocuous posts may inadvertently disclose far more information than they seem, allowing adversaries to deduce a users' relationships, routine or even whereabouts using open-source investigative techniques such as geolocation. In Kindynis' experience, both publicly viewable and private social media posts and messages have been presented by police whilst interviewing suspects, and as evidence in court in the prosecution of graffiti writers and urban explorers.

If you absolutely must use social media for research purposes, consider the potential information security risks posed and take precautions. You could use multiple, pseudonymous accounts for different elements of your research project. If you wish to conceal your identity from other users, these accounts should be completely firewalled from, and should never interact with any accounts you interact with from any personal social media accounts. Never use the same usernames or profile pictures as your other social media accounts. Take time to familiarise yourself with the privacy and security settings on different social media platforms (these are often difficult to find) and think carefully about what information you upload and what it could potentially, inadvertently reveal about you. Small pieces of biographical information, once pieced together, can potentially be used to build a more comprehensive picture of who you are.

Passwords

- Use secure passwords on phones and laptops.

University IT Departments can offer advice on secure passwords, but here we offer a pithy account. Turn off biometric access to devices such as facial recognition and fingerprint unlock. The police, or anyone else for that matter, can force you to unlock your phone using biometric authentication. Moreover, in some jurisdictions, biometrics offer less legal protection than passcodes (see Albergotti, 2014). Next, use a strong passcode. Four- and even six-digit numeric passcodes are vulnerable to "brute force" attacks (trying every possible combination) within a matter of days, whereas passcodes longer than 10 digits can take decades to crack. This is due to the exponential nature of the "cost" of cracking

passcodes (how long it takes).

For especially sensitive projects, more secure approaches might be required. Carlo and Kampuis suggest using a password manager such as KeePassX (2016: 67). This automatically generates long, random passwords and is a good option if you trust your laptop. It does require you to have one master password or passphrase. A passphrase is a sequence of words that is much longer and stronger than a traditional password, but easy to remember. You can generate a random password using the Schneier scheme, taking a memorable sentence and turning initials into numbers and symbols (Carlo and Kamphuis, 2016: 68). For example, 'this little piggy went to market' might become 'tlpWENT2m'. The "diceware" method provides another very secure option for generating long, random passphrases.[6] But, recall that police may have the power to demand you hand over passwords for devices.

Encryption for communications and research data

- Use encrypted, not University, email services;
- Turn on encryption on devices;
- Use encryption software if you need to send data.

Secure passwords are important but arguably somewhat "cosmetic". Without encrypting the data they protect, passwords can be bypassed by, e.g. removing your device's hard drive and accessing it directly.

First, communications. Encryption turns the text of messages into code that is very difficult for someone without permission to 'crack'. Whilst courts can demand that data be provided unencrypted, encrypting your data gives you much better protections against accidental disclosure or against a sophisticated non-state adversary. University email is not generally encrypted and can be read by people at the University. To state the obvious, it would be a bad idea to use your University email account to receive documents relating to BlueLeaks. Instead, compartmentalise: sign up for an encrypted email service such as Proton Mail.[7] At the time of writing, the gold standard for secure email is the Pretty Good Privacy (PGP) encryption program (see Electronic Frontier Foundation, no date; Carlo and Kamphuis 2016). However, PGP is unfortunately still somewhat complicated and time-consuming to use. If you are planning on contacting respondents by email, it is worth

[6] See https://www.eff.org/dice
[7] Be aware that only emails between Proton Mail users are end-to-end encrypted.

researching the most recent best practice for encrypted email. For example, Outlook now offers the option of encryption. As we note above, messaging apps such as Signal are encrypted.

Next, research data. Devices such as computer hard drives, external drives, USB drives and voice recorders can be set up for 'full-disk' encryption (this encrypts everything on the device). Apple's operating systems have inbuilt encryption, called FileVault, which works in the background once enabled. If working on other operating systems, or sending information between operating systems, Carlo and Kamphuis recommend using the open-source encryption software Veracrypt (2016: 37).

Reflection: Information security in the "real world"

Part of the difficulty with trying to limit the scope of this discussion to "information security" is the temptation to think of this as something that is managed from behind a screen: as having to do with passwords, and usernames and cookies and IP addresses. The problem, of course, is that in the era of "big data" and its monetisation, our behaviour in the "real world" – especially in the digital-and-physical hybrid space of cities such as London, which bristle with CCTV cameras and sensors – is increasingly rendered as data. The processes through which such information is gathered and analysed are opaque - black boxed - increasingly undertaken by algorithms (the sheer magnitude of data being gathered is too vast for humans to process). As Kazanksy writes, knowing 'how different institutions exploit data presents an ongoing challenge, requiring the expertise and power to untangle increasingly complex and opaque technological and institutional arrangements. The how and why of potential surveillance are thus wrapped in a form of continuously produced uncertainty' (2021: 1). Was it Eyal Weizman's flight patterns or bank transactions that lead the algorithm to flag him as a risk? Or, was someone in his call list under surveillance? We simply do not know. Indeed, there are countless possibilities since there is simply so much data collected about individuals in the course of everyday life. The traces of our digital behaviour begin to bleed into the physical with cell site metadata, ATM transactions, Automatic Number Plate Recognition systems and "smart" card and key access to public transport, our offices and homes. Ultimately, maintaining information security requires us to reflect on our behaviour, movement, interactions and communication in new and challenging ways.

Conclusion

As Lee says, ‘dangers are never totally manageable and, as with anyone else, researchers can be unlucky’ (1995: 9). Nonetheless, the risks of research on crime and illegal activities are often exaggerated (Polsky 1967; Lee 1995). Our aim is to take a clear-eyed look at the possible threats to our data in our networked world.

Good information security is essential for those researching crime, deviance, activism and protest, but all researchers should have a basic working knowledge of good practice. We increasingly rely on digital and networked devices for communicating with respondents, recording and storing interviews, fieldnotes and more. Whilst these technologies come with myriad benefits for researchers, we ought to properly understand and mitigate the risks of using such technologies. We owe it to our respondents – and ourselves – to manage these devices and their data in ways that reflect our status as professional researchers. This article sketches out some principles of information security for academic researchers, drawing on Carlo and Kamphuis’ (2016) Information Security for Journalists, and the Electronic Frontier Foundation’s guide to Surveillance Self Defense (no date). There can be no ‘one size fits all’ solution and individual researchers need to plan ahead, reflect on the possible threats to their data during and after fieldwork, and consider the level of information security measures required to reasonably defend against threats to data. Sluka advises, ‘it is no doubt better to be a bit paranoid about such things than it is to be a bit complacent about them’ (1995: 288).

References

al-Rasheed, M. (2021) 'Pegasus Project: Why I was targeted by Israeli spyware', *Middle East Eye*, 20 July. Available at: https://www.middleeasteye.net/opinion/pegasus-israel-saudi-arabia-why-targeted-spyware (Accessed 30 July 2021).

Albergotti, R. (2014) 'Judge rules suspect can be required to unlock phone with fingerprint', *Wall Street Journal*, 31 October. Available at: https://www.wsj.com/articles/BL-DGB-38641 (Accessed 29 July 2021).

Ancrum, C (2013) Stalking the margins of legality: Ethnography, participant observation and the post-modern 'underworld'. In: Winlow, S. and Atkinson, R. (eds.) New Directions in Crime and Deviancy. London: Taylor and Francis, pp. 113-126.

Anderdal Bakken, S. and Kirstine Harder, S. (2022) 'From dealing to influencing: Online marketing of cannabis on Instagram', *Crime, Media, Culture*, p. 17416590221081166. Available at: https://doi.org/10.1177/17416590221081166.

Bandari, E., Wessler, N.F., and Yachot, N. 2018. Can border agents search your electronic devices? It's complicated. https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/can-border-agents-search-your-electronic [accessed 29th July 2021].

Barton, G. and Poitras, L. (2013) 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', *The Washington Post*, 6 June. Available at: https://web.archive.org/web/20130824083615/http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers (Accessed 27 July 2021).

BBC News. 2022. Koshka Duff: Professor says she faced victim blaming over police claim. 26th January. https://www.bbc.co.uk/news/uk-60141559 [accessed 7th September 2022].

BBC News 2021. Matthew Hedges: UK academic files claims over UAE 'torture'. BBC News. 5th May. https://www.bbc.co.uk/news/uk-england-tyne-56998407

BBC News. 2011. Police Agree £20,000 payment over Rizwan Sabir arrest. 14th September. https://www.bbc.co.uk/news/uk-england-nottinghamshire-14923411 [accessed 27th July 2021].

Beskow, L.M., Dame, L. and Costello, E.J., 2008. Certificates of confidentiality and the compelled disclosure of research data. Science (New York, NY), 322: 1054-1055.

Breen-Smyth, M., 2020. Interviewing combatants: lessons from the Boston College Case.

Contemporary Social Science, 15(2), pp.258-274.

British Society of Criminology. (2015) Statement of Ethics, 2015. https://www.britsoccrim.org/documents/BSCEthics2015.pdf

Campbell, D. and Campbell, D. (2021) How a proposed secrecy law would recast journalism as spying. 20th July. *The Guardian.* https://www.theguardian.com/commentisfree/2021/jul/20/proposed-secrecy-law-journalism-spying-home-office-public-interest-whistleblowing

Carlo, S. and Kamphuis, A. (2014) Information Security for Journalists. Version 1. Commissioned by the Centre for Investigative Journalism.

Carlo, S. and Kamphuis, A. (2016) I*nformation Security for Journalists*. Version 1.3. Commissioned by the Centre for Investigative Journalism.

Carter, C. (2014) 'Academic prosecuted for exploring forbidden Britain', The Telegraph, 23 May.

Coleman, G. (2014) *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London, UK: Verso.

Coomber, R. (2002a) Signing your life away? Why Research Ethics Committees (REC) shouldn't always require written confirmation that participants in research have been informed of the aims of a study and their rights–the case of criminal populations. (Commentary). *Sociological Research Online* 7(1).

Coomber, R. (2002b) Protecting our research subjects, our data and ourselves from respective prosecution, seizure and summons/ subpoena. *Addiction Research & Theory* 10(1): 1–5.

Corti, L., Van den Eynden, V., Bishop, L. and Woollard, M., 2019. *Managing and sharing research data: a guide to good practic*e. London: Sage.

Cuevas, J. A. (2018) 'A new reality? The far right's use of cyberharassment against academics', Academe,

Dekeyser, T. and Garrett, B.L., 2018. Ethics≠ law. Area, 50(3), pp.410-417.

Deutch, J. and Habal, H. (2018) 'The Syrian Archive: A Methodological Case Study of Open-Source Investigation of State Crime Using Video Evidence from Social Media Platforms', *State Crime Journal*, 7(1), pp. 46–76. Available at: https://doi.org/10.13169/statecrime.7.1.0046.

DutchNews.nl (2021) 'Public prosecutor to investigate far right agitators Vizier op Links', *DutchNews.nl*, 26 May. Available at: https://www.dutchnews.nl/news/2021/05/public-prosecutor-to-investigate-far-right-agitators-vizier-op-links/ (Accessed 27 July 2021).

Electronic Frontier Foundation (no date). Surveillance Self Defense. Available at https://ssd.eff.org. Accessed 13 July 2021.

Elliott, T. and Fleetwood, J., 2017. Law for ethnographers. Methodological Innovations, 10(1), p.2059799117720607.

Emirates Centre for Human Rights. 2018. UAE talking to UK over spying charge for Matthew Hedges. 18th October. Emirates Centre for Human Rights. https://echr.org.uk/uk-talking-to-uae-over-spying-charge-for-matthew-hedges/ [accessed 27th July 2021].

Ethics Policy Note no. 12. https://www.sheffield.ac.uk/polopoly_fs/1.112762!/file/Research-Ethics-Policy-Note-12.pdf

Ferrell, J., 1995. Urban graffiti: Crime, control, and resistance. *Youth & Society*, *27*(1), pp.73-92.

Fillion, E. 2019. Encrypt Now: Research Ethics and Digital Security. https://www.concordia.ca/cunews/offices/vprgs/sgs/public-scholars-18/2019/01/08/encrypt-now-research-ethics-and-digital-security.html

Flood, A. (2020) 'Author of book about victim blaming bombarded with misogynist abuse', The Guardian, 24 April. Available at: https://www.theguardian.com/books/2020/apr/24/author-book-victim-blaming-misogynist-abuse-jessica-taylor (Accessed 27 July 2021).

Garrett, B. 2013. *Explore everything: Place Hacking the City*. London: Verso.

Garrett, B. L. 2011. 'Finding Common Ground: an Open Letter to BTP', *Place Hacking*, 27 June. Available at: https://web.archive.org/web/20110719073617/https://www.placehacking.co.uk/2011/06/27/finding-common-ground-open-letter-btp/ (Accessed 27 July 2021).

Gray, G. and Benning, B. (2019) 'Crowdsourcing Criminology: Social Media and Citizen Policing in Missing Person Cases', *SAGE Open*, 9(4), p. 2158244019893700. Available at: https://doi.org/10.1177/2158244019893700.

Green, G., Barbour, R.S., Barnard, M. and Kitzinger, J., 1993, November. "Who wears the trousers?": Sexual harassment in research settings. In Women's Studies International Forum 16(6): 627-637.

Greenwald, G. (2013) 'NSA collecting phone records of millions of Verizon customers daily', *The Guardian*, 6 June. Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (Accessed 27 July 2021).

Greenwald, G. and MacAskill, E. (2013) 'NSA Prism program taps in to user data of Apple,

Google and others', *the Guardian*, 7 June. Available at: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (Accessed: 28 July 2021).

Greyson, D., Cooke, N., Gibson, A. and Julien, H. (2019) 'Online targeting of researchers/academics: Ethical obligations and best practices, Proceedings of the Association for Information Science and Technology, 55(1): 684 – 687.

Grundy, S., 2017. A history of white violence tells us attacks on black academics are not ending (I know because it happened to me). Ethnic and Racial Studies, 40(11), pp.1864-1871.

Geijer, H. (2022) Mobile Phone Security for Activists and Agitators. Available at: https://opsec.riotmedicine.net/downloads/ (Accessed 26 July 2022).

Guri, M. (2021) Air-Gap Research Page. Advanced Cyber-Security Research Lab. Cyber-Security Research Center. Ben-Gurion University of the Negev. Available at: https://cyber.bgu.ac.il//advanced-cyber/airgap (Accessed 20 July 2022).

Haggerty, K.D., 2004. Ethics creep: Governing social science research in the name of ethics. Qualitative sociology, 27(4), pp.391-414.

Higgins, E. (2021) *We Are Bellingcat: An Intelligence Agency for the People*. London: Bloomsbury.

Hine, C. (2015) *Ethnography for the Internet: Embedded, Embodied and Everyday*. Routledge.

Ilan, J. (2020) 'Digital Street Culture Decoded: Why criminalizing drill music is Street Illiterate and Counterproductive', *The British Journal of Criminology*, 60(4), pp. 994–1013. Available at: https://doi.org/10.1093/bjc/azz086.

Fleetwood, J. (2014a) *Drug Mules: Women in the International Cocaine Trade*. Basingtoke: Palgrave Macmillan.

Fleetwood, J. (2014b) 'Keeping out of trouble: Female crack cocaine dealers in England', *European Journal of Criminology*, 11(1): 91 – 109.

Kazansky, B. (2021) ''It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance', Big Data & Society, 8(1): 1 - 12.

Kindynis, T. (2017) 'Urban Exploration: From Subterranea to Spectacle', *British Journal of Criminology*, 57(4): 982 – 1001.

Kindynis, T. (2018) 'Bomb Alert: Graffiti Writing and Urban Space in London', *British Journal of Criminology*, 58(3): 511 – 528.

Klippenstein, K and Grim, R. 2021. DOJ threatened MIT researchers with subpoena in collaboration with Bolivian Coup Regime. *The Intercept.* 4th May.

https://theintercept.com/2021/05/04/bolivia-coup-trump-mit-evo-morales/ [accessed 27th July].

Lakhani, N. (2021) 'Revealed: murdered journalist's number selected by Mexican NSO client', *The Guardian*, 18 July. Available at: https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto

Lee, M. (2020) 'Hack of 251 Law Enforcement Websites Exposes Personal Data of 700,000 Cops', *The Intercept*, 15 July. Available at: https://theintercept.com/2020/07/15/blueleaks-anonymous-ddos-law-enforcement-hack/ (Accessed: 27 September 2022).

Lee, R. M. (1993). *Doing research on sensitive topics*. Sage.

Lee, R. M. (1995). *Dangerous fieldwork*. Sage.

Legal Defence & Monitoring Group (2014) No Comment: The Defendant's Guide to Arrest. 5th edition. London: LDMG.

Martin, A. (2022) 'Facebook accused of secretly saving deleted Messenger data and sharing it with police', *Sky News*, 8 July. Available at: https://news.sky.com/story/facebook-accused-of-saving-deleted-messenger-data-and-sharing-it-with-police-12648081 (Accessed 28 July 2022).

Marwick, A. E., Blackwell, L., & Lo, K. (2016) Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment. New York, NY: Data & Society Research Institute. Available at: https://datasociety.net/pubs/res/Best_Practices_for_Conducting_Risky_Research-Oct-2016.pdf

Massanari, A. L. (2018) 'Rethinking research ethics, power and the risk of visibility in the era of the "alt-right" gaze', Social Media + Society, April-June: 1 – 9.

Matthews, D. (2021) 'Sweden mulls law change to fight online hate against researchers', *Times Higher Education*, 1 March. Available at: https://www.timeshighereducation.com/news/sweden-mulls-law-change-fight-online-hate-against-researchers (Accessed 27 July 2021).

Mayor of London (2021) 'Videos and content flagged by social media companies to the Met (1)', 16 December. Available at: https://www.london.gov.uk/questions/2021/5071 (Accessed 28 July 2022).

Meier, B. (2021) *Spooked: The Secret Rise of Private Spies*. London: Hodder and Stoughton.

National Institute for Justice. (2007) Confidentiality and Privacy protections.

https://nij.ojp.gov/funding/confidentiality-and-privacy-protections

Neyfakh, L. (2015) The Ethics of Ethnography. Slate. June 18th. https://slate.com/news-and-politics/2015/06/alice-goffmans-on-the-run-is-the-sociologist-to-blame-for-the-inconsistencies-in-her-book.html

Patrick, J. (2013) *A Glasgow Gang Observed*. Glasgow: Neil Wilson Publishing.

Pegg, D. and Cutler, S. (2021) 'What is Pegasus spyware and how does it hack phones?', *The Guardian*, 18 July. Available at: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones (Accessed 30 July 2021).

Polsky, N. (1967) *Hustlers, Beats and Others.* Transaction Publishers.

Potter, G.R., 2017. Real gates to virtual fields: Integrating online and offline ethnography in studying cannabis cultivation and reflections on the applicability of this approach in criminological ethnography more generally. Methodological Innovations, 10(1), p.1-11.

Priest, D., Timberg, C. and Mekhennet, S. (2021) 'Private Israeli spyware used to hack cellphones of journalists, activists worldwide', *Washington Post*. Available at: https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/ (Accessed: 27 July 2021).

Privacy International (2018) Digital stop and search: how the UK police can secretly download everything from your mobile phone. Available at: https://www.privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile (Accessed 29 July 2021).

Scarce, R. (1994) No Trial (But) Tribulations: When Courts and Ethnography Conflict. *Journal of Contemporary Ethnography*, 23 (20): 123-149.

Sharp, G. and Kremer, E., 2006. The safety dance: Confronting harassment, intimidation, and violence in the field. Sociological methodology, 36(1), pp.317-327.

Shuchman, M., (2014) Researcher-participant confidentiality now a formal concept in Canadian law. *CMAJ*, 186 (4) 250-251.

Singal, J. (2015) 'The Internet Accused Alice Goffman of Faking Details in Her Study of a Black Neighborhood. I Went to Philadelphia to Check.' *The Cut*, 18th June. https://www.thecut.com/2015/06/i-fact-checked-alice-goffman-with-her-subjects.html [accessed 8th July 2021].

Sluka, J. (1995) 'Reflections on managing danger in fieldwork: Dangerous Anthropology in Belfast' in Nordstrom, C. and Robben, A.C. eds. *Fieldwork under fire: Contemporary studies of violence and culture*. University of California Press.

The University of Sheffield (2020) Research Involving Illegal Activities. Research

UK Data Service. (2021). *Prepare and Manage Data*. https://www.ukdataservice.ac.uk/manage-data.aspx

Vitis, L. and Gilmour, F. (2017) 'Dick pics on blast: A woman's resistance to online sexual harassment using humour, art and Instagram', *Crime, Media, Culture*, 13(3), pp. 335–355. Available at: https://doi.org/10.1177/1741659016652445.

Weizman, E. (2019) 'Open verification'. E-Flux, June 2019. Available at: https://www.e-flux.com/architecture/becoming-digital/248062/open-verification/

Weizman, E. 2020. Homeland Security algorithm" prevents me from joining you today. A statement from Eyal Weizman. *Forensic Architecture.* 20th February. https://forensic-architecture.org/programme/news/homeland-security-algorithm-prevents-me-from-joining-you-today-a-statement-from-eyal-weizman [accessed 27th July 2021).

Wellsburcombe Solicitors. (no date). The police have asked me for my phone PIN, do I have to give it to them? https://www.wellsburcombe.co.uk/the-police-have-asked-me-for-my-phone-pin-do-i-have-to-give-it-to-them/

Williams, M.L. and Burnap, P. (2016) 'Cyberhate on Social Media in the aftermath of Woolwich: A Case Study in Computational Criminology and Big Data', *The British Journal of Criminology*, 56(2), pp. 211–238. Available at: https://doi.org/10.1093/bjc/azv059.

Wood, M.A. (2018) '"I just wanna see someone get knocked the fuck out": Spectating affray on Facebook fight pages', *Crime, Media, Culture*, 14(1), pp. 23–40. Available at: https://doi.org/10.1177/1741659016667437.

Yar, M. (2012) 'Crime, media and the will-to-representation: Reconsidering relationships in the new media age', *Crime, Media, Culture*, 8(3), pp. 245–260. Available at: https://doi.org/10.1177/1741659012443227.

Legal Case:

R vs Ivor Bell [2019] NICC 20 Application to Exclude the Boston Tapes Evidence. REF OHA11086 16th October, 2019.