Topic Piece

Research Ethics
2018, Vol. 14(4) 1–17

DOI: 10.1177/1747016117750312
journals.sagepub.com/home/rea
SAGE

‘Google wants to know your location’: The ethical challenges of fieldwork in the digital age

Sebastian van Baalen
Uppsala University, Sweden

Abstract

Information communications technologies (ICTs) like laptops, smartphones and portable storage devices facilitate travel, communication and documentation for researchers who conduct fieldwork. But despite increasing awareness about the ethical complications associated with using ICTs among journalists and humanitarians, there are few reflections on digital security among researchers. This article seeks to raise awareness of this important question by outlining three sets of ethical challenges related to digital security that may arise during the course of field research. These ethical challenges relate to (i) informed consent and confidentiality, (ii) collecting, transferring and storing sensitive data, and (iii) maintaining the personal security and integrity of the researcher. To help academics reflect on and mitigate these risks, the article underscores the importance of digital risk assessments and develops ten basic guidelines for field research in the digital age.

Keywords

digital data, digital security, fieldwork, guidelines, research ethics

Introduction

Information and communications technologies (ICTs) are rapidly changing the way researchers conduct fieldwork. The proliferation of ICTs like laptops, smartphones and portable storage devices facilitate travel, communication and

Corresponding author:
Sebastian van Baalen, Department of Peace and Conflict Research, Uppsala University, Gamla Torget 3, 1st floor, Uppsala, SE-751 20, Sweden.
Email: sebastian.van-baalen@pcr.uu.se

documentation in the field. New software enables rapid and more effective data collection, and social media such as Facebook, WhatsApp and Twitter increasingly allow field researchers to keep in contact with their respondents when not in the field. This development has enabled a more sophisticated and elaborate way of gathering and analysing data and is likely to continue to greatly aid future fieldwork (Fileborn, 2016; Hankey and Clunaigh, 2013).

Despite the many benefits of adding ICTs to the toolbox of field researchers, they also pose new ethical challenges. Poorly protected digital data can be accessed from anywhere in the world and spread rapidly to a very large number of individuals (Aldridge et al., 2010). ICTs allow actors to trace the identities, whereabouts and activities of researchers and respondents in the field (Lyall, 2015: 205). Social media accounts allow anyone to compile vast amounts of information about the researcher that can be used against him or her (Andrew, 2016). These digital risks are real and should not be treated lightly. Freedom on the internet declined for the sixth consecutive year in 2016 as more and more governments restricted access to and increased surveillance over digital content, social media and communication applications (Freedom House, 2016). Some authoritarian governments, like the one in Egypt, have shut down the internet entirely to quell digital dissent (Gohdes, 2015: 353–354). Human rights defenders and journalists around the world testify that digital risks have been amplified over the course of the past few years (CPJ, 2012; Hankey and Clunaigh, 2013). In a survey carried out by PEN America, 'many' American writers reported that they assume their communications to be monitored, and 16 percent said they had engaged in self-censorship as a result (PEN America, 2013: 5–6). Two recent cases involving sensitive fieldwork data collected by academics – the seizure of the Boston College Tapes (Sampson, 2015) and the lawsuit against a British ethnographer doing research on urban explorers (Garrett, 2014) – highlight how similar processes are starting to impair the ability of researchers to collect data on sensitive topics (see also Tanczer et al., 2016).[1] It is therefore both timely and imperative that academics engage in a more thorough reflection about the ethics of field research in the digital age.

This article reflects on a set of ethical challenges associated with fieldwork in the digital age. I define fieldwork broadly as the collection or generation of data or experiences in a physical socio-political or geographical site where the researcher spends time, which hence excludes online research and remote data collection.[2] Although questions pertaining to digital security are increasingly raised among journalists and humanitarians (CPJ, 2012; UNOCHA, 2014), as well as in the medical sciences (Myers et al., 2008), there are no comprehensive overviews of the specific digital risks that researchers may encounter in 'the field'. Standard works on the ethics and practicalities of fieldwork rarely convey more than cursory references to digital security (see, for example, Höglund, 2011; Lee, 1995; Scheyvens, 2014; Sriram et al., 2009; Wood, 2006).[3] A number of articles have

made vital contributions by outlining broader issues concerning digital security and online research ethics for researchers (see, for example, Aldridge et al., 2010; Fileborn, 2016; Hankey and Clunaigh, 2013; Rodham and Gavin, 2006; Tanczer et al., 2016), but none of these articles specifically focuses on the broader ethical challenges that relate to field research. This article seeks to fill this important gap in the existing literature.

The purpose of this article is twofold. First, it seeks to raise awareness of the ethical challenges associated with digital security faced by academics conducting fieldwork.[4] It does so by discussing digital risks and solutions in relation to three broader and overlapping themes in the ethics literature: (i) informed consent and confidentiality, (ii) collecting, transferring and storing sensitive data, and (iii) maintaining personal integrity and security. The reflections are based on a review of the existing literature on digital security, particularly in journalism, as well as my own experiences conducting field research on political violence and armed conflict, both as a journalist and in my dissertation project on rebel governance. Although I thus reflect on digital risks from the vantage point of peace and conflict research, I nonetheless believe that many of the issues raised in the ensuing discussion are also relevant, but not necessarily exhaustive, for academics carrying out fieldwork in the social sciences more broadly. Second, the article seeks to help academics reflect on and mitigate these risks by promoting the importance of digital risk assessments and developing ten basic guidelines for field research in the digital age. Although these guidelines partly build on suggestions about safe digital storage and communication by other scholars (e.g. Aldridge et al., 2010; Tanczer et al., 2016), it goes beyond these accounts by deepening the discussion and also reflecting on the issues of informed consent and personal integrity regarding fieldwork in the digital age. The most important conclusion that arises from this discussion is that the concern for digital security is no longer an optional inclination that only applies to 'computer nerds', but an inescapable dimension of twenty-first century fieldwork that should permeate the entire research process.[5]

Understanding digital risks in field research

Research ethics focus on protecting the safety and integrity of research participants (the do-no-harm principle) and anticipating ethical challenges through careful preparation is the be-all and end-all of any field research. Maintaining digital security is no exception. To start thinking about digital risks, most practical guidelines stress the need to evaluate the project by using some sort of digital risk assessment protocol. Digital risk assessments force researchers to consider the potential threats they may face, the vulnerabilities that their devices and practices exhibit, and the capacities they have (Tactical Technology Collective and Front Line Defenders, 2017). The level of threat could, for instance, vary with the topic

Table 1. A simple digital risk assessment protocol.

• Threats
• Are you covering a sensitive topic? Why is it sensitive?
• What is known about digital censorship and surveillance in your fieldwork location?
• Who are the potential adversaries likely to pose a threat to your digital security?
• How will these threats be manifested?
• Vulnerabilities
• What electronic devices will you be using during your fieldwork?
• How will you collect, store and transfer sensitive data?
• How will you communicate when in the field?
• How will you use the internet while in the field?
• Capacities
• What are your current capacities with regard to digital security?
• Who can help you to improve your digital security?
• What measures can you reasonably implement when in the field?

under investigation and the fieldwork location, while vulnerabilities are more closely related to the type of electronic devices researchers have and the way they use them (Rory Peck Trust, 2016). Investigating transnational terror networks may, for example, require much more advanced digital security precautions than studying street vendors, because the former topic is highly sensitive, resides under special jurisdiction, and is likely to attract the attention of actors who maintain greater capacities for digital surveillance. Table 1 provides an example of a simple digital risk assessment protocol.[6]

Conducting a digital risk assessment before embarking on field research is no different from compiling a physical security assessment (Mertus, 2009) or undertaking the comprehensive ethics reviews required by institutional review boards (IRBs), and can fruitfully be conducted as a part of or in conjunction with these assessments. This does not mean that researchers should be paranoid about digital security and constantly look over their digital shoulder. Adopting meticulously extensive digital security precautions may make fieldwork impossible, and most researchers are unlikely to encounter highly determined and technically sophisticated adversaries, even when researching sensitive topics. As noted by the Committee to Protect Journalists (CPJ, 2012: 16),

> Good information security is rarely about fending off sophisticated attacks and Hollywood-style hackers. It's about understanding what you have to protect and the motives and capabilities of those who might want to disrupt your work, then developing consistent habits based on those assessments.

Being sensitive about digital risks can also bring certain benefits to researchers. Thinking and talking about digital security can be a way to establish rapport with respondents. By encouraging informants to consider potential digital risks online and by visibly taking action to protect communication and data, researchers can

signal sincerity and professionalism to the people they study (Parkinson and Wood, 2015: 23). Reflecting on her research on media activism in Egypt, Radsch (2009: 94) notes that: 'Making sure that my informants were aware of my efforts to maintain the security of my data through password protection and encryption was an important part of preserving access, credibility and safety'.

Only when we understand the level of risk that pertains to our project can we start to consciously develop habits that increase our capacity for mitigating threats and lowering vulnerabilities. Below, I discuss three sets of ethical challenges that may arise in association with fieldwork in the digital age and outline some ways through which we can cope with them.

Informed consent and confidentiality

The first set of ethical challenges concerns informed consent and the confidentiality of research participants. The norm of informed consent stipulates that research participants must consent to their participation with a full understanding of the potential risks and benefits (Wood, 2006: 379). IRBs often apply this norm and demand that researchers account for their informed consent procedures in their ethical reviews (Hemming, 2009). The proliferation of ICTs should be reflected in informed consent procedures, in several ways. First, research participants should be properly informed about any digital risks that participation may entail. When relevant, researchers should inform participants about the measures taken to protect the data and how they can communicate with the researcher without fearing interception or surveillance. Second, the procedure should reflect the fact that research publications are usually made available online and that participating hence makes respondents' views and experiences accessible to a much wider audience than paper-based publications. This is particularly important if we intend to share interview transcripts with other researchers or upload them in an online repository (Cramer, 2015; Parkinson and Wood, 2015). Of course, informed consent regarding digital security and online publication should not overburden research participants and should strive to explain these issues in an accessible language.

Protecting participants who wish to remain anonymous is imperative, especially for researchers who study sensitive topics such as political violence, organized crime or socially stigmatized behaviours (see, for example, Brounéus, 2011: 141; Kvale, 2007: 27–28; Wood, 2006: 381). This responsibility to safeguard the identities of research participants is often covered in professional ethics requirements (Banks and Scheyvens, 2014: 168–169). Confidentiality measures commonly include attempts to anonymize field notes and interview transcripts, certain movement precautions in the field, and the safe storage of collected data (further discussed below). Informed consent procedures further require that participants have the ability to withdraw their participation altogether. These efforts are indeed

important to protect the identity of those who provide sensitive data, but may be inadequate in a digital society.

A first risk is that the surveillance of digital communication by security agencies or other actors may compromise the identity of respondents. Communication surveillance is probably among the most common forms of digital risks (CPJ, 2012: 19). Authoritarian states are notorious for monitoring digital communication, but similar challenges may exist in democratic societies. Academics who conduct research on topics that fall under special jurisdiction, such as terrorism or organized crime, may be particularly likely to attract the interest of security agencies. Communicating with high-risk respondents may induce the phone company to record the content of our call or text and share it with the authorities (CPJ, 2012: 18). Not all digital surveillance is, however, conducted by state agencies. Because spyware is readily available online, simple online surveillance can be managed by virtually anyone who has an interest in knowing with whom we communicate and about what.

The most straightforward way to safeguard the anonymity of participants is to use encrypted communication methods. Although user-friendly encryption solutions rarely deter security agencies or professional hackers, they do provide solid barriers against interception by public officials, criminals or other actors who may want to access our or our respondents' communication. Popular encryption solutions include Signal for Android and iPhone, and Jitsi for video conference calls (CPJ, 2012: 19; Tanczer et al., 2016: 351). Some of the best encryption solutions for email are GNU Privacy Guard (GPG) and Pretty Good Privacy (PGP), and these can be integrated in email programmes like Outlook, Thunderbird and Apple Mail (CPJ, 2012: 20). Some of these solutions do, however, require quite advanced computer skills that may require the researcher to consult the university's IT department.

Certain general practices thought to safeguard informed consent and confidentiality may actually contribute to further insecurity. Providing confidential respondents with contact details that allow them to withdraw their participation could, for example, reveal – rather than conceal – their identity if such requests are intercepted. For participants with a certain level of digital literacy, one way to overcome this risk is to encourage confidential informants to contact us using Signal or to provide a step-by-step guide for encrypted email communication under contact information at the research project website. For participants who are less familiar with encryption or do not have access to smartphones and computers, old-fashioned methods like regular mail or contact through an entrusted third party may be more appropriate.[7]

A second risk regarding participant confidentiality originates in poor, careless or insufficient anonymization practices. Sriram (2009) has pointed out that researchers in the post-research and pre-publication stages of a research project may be particularly prone to sharing paper drafts that, among other things, are insufficient in terms

of anonymization. As such drafts may be widely shared beyond the control of the author it can put respondents at risk. Digital files, including Microsoft Word documents, also tend to hide code – so-called metadata – that can be used to retrieve previous versions, comments, track-changes and personal information from the file, hence rendering anonymization procedures useless. This means that even anonymized documents may reveal the identity of respondents to a technically skilled individual (Aldridge et al., 2010: 9). The same goes for other digital files; photographs documenting the results of a focus group discussion may, for instance, contain the GPS coordinates of the location where the picture was taken.

Two specific measures may alleviate these risks. First, researchers should take great care when disseminating early drafts based on fieldwork data and make sure that they do not contain any information that may compromise the anonymity of respondents (Sriram, 2009: 67). Second, all digital data files that are not stored on password-protected and encrypted hard drives, as well as data that are shared with colleagues or made available online, should undergo so-called digital reduction (Tanczer et al., 2016: 9). Digital reduction entails a decoding process whereby documents are sanitized from hidden code and information. Several technical solutions are currently available, and easy-to-follow guides can be found online.[8]

Collecting, transferring and storing sensitive data

A second set of ethical challenges relate to the collection, transfer and storage of sensitive data. Although digital data management may appear safer than carrying notebooks, it does not automatically enhance the security of the data, and often leads to new security risks that need to be acknowledged and managed (Aldridge et al., 2010: 5). The theft, loss, confiscation or interception of digitally held data is often harder to detect than the loss of paper copies because the thief can copy sensitive files and read emails without leaving a trace (Aldridge et al., 2010: 3; CPJ, 2012: 17). Digital data are also especially sensitive as they can be easily duplicated and quickly transmitted to unauthorized people (Myers et al., 2008: 793). When left unprotected, digital files are just as easy to confiscate and read as notebooks. A British ethnographer, conducting research among urban explorers trespassing off-limit sites such as abandoned buildings and construction sites, reflected after his arrest and court proceedings that:

> I feel an enormous amount of guilt over the knowledge that I exacerbated the legal problems of my project participants by unintentionally supplying the police with a (very well organised) ready-made package of evidence that I naively had stored on my computer unencrypted. (Garrett, 2014)

The theft, loss, confiscation or interception of digital data can be both physical (e.g. the theft of a laptop) and digital (e.g. unauthorized server access). Oftentimes,

our servers contain more versions of our data than we are aware of because digital data tend to proliferate as they are transferred between different storage devices, managed in different versions, held in various locations and by different individuals, and during different phases of the research process. As a consequence, a single voice-recorded and transcribed interview may proliferate into tens of different copies and versions that may spread rapidly (Aldridge et al., 2010: 3–4).

There are many different procedures and tools that can help researchers protect their data. Aldridge et al. (2010: 6–9) suggest that, among other things, researchers should ensure that they apply strong passwords,[9] have clear routines for secure data storage and deletion, and exercise great care when sharing digital data through, for example, email. For larger projects, they also propose that researchers devise a written policy on data management that is understood by all members of the research team. Sensitive data can be encrypted by using mathematical transformations that make it unintelligible without a de-encryption key. Encrypted data storage can be facilitated by encryption software, for example Veracrypt or Apple's Filevault, and tools like AbsoluteShield Field Shredder, CleanUp and Steganos Privacy Suite can delete files permanently. It is also recommended to enable password protection of sensitive PDF and Word files. When operating in the field, another sensible solution is to avoid storing sensitive data on our laptop altogether, and instead use smaller storage devices like USB sticks and memory cards that are easier to hide. In addition, immediate anonymization of digital data by exchanging names with unique identifier numbers is a way to guard the information in case of loss.[10] Although these different measures are often enough to address the needs of researchers operating in the field, one should remember that even though encryption restricts access, it often does not hide the fact that our device contains a secret folder.[11] The Trump administration recently announced that passengers entering the US can be forced to give up passwords and mobile phone contacts to border security (Hern, 2017). Because researchers can be forced to give up their passwords under the pressure of police or custom officers, it is critical that scholars always consider whether a particularly sensitive piece of information should be documented at all (Mertus, 2009: 173).[12]

It is also important that field researchers contemplate the ethical risks of including third parties in the data generation process. ICTs have greatly enhanced the toolkit of field researchers and enabled faster data collection in previously inaccessible areas and at a reduced cost. Analytical software, both qualitative and quantitative, allows researchers to comprehend larger and more complex data sets and has opened several new research avenues (Firchow and MacGinty, 2017: 30–31). A less acknowledged feature of these technologies is that they introduce new actors into the data generation process over which researchers have very little influence. Whereas recording survey data or field notes manually only requires pen and paper (and maybe an enumerator or survey company), using tablets may

introduce several third parties to the process: application developers; mobile, internet and data storage companies; and government regulators. This process 'relies on the goodwill and security consciousness of multiple organizations, often in different jurisdictions' (UNOCHA, 2014: 7). This is not necessarily problematic, as it depends on the country context and research topic, but researchers who collect sensitive data must be aware of the additional challenges technology introduces in the data generation process. Few researchers would, for instance, be prepared to share data on collective protest action with the Ethiopian government, but by using ICTs for collecting such data it can become available to the authorities through local internet providers or government regulators. Similar challenges can arise when using cloud services like iCloud, Dropbox and Google Docs. Although cloud services may be useful for researchers working in high-risk field sites (Lyall, 2015: 205), these services should not be used without first considering that they are not always properly encrypted or safe from hackers and, more significantly, the companies can be forced to give up user data under certain legislation (Holpuch, 2016). Because the risks associated with third-party inclusion may be hard to overcome both technically and legally, researchers must carefully consider to what extent this risk is relevant for their project and whether the benefits outweigh the risks.

Maintaining personal integrity and security

A third set of ethical challenges surrounds the integrity and security of the researcher. Protecting oneself is not only a moral imperative in and of itself, but is also important because overlooking personal security may indirectly influence participants or other people associated with the researcher (Mertus, 2009: 166). ICTs can facilitate both physical risks, for example through easy access to vast amounts of personal information that can be used to threaten the researcher, and psychological risks, for example through mobilizing online harassment and hate mobs (Andrew, 2016).

Maintaining personal integrity and security is increasingly difficult because of the digital footprint researchers leave online. Activity online does not pass unnoticed, and a quick online search can often reveal a great deal of personal information, including our contact details, families' whereabouts, relationships and political opinions. Using this information for malicious purposes is commonly referred to as doxing (Andrew, 2016). In most instances the information is harmless, but in extreme cases such information can be used to discredit, arrest or target academic researchers. This has been the case following the attempted coup d'état in Turkey, where the authorities have engaged in a massive purge of academics, journalists and activists (Reuters, 2016). What can be considered sensitive personal information can also differ radically between different research contexts,

and authoritarian regimes are often capricious in their efforts to quell dissent. The authorities in Azerbaijan, for instance, using local phone records, arrested and questioned the 'ethnic pride' of people who cast their vote on long-time enemy Armenia in the Eurovision Song Contest in 2009 (*The Guardian*, 2009). To avoid unanticipated risks from doxing, researchers who are working on sensitive topics should, at a minimum, map the type of information that is available about them online. Simple measures include making social media profiles private, terminating old accounts, and requesting to be deleted from online registries. Sometimes just becoming aware of the information available may be enough to determine to what extent personal details can and should be kept secret or not (see also Fileborn, 2016: 108–111).

Our online activity may also reveal a great deal of information about our research interests and attract the attention of security agencies (Tanczer et al., 2016: 349). Because our computers are uniquely configured, it is possible for online trackers to identify the computer from which a certain website was accessed even when we hide our IP numbers. This is called a digital fingerprint.[13] The best way to mitigate the risk of online surveillance is to invest in a few relatively simple cryptographic circumvention tools. These services allow users to browse the internet through different proxy servers that make it harder to trace the origin of the activities. A common form of cryptographic circumvention is the virtual private network (VPN), which redirects user traffic through multiple servers around the world. The selection of VPN services has increased rapidly in recent years, and many of them have been customized to service users with relatively limited computer skills. All have strengths and weaknesses and differ widely in price; scholars who seek to browse the internet anonymously should therefore conduct the necessary background research (or consult their IT departments) to find a service that caters to their specific needs. Another user-friendly tool is the Tor network – an internet browser that enables the user to access the internet anonymously.[14] Because VPNs and Tor operate according to different logics, most guidelines recommend users to employ these tools in concert.

Electronic devices may also compromise the movements of researchers operating in the field (Lyall, 2015: 205). Although the tracking of researchers through their smartphones may invoke Orwellian associations that seem far removed from the everyday experience of most field researchers, many scholars have recounted that their movements were monitored by security agents or local officials (Thomson, 2009). Indeed, some of the governments with a reputation for closely monitoring researchers, like Rwanda and Israel, also possess sophisticated technological capabilities when it comes to digital surveillance. Security agencies can monitor the movements of individuals by geo-tracking their cell phones or other digital devices. One way to mitigate the threat of surveillance and tracking, as done by Parkinson during her field research in Lebanon, is to remove the battery

from our cell phone (or leave it behind), maintaining an unregistered number, and buying credits using cash only (CPJ, 2012: 19; Parkinson and Wood, 2015: 23). Other devices, such as laptops, can also be targeted and used to spy on the researcher by turning on the webcam and microphone, often with the help of free and easy-to-use spyware. In China, foreign academics have reported that the Chinese authorities have broken into their hotel rooms to install spyware on their computers (Shih, 2015: 22). It may also be sensible for researchers to carefully consider how they use social media during fieldwork, because posting pictures on services like Instagram or Facebook may effectively leave a GPS trail to the places we visit.

Another potential digital risk in politically volatile environments is phishing, which refers to attempts to obtain sensitive information or discredit individuals by disguising as a trustworthy entity, for example as a website, email or Facebook group. Such attempts are common in authoritarian states where security agencies seek to lure political opponents to reveal their true loyalty. Security agencies may attempt to have political activists visit illegal websites that make them prosecutable. Cyber criminals are also known to use different phishing techniques to hold people's computers for ransom (so-called ransomware) or by installing spyware on computers.[15] The easiest way to guard against phishing attacks is to use common sense and never click on unknown or suspicious links.

Finally, the interruption of network services may compromise the field researcher's personal security or obstruct our ability to effectively conduct field work. Foreign correspondents in China, for instance, have reported intentional distributed denial-of-service (DDoS) assaults on their servers as a means of crippling their reporting effectiveness (O'Brien, 2011). Governments regularly restrict or deny access to sensitive digital content or popular social media outlets, hence making communication more difficult (Freedom House, 2016). The interruption of network services can be particularly precarious when coinciding with political upheavals, war or natural emergencies, as field researchers are increasingly dependent on cell phone signals, GPS and internet services. Although there are ways to access the internet even under such extraordinary circumstances, they are technically challenging and unreliable. Researchers that operate in such volatile environments can pre-empt the challenges that arise from network interruption by designing emergency evacuation protocols that are not dependent on electronic communication.

Conclusion

This article has sought to contribute to the emerging literature on digital security and online research ethics by outlining and reflecting on three sets of ethical challenges that may arise during the course of fieldwork and by providing some initial

Table 2. Basic guidelines for digital security in field research.

1.	Conduct a digital risk assessment.
2.	Devise a realistic routine for safe data management.
3.	Map your 'online-self' before leaving for fieldwork and avoid unnecessary social media activity.
4.	Always seek informed consent before sharing data in online archives.
5.	Use strong password protection on all electronic devices and sensitive files.
6.	Store fieldwork data in encrypted folders or on encrypted disks.
7.	Avoid sensitive tasks when connected to public networks or when visiting non-encrypted websites.
8.	Contemplate the risks of using ICTs to collect and record data.
9.	Beware of metadata in publically circulated documents and files.
10.	Use encryption when communicating with confidential research participants.

thoughts on how to mitigate these risks. I summarize these as a number of basic guidelines in Table 2.[16] These guidelines differ from existing recommendations by also taking informed consent and personal integrity into account, in addition to known concerns regarding data security and communication (see Aldridge et al., 2010; Tanczer et al., 2016). Although these guidelines may go some way in alleviating digital risks for field researchers, one should keep in mind that they at best constitute necessary, and not sufficient, conditions for digitally secure fieldwork. Sound digital risk assessment is about anticipating risks and weighing them against the possible consequences of a security breach. Given that technical solutions can seem daunting to most academics, researchers who plan to undertake research on sensitive topics and in dangerous environments are recommended to always seek technical and legal advice.

Two important caveats are in order. First, it is important to note that certain security precautions can themselves constitute a security risk because the use of, for instance, encryption and circumvention tools may signal suspicious activity and hence attract undue attention (Tanczer et al., 2016: 351). Some authorities specifically crack down on encryption software users, and protocols like PGP and GPG are illegal in certain countries (Hankey and Clunaigh, 2013: 541). Researching topics that fall under special jurisdiction may also allow law enforcement agencies to search or seize our devices. When possible, transparency and efforts to ensure local cooperation and acceptance may still be the most viable approach to protect researchers, respondents and data against digital risks (see UNOCHA, 2014: 17).

Second, researchers should remain cautious about employing technical solutions to what are essentially ethical problems (see Hankey and Clunaigh, 2013: 540). Digital risks are clearly technical in nature, but like all ethical challenges of fieldwork they arise as a result of factors that have more to do with the research topic and specific context than the mere existence of surveillance technology or spyware. Technical measures may induce a false sense of security that can put both the researcher and his or her respondents at risk and divert attention from

critical ethical considerations regarding the viability of fieldwork or the basic moral impediments of academic research. If fieldwork is deemed too risky for the respondents or researchers, scholars are better off redesigning or abandoning their project than carefully calibrating their Firewall (see Wood, 2006: 374).

Two general suggestions that may facilitate further discussion on digital risks in fieldwork emerge from the preceding discussion. The first suggestion is an invitation to other scholars to reflect on ethical challenges that they have encountered when doing fieldwork. A key message in the existing literature and in this article is that digital risks are context-dependent and that there are no universal solutions. Efforts to improve digital risk assessments would be greatly aided if scholars more frequently were to report and reflect on digital security challenges they have experienced, as is the case with regard to other ethical considerations. We also need more elaborate ethical debates about how the use of ICTs during fieldwork affects selection bias, the ethics of remote sensing tools, and the use of social media in research (see, for example, Fileborn, 2016; Firchow and MacGinty, 2017). The second suggestion is that it might be a good idea for university departments, IRBs and social science associations to develop concrete guidelines for digital risk assessments and provide up-to-date tools and methods for dealing with potential risks.[17] Although the preceding discussion has focused on what individual researchers can do to mitigate digital risks related to field research, it is important that the academic community develops firm institutional support and training regarding these issues. This discussion does not claim to be exhaustive, and the proposed guidelines are unlikely to deter highly determined actors from transgressing confidentiality measures or accessing our digital data. It is, however, my hope that this article will spur increased awareness and reflection of this important topic among researchers engaged in fieldwork.

Acknowledgements

The author would like to express his gratitude to Ulrika Sundling at the Security Department at Uppsala University, the participants at the Ethics in Field Research in Peace Research-course (Uppsala University), and the "Tuesday Group" for their encouragements for writing this article and their constructive comments on an earlier draft of this article. I am also thankful for the insightful comments provided by an anonymous reviewer.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

All articles in Research Ethics are published as open access. There are no submission charges and no Article Processing Charges as these are fully funded by institutions through Knowledge Unlatched, resulting in no direct charge to authors. For more information about Knowledge Unlatched please see here: http://www.knowledgeunlatched.org.

Notes

1. Both researchers had their digital data seized by law enforcement authorities and later contemplated how better digital security could have mitigated some of the resulting consequences for their research participants. Although such challenges could probably be mitigated by measures such as the Certificate of Confidentiality provided by the US Department of Health (see https://humansubjects.nih.gov/coc/background), which protects health researchers against having their data seized by law enforcement authorities, they are unlikely to work equally well when working on politically sensitive topics like terrorism or in countries with poor rule of law.
2. On the ethics of 'virtual fieldwork' see, for example, Rodham and Gavin (2006), Décary-Hétu and Aldridge (2015) and Barratt and Maddox (2016). On remote data collection see, for example, Firchow and MacGinty (2017).
3. It should be noted that Lee (1995) was published before ICTs were commonplace.
4. Beyond the specific risks associated with fieldwork, there are also broader issues pertaining to digital security that are beyond the scope of this article, for example viruses, ransomware, malware and distributed-denial-of-service (DDoS) attacks that make digital services unavailable. For more information on these risks see, for example, Tactical Technology Collective and Front Line Defenders (2017) or consult your IT department.
5. Hankey and Clunaigh (2013: 546) draw a similar conclusion for human rights defenders.
6. The protocol is a simplified version of two more advanced templates for carrying out digital risk assessments, the guidelines provided by Tactical Technology Collective and Frontline Defenders (available at https://securityinabox.org/en/lgbti-mena/security-risk/) and the protocol by the Rory Peck Trust, an organization working to ensure the safety of freelance newsgatherers around the world (available at https://rorypecktrust.org/resources/digital-security/digital-risk-assessment/downloads?cu=en-GB).
7. I owe this point to the insightful comments by an anonymous reviewer.
8. Simple, and less sophisticated, solutions include the guidelines provided by the word-processing software companies, such as the step-by-step guide provided by Microsoft Office (see https://support.office.com/en-us/article/Remove-hidden-data-and-personal-information-by-inspecting-documents-356b7b5d-77af-44fe-a07f-9aa4d085966f).
9. The KeePass application (KeePass for Windows/Android and KeePassX for Mac/iPhone) allows users to store passwords behind solid encryption.
10. Lane (2016: 83) provides one example of how to allocate such unique identifier numbers.
11. Veracrypt has a deniability function which allows users to hide their encrypted folders.
12. On travelling with your data, see the guidelines provided by the Electronic Frontier Foundation (Schoen et al., 2011).
13. Services like Panopticlick (https://panopticlick.eff.org/) can analyse how well your browser and add-ons protect you against online tracking and assess how unique your digital fingerprint is. It also provides advice on how to increase your anonymity online.
14. More information about the Tor Project and downloads are available at https://www.torproject.org/.
15. Consider, for instance, the many invitations to serve as editors for an obscure journal that end up in our email inboxes on a daily basis.
16. On data security, see also the 14 guidelines developed by Aldridge et al. (2010). Some of the guidelines outlined here (notably number 2, 5, 6 and 9) are based on their guidelines.
17. Tanczer et al. (2016: 352) make a similar point.

ORCID iD

Sebastian van Baalen https://orcid.org/0000-0003-3098-5587

References

Aldridge J, Medina J and Ralphs R (2010) The problem of proliferation: Guidelines for improving the security of qualitative data in a digital age. *Research Ethics Review* 6(1): 3–9.

Andrew AD (2016) Even doing academic research on video games puts me at risk. *The Establishment*. Available at: https://theestablishment.co/even-doing-academic-research-on-video-games-puts-me-at-risk-1c48febb0c96#.elspur9ug (accessed 7 March 2017).

Banks G and Scheyvens R (2014) Ethical issues. In: Scheyvens R (ed.) *Development Fieldwork: A Practical Guide*. London: SAGE, 160–187.

Barratt MJ and Maddox A (2016) Active engagement with stigmatised communities through digital ethnography. *Qualitative Research* 16(6): 701–719.

Brounéus K (2011) In-depth interviewing: The process, skill and ethics of interviews in peace research. In: Höglund K and Öberg M (eds) *Understanding Peace Research: Methods and Challenges*. Oxon: Routledge, 130–145.

CPJ (2012) *Journalist Security Guide: Covering the News in a Dangerous and Changing World*. New York: Committee to Protect Journalists. Available at: https://cpj.org/reports/2012/04/journalist-security-guide.php (accessed 27 February 2017).

Cramer K (2015) Transparent explanations, yes. Public transcripts and fieldnotes, no: Ethnographic research on public opinion. *Qualitative & Multi-Method Research* 13(1): 17–20.

Décary-Hétu D and Aldridge J (2015) Shifting through the net: Monitoring of online offenders by researchers. *The European Review of Organised Crime* 2(2): 122–141.

Fileborn B (2016) Participant recruitment in an online era: A reflection on ethics and identity. *Research Ethics* 12(2): 97–115.

Firchow P and MacGinty R (2017) The practicalities and ethics of mobile phone surveys in conflict-affected contexts. *International Studies Perspectives* 18(1): 28–37.

Freedom House (2016) *Silencing the Messenger: Communication Apps under Pressure*. Freedom on the Net, Washington, DC: Freedom House. Available at: https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf (accessed 23 January 2017).

Garrett B (2014) Place-hacker Bradley Garrett: Research at the edge of the law. *Times Higher Education (THE)*. Available at: https://www.timeshighereducation.com/features/place-hacker-bradley-garrett-research-at-the-edge-of-the-law/2013717.article (accessed 3 May 2017).

Gohdes AR (2015) Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research* 52(3): 352–367.

Hankey S and Clunaigh DÓ (2013) Rethinking risk and security of human rights defenders in the digital age. *Journal of Human Rights Practice* 5(3): 535–547.

Hemming J (2009) Exceeding scholarly responsibility: IRBs and political constraints. In: Sriram CL, King JC, Mertus JA, et al. (eds) *Surviving Field Research: Working in Violent and Difficult Situations*. Oxon: Routledge, 21–37.

Hern A (2017) UK tourists to US may get asked to hand in passwords or be denied entry. *The Guardian*, 9 April. Available at: https://www.theguardian.com/us-news/2017/apr/09/

uk-tourists-to-us-may-get-asked-to-hand-in-passwords-or-be-denied-entry (accessed 14 August 2017).

Höglund K (2011) Comparative field research in war-torn societies. In: Höglund K and Öberg M (eds) *Understanding Peace Research: Methods and Challenges*. Oxon: Routledge, 114–129.

Holpuch A (2016) Tim Cook says Apple's refusal to unlock iPhone for FBI is a 'civil liberties' issue. *The Guardian*, 22 February. Available at: https://www.theguardian.com/technology/2016/feb/22/tim-cook-apple-refusal-unlock-iphone-fbi-civil-liberties (accessed 21 April 2017).

Kvale S (2007) *Doing Interviews*. London: SAGE.

Lane J (2016) *Big data and anthropology: Concerns for data collection in a new research context*. Available at: https://www.anthro.ox.ac.uk/sites/default/files/anthro/documents/media/jaso8_1_2016_74_88.pdf (accessed 20 April 2017).

Lee RM (1995) *Dangerous Fieldwork*. Thousand Oaks: SAGE.

Lyall J (2015) Process tracing, causal inference, and civil war. In: Bennett A and Checkel JT (eds) *Process Tracing: From Metaphor to Analytical Tool*. Cambridge: Cambridge University Press, 186–207.

Mertus JA (2009) Maintenance of personal security: Ethical and operational issues. In: Sriram CL, King JC, Mertus JA, et al. (eds) *Surviving Field Research: Working in Violent and Difficult Situations*. Oxon: Routledge, 165–176.

Myers J, Frieden TR, Bherwani KM, et al. (2008) Ethics in public health research: Privacy and public health at risk: Public health confidentiality in the digital age. *American Journal of Public Health* 98(5): 793–801.

O'Brien D (2011) *Exposing the internet's shadowy assailants*. Committee to Protect Journalists. Available at: https://www.cpj.org/2011/02/attacks-on-the-press-2010-internet-analysis-danny-obrien.php (accessed 27 February 2017).

Parkinson SE and Wood EJ (2015) Transparency in intensive research on violence: Ethical dilemmas and unforeseen consequences. *Qualitative & Multi-Method Research* 13(1): 22–27.

PEN America (2013) *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*. New York: PEN American Center. Available at: https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (accessed 3 May 2017).

Radsch C (2009) From cell phones to coffee: Issues of access in Egypt and Lebanon. In: Sriram CL, King JC, Mertus JA, et al. (eds) *Surviving Field Research: Working in Violent and Difficult Situations*. Oxon: Routledge, 91–107.

Reuters (2016) Turkey seeks arrest of university academics in Gulen-related probe: Media. *Reuters*, 9 December. Available at: http://www.reuters.com/article/us-turkey-security-university-idUSKBN13Y0E0 (accessed 3 May 2017).

Rodham K and Gavin J (2006) The ethics of using the internet to collect qualitative research data. *Research Ethics Review* 2(3): 92–97.

Rory Peck Trust (2016) *Digital Security Risk Assessment Guide*. London: Rory Peck Trust. Available at: https://rorypecktrust.org/resources/digital-security/digital-risk-assessment/downloads?cu=en-GB (accessed 6 March 2017).

Sampson F (2015) 'Whatever you say …': The case of the Boston College Tapes and how confidentiality agreements cannot put relevant data beyond the reach of criminal investigation. *Policing* 10(3): 222–231.

Scheyvens R (ed.) (2014) *Development Fieldwork: A Practical Guide*. London: SAGE.

Schoen S, Hofmann M and Reynolds R (2011) *Defending Privacy at the U.S. Border: A Guide for Travelers Carrying Digital Devices*. San Francisco: Electronic Frontier Foundation. Available at: https://www.eff.org/document/defending-privacy-us-border-guide-travelers-carrying-digital-devices (accessed 10 May 2017).

Shih V (2015) Research in authoritarian regimes: Transparency tradoffs and solutions. *Qualitative & Multi-Method Research* 13(1): 20–22.

Sriram CL (2009) Maintenance of standards of protection during writeup and publication. In: Sriram CL, King JC, Mertus JA, et al. (eds) *Surviving Field Research: Working in Violent and Difficult Situations*. Oxon: Routledge, 57–68.

Sriram CL, King JC, Mertus JA, et al. (eds) (2009) *Surviving Field Research: Working in Violent and Difficult Situations*. London and New York: Routledge.

Tactical Technology Collective and Front Line Defenders (2017) *How to assess your digital security risk*. Security-in-a-box. Available at: https://securityinabox.org (accessed 26 April 2017).

Tanczer LM, McConville R and Maynard P (2016) Censorship and surveillance in the digital age: The technological challenges for academics. *Journal of Global Security Studies* 1(4): 346–355.

The Guardian (2009) Azerbaijan authorities interrogate music fans in Eurovision probe. *The Guardian*, 18 August. Available at: https://www.theguardian.com/music/2009/aug/18/azerbaijan-authorities-interrogate-music-fans (accessed 23 January 2017).

Thomson SM (2009) 'That is not what we authorised you to do …': Access and government interference in highly politicised research environments. In: Sriram CL, King JC, Mertus JA, et al. (eds) *Surviving Field Research: Working in Violent and Difficult Situations*. Oxon: Routledge, 108–123.

UNOCHA (2014) *Humanitarianism in the age of cyber-warfare: Towards the principled and secure use of information in humanitarian emergencies*. OCHA Policy and Studies Series, Occasional Policy Paper. New York: United Nations Office for the Coordination of Humanitarian Affairs.

Wood EJ (2006) The ethical challenges of field research in conflict zones. *Qualitative Sociology* 29: 373–386.