

5-27-2018

Nothing to Hide, Nothing to Fear? Tools and Suggestions for Digital Data Protection

Jedidiah C. Anderson

Furman University, jed.anderson@furman.edu


Erik Skare

University of Oslo, erik.skare@ikos.uio.no

Courtney Dorroll

Wofford College, dorrollcm@wofford.edu

Follow this and additional works at: <https://nsuworks.nova.edu/tqr>

 Part of the [Bilingual, Multilingual, and Multicultural Education Commons](#), [Curriculum and Social Inquiry Commons](#), [Educational Methods Commons](#), [Near Eastern Languages and Societies Commons](#), and the [Quantitative, Qualitative, Comparative, and Historical Methodologies Commons](#)

Recommended APA Citation

Anderson, J. C., Skare, E., & Dorroll, C. (2018). Nothing to Hide, Nothing to Fear? Tools and Suggestions for Digital Data Protection. *The Qualitative Report*, 23(5), 1223-1236. Retrieved from <https://nsuworks.nova.edu/tqr/vol23/iss5/14>

This How To Article is brought to you for free and open access by the The Qualitative Report at NSUWorks. It has been accepted for inclusion in The Qualitative Report by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.



Nothing to Hide, Nothing to Fear? Tools and Suggestions for Digital Data Protection

Abstract

The developing cyber-infrastructure has provided new tools, methods, and opportunities to conduct research. However, the Snowden leaks and subsequent developments proved that the same infrastructure has made all-encompassing surveillance possible – posing new challenges for researchers when engaging with those they are obligated to protect. As the cyber-infrastructure simultaneously opens up new possibility-spaces for circumventing structures of surveillance, while drawing on the authors' own experiences, this article presents a number of tools and suggestions that will aid the researcher to engage more responsibly and safely with the research subject digitally.

Keywords

Surveillance, Source Protection, Data Protection, Digital Fieldwork, Encryption, Field Methodology

Creative Commons License



This work is licensed under a [Creative Commons Attribution-Noncommercial-Share Alike 4.0 License](https://creativecommons.org/licenses/by-nc-sa/4.0/).

Acknowledgements

This work was supported by the Aspen Institute under the Stevens Initiative.

Nothing to Hide, Nothing to Fear? Tools and Suggestions for Digital Data Protection

Jedidiah Anderson

Furman University, Greenville, South Carolina, USA

Erik Skare

University of Oslo, Norway

Courtney Dorroll

Wofford College, Spartanburg, South Carolina, USA

The developing cyber-infrastructure has provided new tools, methods, and opportunities to conduct research. However, the Snowden leaks and subsequent developments proved that the same infrastructure has made all-encompassing surveillance possible – posing new challenges for researchers when engaging with those they are obligated to protect. As the cyber-infrastructure simultaneously opens up new possibility-spaces for circumventing structures of surveillance, while drawing on the authors' own experiences, this article presents a number of tools and suggestions that will aid the researcher to engage more responsibly and safely with the research subject digitally. Keywords: Surveillance, Source Protection, Data Protection, Digital Fieldwork, Encryption, Field Methodology

Introduction

It is the duty of the researcher to ensure that any human subject does not come to physical harm or psychological risk because of the research process, and to secure its well-being. Unfortunately, in the history of science, this has not proven to be the case. Following the Second World War, for example, twenty-three physicians and scientists stood trial accused of inflicting vile and lethal procedures on vulnerable populations (Leaning, 1996). More than 400 African Americans with syphilis remained untreated between 1932 and 1972 for researchers to study the disease (Orb, Eisenhauer, & Wynaden, 2000). Although circumstances change, and the dilemmas that we face may come forth as new, the ethical principle of protection nevertheless remains the same.

With the development of the cyber-infrastructure, it provides the researcher with new tools to obtain information, streamline the research process, and develop new approaches to understand scientific findings. Further, the new infrastructure enables the researcher to engage with research subjects, discuss, and learn from them while, indeed, sitting thousands of miles away. The new possibility-spaces enabled by the Internet are, however, not without problems or causes for concern. As the Snowden leaks revealed, the cyber-infrastructure has also enabled a situation in which structures of surveillance become saturated and more all-encompassing. According to Bauman et al. (2014), the scale and reach of the programs of the National Security Agency (NSA) surprised even seasoned observers.

As an increasing number of people become users of digital services and social networks such as Facebook, Skype, Twitter, and Google, to mention just some, we may assume that the same applies for researchers who may benefit from these services when obtaining information and engaging digitally with research subjects and colleagues. Yet, as van der Velden (2015)

notes, the data leakage (feeding off on already circulating data) is one of the basic methods of collecting data for the NSA (p. 186). Further, Lyon (2014) warns against how far security and intelligence agencies depend on data obtained from the social realm. Moreover, through the simple use of computers, an increasing number of researchers digitize sensitive data either by saving it on said computer or by uploading it to a cloud-service. The revelations of both state and corporate surveillance have then far-reaching consequences for how we employ digital tools and digitization of data while adhering to the duty of protecting research subjects who may come to harm if a third party with bad intent obtains desired information. Whether we are using our iPhones, sending an email, having a conversation through Skype or Facebook, uploading our information to Dropbox or the institution's local cloud service, the surrounding context of possible surveillance does not change.

The authors of this paper do not intend to draw a dystopian image of current affairs, or to advocate some form of Neo-Luddism by opposing the use of new technology. We emphasize instead that while all-encompassing surveillance is enabled by the new cyber-infrastructure, the very same infrastructure additionally creates new possibility-spaces to circumvent said surveillance. It is our belief that the researcher who employs digital tools, and who is sincere about avoiding physical harm or psychological risk for the subject, must be aware and equally cautious of the possibility that the research data may fall into the wrong hands. To ignore this issue is equally to fail in our responsibilities towards those who put their trust in us and our handling of the data that they provide.

Indeed, the topic of surveillance has been heavily covered in scholarly literature, most notably in Marx' (2016) *Windows into the Soul: Surveillance and Society in an Age of High Technology* and Harcourt's (2015) *Exposed: Desire and Disobedience in the Digital Age*. Marx provides a taxonomy of the various apparatuses that are used in surveillance in a modern society, as well as an analysis of their goals, and their change and continuity over time (Marx, 2016), while Harcourt (2015) adds to this analysis a discussion on the potential for digital disobedience and resistance. Additionally, numerous peer-reviewed articles and essays on the topic have been published in edited collections from a feminist perspective. Most notably, Paech problematizes the role of commercial interests and platform owners in virtual ethnography (Paech, 2009, pp. 201-203), and Zelezny-Green examines the ethical issues in researching cell phone usage by young girls (Zelezny-Green, 2016, p. 71). Smith, in her essay "Not-Seeing: State Surveillance, Settler Colonialism, and Gender Violence Surveillance" in the edited collection *Feminist Surveillance Studies*, critiques modern surveillance studies arguing that the dynamics of settler colonialism and white supremacist systems also need to factor into analyses of surveillance (Smith, 2015, p. 23).

Considering the coverage of surveillance in scholarly literature, it is our belief that researchers do not ignore the issue of cyber-security dishonestly or intentionally. Instead, it may (partly) be a result of lacking knowledge and skills, and the bewilderment of where to begin when wanting to secure sources and material. It is then important to avoid the exotizing of the security process such as when the DEFCON Hacking Convention website (n.d.) remarked, "[...] reporters, researchers, and activists are having to behave more and more like spies to protect their data and identities [*sic*] while participating online." While emphasizing the importance of sound digital routines, this statement simultaneously portrays the process as something far more sinister than it is. Illustrating the matter, all authors of this article are Middle East and North Africa (MENA)-focused academics who do not come from a cyber-security background, but who have learned about some of the necessary measures while operating in environments where compromising data can prove dangerous for research subjects. It is a goal then that the tools that are suggested in this article are not challenging to install, to use, or to update. Although some of the tools suggested in this article, such as the live operating system The Amnesic Incognito Live System (Tails), may require some more

effort than others, none of the tools in this article require specific and advanced skills in computers and coding.

This article consists of three parts. First, the three of us present personal experiences analyzed through the research methods of ethnography and oral history with the dilemma of employing digital tools and the inherent challenges that may be involved. The second part proceeds from these experiences to discuss some of the tools that researchers may employ when attempting to secure their sources and data. We (Dr. Anderson, who conducted an ethnography and oral history of LGBTIQ activists in the Middle East, Dr. Dorroll, who led a virtual exchange between students in the Middle East and students in the US, and Erik Skare, who conducted qualitative interviews online with Palestinian hacktivists) have divided this part into two sections, first, securing the means of information storage, and, secondly, securing means of communications. Last, we summarize and conclude the discussion in this article.

The Necessity of Data Protection: Some Experiences

LGBTIQ¹ Activists in the Arab World and Cyber Challenges – Anderson

Unlike many ethnographic researchers, I intentionally blurred the lines between myself as a researcher, and as an activist. I volunteered for Helem (the primary LGBTIQ rights group that I studied in Lebanon), and participated in demonstrations, events, and teach-ins at gay bars, indistinguishable in my participation from any of Helem's other members. I wrote in its center and discussed and shared my research with anyone that had even the slightest interest. I also maintained an academic interest in the activities of Helem's activists outside and interviewed several who worked in Palestinian refugee camps about their work there for an oral history project.

However, my ethnographic work focusing on LGBTIQ activism in Lebanon, Iraq, and Israel/Palestine has made me aware of not only the risks that Arab LGBTIQ activists face in the physical sphere, but of the risks that they face on the Internet due to online exploitation. This ethnographic work has led me to become deeply interested, to look for, and to implement what I consider best practices in order to ensure the security of my ethnographic sources and informants to the highest extent possible.

As government surveillance of LGBTIQ activists and other political dissidents in the MENA region tends to be overt and publicly known, a large amount of literature about data and source is available in both English and Arabic about how to protect both one's self and one's sources when engaged in either journalistic or ethnographic work in the MENA region. The Committee to Protect Journalists, in a report on technology security, describes a situation in which access to Israeli contact information poses a danger to the researcher working in an Arab country (O'Brien, 2015). This scenario was relevant to the ethnographic work that I did, given that I worked in both Lebanon and Israel/Palestine, two states that are still technically at war with each other. This made it necessary to take cybersecurity concerns into account when planning my fieldwork. I abstained from contacting Israelis while in Lebanon, unless I was asking a third party in the United States or the EU about their contacts in Israel that would be relevant to my research. I put contact information that I received into a plain-text file that I stored on an encrypted data storage cloud (which was not directly accessible from either my smartphone or my laptop) rather than store it in my normal phone contacts, and immediately deleted the original communication.

When I prepared to cross the Allenby Bridge from Jordan into Israel, cybersecurity became even more important. There are numerous stories of laptops and smart phones being

¹ LGBTIQ stands for lesbian, gay, bisexual, transgender, intersex, and queer.

searched – and in one case, two Palestinian-Americans traveling together were forced to login to their email by Israeli security and had it searched upon arriving at Ben Gurion airport. They were subsequently denied entry into Israel (Doughman & Al-Sarabi, 2012). In order to prevent this from happening to me, I “defriended” all Palestinian friends on my Facebook account, and subsequently “refriended” them after my research was concluded. (It would have been better, in retrospect, to deactivate my Facebook account entirely.) I also went through all of my email accounts, searching for keywords such as “Israel,” “Palestine,” and “West Bank,” and permanently deleted all of those emails.² I then took all of my Lebanese contacts, turned those contacts into “v-card” files (files solely comprised of contact information that can be directly downloaded into a smartphone’s contacts), and uploaded them to my encrypted online cloud service. This procedure was carried out along with all electronic documents related to my research, and I then deleted all traces of those files and contacts (as well as connection to the cloud service) from my smartphone and laptop. I only re-downloaded those files and contacts after I left Israel. Additionally, I maintained social media silence, only using the “message” function on my Facebook to communicate with people. I also uploaded all of my sound recordings of interviews and transcripts that I did to my cloud service as soon as possible, and erased them immediately afterwards from my laptop.

Palestinian Hackers and Digital Fieldwork – Skare

Writing a master’s thesis on the digitization of the Palestinian resistance in general, and on Palestinian hackers in particular, I conducted a number of interviews online with hacker groups such as Gaza Hacker Team and KDMS Team. There were several reasons for doing so. First, I did not know how to approach them in the physical sphere, and, secondly, the two aforementioned teams are located in the Gaza Strip, currently under blockade with severe travel restrictions imposed.

As I had no prior experience in the use (or theory) of encryption, proxy-servers and related security measures, it was the exchange with the Palestinian hacker groups who made me aware of its necessity. As I obtained an email address with which I could contact a member of Gaza Hacker Team, I sent an email with a number of questions, hoping for an answer. When doing so, I attempted to be polite and transparent – providing the full description of my project, who I was, and institutional affiliation. As this should be the norm for any fieldwork, the need of transparency and a thorough presentation was nevertheless amplified when doing so digitally. That is, fieldwork on the ground, unlike digital fieldwork, is fundamentally visual and material in nature, during which the interviewee and the researcher can see each other, assess body language, tone of voice and appearance. This nature of visibility and materiality is potentially altered during digital fieldwork. For example, when an interviewee receives a digital message, there is much less information to process in order to evaluate the authenticity of the request, limited to the (potentially false) name of the researcher, the subject at hand and the text that has been sent. There is no appearance, no physical presence, no body language or voice adding to the overall impression of whom requests information about the interviewees.

Another issue is that of security, of which I became painstakingly aware. A couple of hours after I sent the first email to the member of Gaza Hacker Team, I lost access to my email account without the ability to log in. Persisting for two days, when I regained access to my account, I saw that there had been several log ins from both the Gaza Strip and from Tel Aviv

² It is important to note that although a file is deleted and subsequently removed from the recycle bin, it has not been deleted from the computer drive. Instead, the file on the computer is marked as unused, can subsequently be overwritten, and can thus be retrieved. In other words, if you are in need of truly deleting the file, you will have to take additional steps.

(I was at that time residing in Jerusalem). As the communication with Gaza Hacker Team continued after the incident, I immediately revealed to the member that it was highly probable that my email account had been hacked, and that we should act accordingly. We corresponded for a period with this in mind, both being careful with the questions posed and the answers provided.

Virtual Exchange Challenges under the al-Sisi Regime – Dorroll

I was awarded a grant from the Stevens Initiative to, in part, coordinate a virtual exchange relationship³ between Lydon College located in the American South and Cairo College in Egypt.⁴ In the virtual exchange, students utilized social media, including a Facebook group, a WordPress blog to discuss movies watched by both Cairo College and Lydon students, and spoke to each other over Skype.

Using virtual exchanges is an excellent method to help connect students. Yet, there are also a number of cyber-vulnerabilities. For example, it was necessary to analyze the governmental structures and laws of the various countries we were interacting with to make sure discussion topics did not create danger for the students involved. The Facebook group on which asynchronous activities took place was set to closed, preventing people not affiliated with the project from joining, in order to provide further privacy to the students participating in the group.

Professors administered the Facebook group that we created linking students from Cairo and the American South. The professor at Cairo College worked as the gatekeeper to friend requests from Cairo College students and I, the Lydon professor, acted as the gatekeeper for Lydon students. The criteria to be added to the group was that students had to be enrolled in the Virtual Exchange club at Cairo College (after a selection process that included an application and one-on-one interview), or the student had to be enrolled in the class at Lydon that was using the virtual exchange as a part of their semester activities.

An issue that we faced was infrastructural in nature, constituting a “digital divide.” First, the Cairo College students did not have wireless internet on campus, so the professor had to reserve an off-campus venue that provided wireless internet for our Skype sessions. Secondly, uploading videos to the Facebook group also required that the Cairo College students had enough bandwidth to upload successfully. Students would often record their videos and then wait to upload them when they had a scheduled meeting at the venue with wireless internet. Professors monitored the Skype discussions in order to ensure that topics did not get into territory that would be deemed illegal or socially taboo, and students did not interact on Skype one-on-one.

The chilling effect that the regime of Abdel Fattah al-Sisi had on the interactions between students at Lydon and students at Cairo College did not go unnoticed by the Lydon students who participated in the virtual exchange. This was reflected in an anonymous survey seeking to get their feedback on the idea of working with vulnerable populations and using the ethnographic method with new communication technologies. Some of the students observed that government social media restrictions “played a role” in “them wanting to talk about some

³ Pseudonyms are employed for the colleges involved in the virtual exchange to further protect the identities of the students involved.

⁴ Virtual exchanges create collaborative learning environments linking students across cultures with the use of digital technologies. Much like study abroad allows students to learn about other cultures and languages the virtual exchange is used in classrooms to allow digital connection, and in Dorroll’s case linked students from the American South with students in Egypt through the use of Skype, Facebook, and WordPress blogs.

things but they could not,” as “they can get into trouble if they say things on the internet that is not approved by the country itself.” They also observed that:

[Egyptian censorship and surveillance] causes them to not be able to truly speak what is on their minds or to give certain aspects of their culture that may affect them every day. To me it seems that they talk a lot about the basic cultural stuff but because of the limitations over Facebook they are not able to share the role of the government and the military in their day to day lives, which must be a huge part given the fairly repressive regime they live under. They also have to be extra careful what they do talk about and how they talk about it, which is only extra stress on their part. They can't even give their full opinion on something simple if they fear it may touch on something they may get in trouble for.

When asked how the virtual exchange would have been different if the restrictions were not in place, the students claimed that they were “sure that we would have done a few things differently and would have gotten back totally different responses.” Another student would have probably “asked them questions about how they feel about the government and the way it runs, because under the restrictions they would be at risk with questions like that.” Another said the following: “I would have liked to know their full story and how they truly feel about their culture. Do they ever get frustrated with the restrictions because their authority gives them no freedom?”

Circumventing Structures of Surveillance: Possible Tools for Researchers

There are several parts to stress from the experiences presented in the preceding part of this article. First, the issue of storing information, and, secondly, to communicate with the research subjects digitally. In order to make comprehensible and to simplify the means, methods and tools that researcher can employ, we may categorize them as the following: Tools to secure the means of communication, and tools to secure the means of information storage. Regarding the latter, today it is nearly impossible to avoid the issue of encryption when we discuss how we can secure and protect sensitive information about our research subjects. As Rogaway (2015), p. 1 [a] states, “cryptography rearranges power: It configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension.”

Securing the Means of Information Storage

As Anderson uploaded his data to a data storage cloud (although encrypted), it is important to emphasize that to do so is not a priori a breach in terms of securing the well-being of the research subject, although it does have considerable disadvantages. For example, one of the most widely used file hosting services (most likely also for researchers) is Dropbox operated by the American company Dropbox Inc. Not only can Dropbox be used in order to save space on the computer, it can also be used in order to avoid having sensitive information on the computer when crossing borders, airport controls and other spaces in which state authorities or others' institutions can get access to sensitive data, as shown by Anderson's case. However, one of the problems with using Dropbox is that it does not pursue a “zero knowledge system,” (i.e., a system when the service that hosts the files and information of researchers does so without actually having access to it). Dropbox explicitly states that they will willingly

decrypt all of the data that you have stored, and hand it over to law enforcement if the latter should send them a subpoena.

Researchers must then question the use of the aforementioned cloud service, or any that does not pursue a zero-knowledge system, and instead look into alternative cloud services (such as SpiderOak or Tresorit), which encrypts the information that is uploaded without the hosts being able to read, access or decrypt it. This means a more secure – albeit not foolproof – way to store sensitive information (however, it is important to note that if the researcher loses the password, then it will not be possible to retrieve the data). Further, because the use of these “zero knowledge” services leave the only unencrypted versions of our information on our local computers, researchers should also spend some effort encrypting either the entire hard drive of the computer or the selected files and information that need to be secured. As Verizon Data Breach Report 2016 showed, academia saw twenty-nine large data breaches of a total of 254, with breach being defined as “an incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party” (Verizon, 2016).

Several programs for the encryption of single files or parts of information are available such as BitLocker, FolderLock and VeraCrypt, which are easy to use and, in several instances, free. The two options of encrypting the entire drive or just some of the information have both advantages and disadvantages. Whereas the former encrypts and secures the whole computer, the researcher will in the worst-case scenario lose everything if the system is corrupted. The latter only secures certain information such as encrypting one or several folders or encrypting one single file such as an audio recording of an interview – necessitating a password in order to get access to the information. However, the rest of the computer is vulnerable and can still be compromised in the wrong hands.

In other words, all of these services can be compromised, even when encrypted (either by default or by the researcher). The question is then whether researchers should avoid storing information and data on cloud services at all. Alternatively, the researcher should consider avoiding uploading and downloading sensitive data, and instead keep the data on a (preferably encrypted) hard or flash drive locked into the office. Or, the researcher should consider avoiding the digitization of data altogether and instead employ pen and paper so that the information cannot be intercepted online. All of these options must be weighed against each other through the researcher’s assessment of the consequences that a breach might have. While doing so, the researcher has a duty to always de-identify the research subjects in such a way that even if the data is compromised, it will not be possible for a third party to recognize those at risk. The Electronic Frontier Foundation (2014a) recommends asking the following questions when performing a threat modeling assessment:

- What do I want to protect?
- Who do I want to protect it from?
- How bad are the consequences if I fail?
- How likely is it that I will need to protect it?
- How much trouble am I willing to go through in order to try to prevent potential consequences?

Whether a third party obtains the information through a cloud service or through the researcher’s written notes does not matter, the potential consequences are the same, and one should carefully ask oneself the questions provided above before choosing the preferred alternative.

Securing the Means of Communications

As proven by both Skare and Dorroll's experiences, securing the means of communications are of adamant importance when attempting to secure the well-being of the research subjects and participants. For example, as can be seen in Dorroll's description of issues encountered over the course of the virtual exchange, protection of the Egyptian participants had to be prioritized, and the largest threat to the students was that emanating from government surveillance, which could be generally assumed before the fact of the virtual exchange. The consequences could potentially have been arrests and detentions of the participants, and it was essential to go to any length needed to prevent these consequences. However, that being said, the implementation of cybersecurity tools was not needed, as basic privacy measures and adherence to the guidelines put forth by the Egyptian faculty involved in the virtual exchange were deemed sufficient to provide safety for the students participating. Indeed, the implementation of excessive cybersecurity tools could have aroused the suspicion of either the Egyptian government or of the Egyptian students, potentially hindering the progress of the virtual exchange. This is something we will return to later in this article.

The Egyptian virtual exchange could have benefited from using a platform with more security and privacy than Skype provides. Jitsi is a web conferencing platform that is free, open source, end-to-end encrypted, and actually provides a greater level of convenience for the end user than Skype in that it does not require the downloading of an additional platform or the exchange of contact information beyond a shared URL and (optional) password for the video conferencing room (Jitsi.org, 2017). On the other hand, research that deals with oppressed groups that are engaged in activism that may or may not be deemed legal by their governments would demand a different threat model. Additionally, if one's sources are in danger if their identities are compromised, and one is facing the risk of having one's electronic media searched upon entering the country, this adds an additional factor to take into account in one's threat modeling, as the questions of surveillance, searching, and anonymity come into play (Flaccus, 2017).

Another important tool is the Virtual Private Networks (VPN). As the authors of this article describe it to students engaged in fieldwork, a VPN is a secure tunnel between the computer of the researcher and the final destination on the internet that uses an intermediary server (proxy server) that your traffic is guided through, hiding your identity. For example, while the researcher sits in California, her traffic will be channeled through a server in Norway, South Africa or Finland, to mention just some. Most universities today offer a free VPN-service through their institutions. However, one should be aware that a VPN-service only protects the researcher from passive surveillance and helps little if one is subjected to active surveillance (for example, but not limited to, state surveillance). Indeed, VPN-services can have issues with data leakages or weak encryption, the provider can log your information (and making it accessible to third parties), and most importantly, a VPN does not help on a computer already infected with malware. Moreover, there are also several countries where VPN-services are not allowed such as in China. In Iran, VPNs are legal, but only through a provider that is registered and approved by the government (O'Driscoll, 2017). In these cases, *if* deemed feasible and necessary, the Tor network provides an additional option when attempting to circumvent surveillance and censorship.

Sometimes colloquially (and somewhat inaccurately) known as "the darkweb," the Tor Project website describes the Tor network as follows:

The Tor network is a group of volunteer-operated servers [...] Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and

individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content [...] Journalists use Tor to communicate more safely with whistleblowers and dissidents. Non-governmental organizations (NGOs) use Tor to allow their workers to connect to their home website while they're in a foreign country, without notifying everybody nearby that they're working with that organization (The Tor Project, Inc., 2017).

The ability of the Tor network to protect the user and the user's communication from surveillance and censorship is something that it is important for the researcher to be aware of and know how to use. However, as noted, just as VPNs, also the usage of Tor are either banned or subject to legal restrictions in a number of countries.⁵ Thus, research into the legality of using these tools in the country that one is doing research in is necessary before hand, as it is trivial for an internet service provider (ISP) to see that one is using the Tor network (although the ISP cannot see the researcher's activity on Tor). Thus, if the use of VPN or the Tor network may compromise your sources because it attracts unwanted attention instead of circumventing it, other means should be pursued.

A third tool for securing the means of communication, and which is not banned, is Pretty Good Privacy (PGP), which a rising number of scholars have begun to employ – used to sign, encrypt and decrypt text messages, emails, files and even whole disk partitions to increase the security of communications. The use of PGP allows the researcher to plan meetings, send and receive information, and to conduct digital fieldwork on sensitive issues and – to a reasonable degree – avoid others accessing it. This would, in theory, allow the researcher not only to communicate more securely with her interviewees by encrypting all messages and communication in which only she and the interviewee possess the key to decrypt the information, but also send and store encrypted sensitive information.

The same applies to modern communication applications such as Signal and WhatsApp. Although the latter has engaged in a partnership with the Open Whisper Systems in order to integrate the encrypted Signal protocol into its product, there are those concerned with privacy who state that one should use Signal instead. For instance, “WhatsApp may retain date and time stamp information associated with successfully delivered messages and the mobile phone numbers involved in the messages, as well as any other information which WhatsApp is legally compelled to collect,” and

Online backups are a gaping hole in the security of WhatsApp messages. End-to-end encryption only refers to how messages are encrypted when they're sent over the internet, not while they're stored on your phone. Once messages are on your phone, they rely on your phone's built-in encryption to keep them safe. (Lee, 2016a)

This implies great vulnerability in retaining and storing the date of the information, in addition to the mobile phone numbers involved. Moreover, Signal is an Open Source application, which means that the code of the application can be read by anyone interested in order to detect flaws or back doors and subsequently remove these.

⁵The Tor network does provide ways of circumventing restrictions on its usage in countries where it is prohibited. It is up to the researcher to determine whether this risk is necessary.

When assessing potential tools for securing digital communication, the same rules apply when considering what tools are beneficial and appropriate (Who do you want to protect? How bad are the consequences if you fail? etc.). Further, the researcher should not be naïve about the capabilities of encryption. A rule of thumb is that even when information and communication are encrypted, one should still be cautious and act as if a third party can read it (stressing the necessity of de-identifying the research subjects). No protective measures in the world will help if the researcher does not apply sound routines. For example, even if the information that was intended to be protected from third parties through encryption, it would be left vulnerable if the password is weak (such as “super2345”). Several password-managing programs exist today, such as LastPass Password Manager, Dashlane, or the Open Source-program KeePassX, allowing the researcher to encrypt and employ strong passwords that, in theory, are not possible to crack without massive efforts and capabilities.

As shown by Skare’s experience, in addition to a strong password, the researcher should spend some time to apply a two-factor authentication where two pieces of information must be applied to log in: the password and another code of verification, for example sent by the service-in-use as a text message to your phone. That is, once the password is typed in, the researcher will be sent an additional code by the service provider before being able to log in. The second piece of information required to log in changes each time one does so. This means that even if the initial password giving access to sensitive information is compromised, it will be useless without the second piece of information. Most services such as Gmail and Facebook are helpful in this issue and provide guides for its users on how to apply such a security measure.

The same applies to smart phones such as iPhones, which are encrypted by default. Researchers should apply a strong password to their phones – at least six characters, and eleven if one is concerned about being hacked by strong adversary such as a state agency (Lee, 2016b). If the researcher believes that there is a danger of forced entry, she has the opportunity to have all data on her phone deleted after ten incorrect attempts to type the password. These measures would only be useful, however, with the implementation of standard computer security procedures, such as using up-to-date antivirus programs, anti-spyware software, and always updating one’s software – measures that are all too easy to ignore and forget but are of immense importance. Even then, as noted, none of these measures are fool-proof and should be approached as such.

It is enough for one phone in the meeting to be hacked in order to eavesdrop on a discussion. Additionally, one should take the GPS-system of modern phones into account, which can potentially track the movement of the researcher, compromising the interviewees, and, thus, it should be left at home. It is important to remember that pen and paper are the most secure method during face-to-face communication with the research subject. Alternatively, the researcher should use a recording device that does not connect to the Internet. That being said, moving from the phone network to Signal in order to coordinate meetings provides a higher degree of security, as well as doing online interviews over Jitsi rather than Skype. Given that WhatsApp is already ubiquitous, it will probably be stress-free to use as a communication platform without raising any issues for one’s self or one’s sources. For transcribing and storing data collected, the Tails Operating System provides several useful features beyond access to the Tor network, which are so important they should be discussed separately in the next part of this article. These are also relevant for the section on the means to secure information storage.

Tails is a live operating system. That is, the researcher can download and install it on a flash drive or SD card, or burn it onto a DVD rather than installing it onto the computer itself. It is also amnesic, meaning that all of the activity that takes place on Tails takes place in the RAM (Random-access memory) of the computer and is automatically erased when the system shuts down, leaving no trace. This means that Tails can be executed through, for example, a

flash drive on one's own computer, someone else's computer, or a public computer at an internet cafe or library to do work while at the same time leaving no trace on the computer that one is using (Tails Development Team, 2017a). While the amnesic nature of the system prevents the user from saving their work on the computer, it does allow one to save the work that one does on a second USB or SD card, or burn it onto a CD or DVD. If one is in a situation where using Tor does not present a risk, one can use Tails to connect to the Internet through the Tor network, as Tails forces all Internet connections to go through Tor in order to provide anonymity to the user (Tails only connects to the Internet if the user explicitly requests it). Further, because of the amnesic nature of the system it is possible to listen to and transcribe interviews, or even write an entire paper while in the field without leaving a trace of it on any machine. This usage of Tails, while not frequently discussed, is further facilitated by audio software, scanning software, graphic design software, and the complete Libre Office suite (which is compatible with Microsoft Office), all of which is included in the Tails download package (Tails Development Team, 2017a, 2017b, 2017c, 2017d, 2017e).

Installation of Tails on a USB or SD card (as opposed to on a DVD) provides the option of saving information on the USB drive or SD card in an encrypted persistent volume set up by Tails on booting. This allows one to keep everything on one USB drive if one chooses, however the Tails website warns against doing this unless absolutely necessary, explaining that

The [fact of the existence of the] persistent volume is not hidden. An attacker in possession of the device can know that there is a persistent volume on it. Take into consideration that you can be forced or tricked to give out its passphrase. (Tails Development Team, 2017f)

If the researcher is using a personal computer and cannot or does not want to send the data or writing over Tor, use of the persistent volume on a USB is a very feasible option. However, the USB is vulnerable to malware if one is using a public computer – a vulnerability that is greatly reduced by using Tails on a DVD, which still allows one to either use Tor or save one's work to another external media device, which the user is still responsible for encrypting (and which is still vulnerable to malware). The researcher should decide what works best based on their threat model.

Summary

According to the UNESCO-published report “Building Digital Safety for Journalism” – determining what impact, if any, government surveillance has on writers and journalists – a substantial number of PEN International's members, a worldwide association of writers, now assume that their communications are monitored. Accordingly, the assumption of being monitored have dire consequences as it proves to harm the freedom of expression by prompting writers to self-censor their work in multiple ways. Examples are the reluctance to write or speak about certain subjects or to pursue research about certain subjects, and the reluctance to communicate with sources, or with friends abroad, in fear of endangering their counterparts (Henrichsen, Betz, & Lisosky, 2015, pp. 22-23).

Given the increasing pervasiveness of surveillance, it is safe to assume that both researchers and research subjects will make these same assumptions or share the same concerns. These are conditions that the researcher has great difficulties altering or preventing. However, a rigorous and transparent set of cybersecurity practices, which are openly shared with research subjects and interviewees, can go far in mitigating these concerns and the chilling effects that they have on research and informant disclosure.

Simultaneously, the new possibility-spaces of the cyber-infrastructure also provides, on the one hand, new opportunities for both research, and cultural and linguistic exchange. Given these developments, virtual exchanges will most likely become a more common and more developed form of pedagogy for both teaching languages and cultures. Videoconferencing, too, will become a commonly used tool for both research and pedagogy. However, this will merely shift these issues of security and logistics from the physical realm to the technological realm.

Grappling with these issues will require considering a number of factors and will require a wide range of possible solutions based on the threat model of one's project. If one is conducting a virtual exchange, for example, simple awareness of the nature of surveillance, open and direct communication with one's virtual exchange partners about topics and forms of communication that might be problematic and enacting reasonable privacy measures may be sufficient. If, instead, one is doing a research project on activists in a country with a repressive government and traveling to said country to do interviews, additional measures may be necessary to protect both one's data and one's informants.

While the contemplation of cybersecurity measures vis-à-vis academic research may cause one to be fearful or worried about doing research, it is important to note that the same developments enabling structures of surveillance also enable the means to circumvent them. As has been noted in this article, cryptography, for example, may enable a potential shift in power dynamics in favor of the vulnerable. Through the understanding and implementation of appropriate cybersecurity tools, academia may potentially stand more prepared to challenge the threats against its integrity and duties. The tools and suggestions provided in this article are not meant to be an exhaustive list. After all, the development of new tools is constant. Instead, by providing a certain segment of tools, we have attempted to show that one does not have to be an expert in coding or computers in order to implement the minimum level of security. It is up to each researcher to determine what tools are required and sufficient, and from there develop and refine the security measures necessary to engage responsibly with the scientific endeavor. No researcher faces the exact same situation, and the threat assessment must correspond to the tasks (and challenges) at hand. For example, as the Electronic Frontier Foundation (2014b) writes, "if you are facing a government that regularly jails dissidents because they use encryption tools, it may make sense to use simpler tricks." As shown by Dorroll's case, if the implementation of an excessive number of tools may attract unwanted attention, then one should also avoid doing so. Cyber-security tools must be employed when deemed efficient and feasible, and not for the sake of it.

No matter how we choose to employ security measures according to our academic and ethical duties, it is clear that we must look at these measures in the context of our research methods, topics, and subjects. To implement new digital security-measures may take time, effort and will for researchers without prior experience, yet, with the Snowden leaks and the revelations of all-encompassing surveillance, it is not sufficient to state that we did not know about the dangers.

References

- Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, 8(2), 121-144.
- DEFCON. (n.d.). *DEF CON® 25 Hacking conference - Call for papers*. Retrieved from <https://www.defcon.org/html/defcon-25/dc-25-cfp.html>
- Doughman, N., & Al-Sarabi, S. (2012, June 2). "Do you feel more Arab or more American?": Two women's story of being detained and interrogated at Ben Gurion. Retrieved from <http://mondoweiss.net/2012/06/do-you-feel-more-arab-or-more-american-two-arab->

- [american-womens-story-of-being-detained-and-interrogated-at-ben-gurion/](#)
Electronic Frontier Foundation. (2014a, August 1). *Assessing your risks*. Retrieved from <https://ssd.eff.org/en/module/introduction-threat-modeling>
- Electronic Frontier Foundation. (2014b, September 13). Want a security starter pack? Retrieved from <https://ssd.eff.org/en/playlist/want-security-starter-pack>
- Flaccus, G. (2017, February 18). *Electronic media searches at border crossings raise worry*. Retrieved from <https://apnews.com/6851e00bafad45ee9c312a3ea2e4fb2c/electronic-media-searches-border-crossings-raise-worryguide.pdf>
- Harcourt, B. (2015). *Exposed: Desire and disobedience in the digital age*. Harvard, MA: Harvard University Press
- Henrichsen, J., Betz, M., & Lisosky, J. M. (2015). *Building digital safety for journalism: A survey of selected issues*. Paris, France: UNESCO.
- Jitsi.org. (2017, March 8). *Jitsi Meet*. Retrieved from <https://jitsi.org/Projects/JitsiMeet>
- Leaning, J. (1996) War crimes and medical science. *British Medical Journal*, 313(1413). Retrieved from <http://www.bmj.com/content/313/7070/1413.short>
- Lee, M. (2016a). *Security tips every signal user should know*. Retrieved from <https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/>
- Lee, M. (2016b). *Battle of the secure messaging apps: How signal beats WhatsApp*. Retrieved from <https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>
- Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, 1(2), 1-13.
- Marx, G. T. (2016). *Windows into the soul: Surveillance and society in an age of high technology*. Chicago, IL: The University of Chicago Press.
- O'Brien, D. (2015). *Technology security*. Retrieved from <https://cpj.org/reports/2012/04/technology-security.php>
- O'Driscoll, A. (2017). *Where are VPNs legal and where are they banned?* Retrieved from <https://www.comparitech.com/vpn/where-are-vpns-legal-banned/>
- Orb, A., Eisenhauer, L., & Wynaden, D. (2000). Ethics in qualitative research. *Journal of Nursing Scholarship*, 33(1), 93-96.
- Paech, V. (2009). A method for the times: A meditation on virtual ethnography faults and fortitudes. *Nebula*, 6(4), 195. Retrieved from <http://www.nobleworld.biz/images/Paech.pdf>
- Rogaway, P. (2015). *The moral character of cryptographic work* [Presentation]. Paper presented at *AsiaCrypt 2015*. Auckland, New Zealand.
- Smith, A. (2015). Not-seeing: State surveillance, settler colonialism, and gender violence. In R. E. Dubrofsky & S. A. Magnet (Eds.), *Feminist surveillance studies* (pp. 21-38). Durham, NC: Duke University Press. <https://doi.org/10.1215/9780822375463-002>
- Tails Development Team. (2017a, August 8). *Tails - About*. Retrieved from <https://tails.boum.org/about/index.en.html>
- Tails Development Team. (2017b). *Tails - Graphics*. Retrieved from https://tails.boum.org/doc/sensitive_documents/graphics/index.en.html
- Tails Development Team. (2017c). *Tails - Office suite*. Retrieved from https://tails.boum.org/doc/sensitive_documents/office_suite/index.en.html
- Tails Development Team. (2017d). *Tails - Printing and scanning*. Retrieved from https://tails.boum.org/doc/sensitive_documents/printing_and_scanning/index.en.html
- Tails Development Team. (2017e). *Tails - Sound and video*. Retrieved from https://tails.boum.org/doc/sensitive_documents/sound_and_video/index.en.html
- Tails Development Team. (2017f). *Tails - Warnings about persistence*. Retrieved from https://tails.boum.org/doc/first_steps/persistence/warnings/index.en.html

- The Tor Project, Inc. (2017). *Tor Project: Overview*. Retrieved from <https://www.torproject.org/about/overview.html.en>
- van der Velden, L. (2015). Leaky apps and data shots: Technologies of leakage and insertion in NSA-surveillance. *Surveillance & Society*, 13(2), 182-196
- Verizon. (2016). *2016 Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
- Zelezny-Green, R. (2016). "Can you really see what we write online?" Ethics and privacy in digital research with girls. *Girlhood Studies*, 9(3) 71-87. <https://doi.org/10.3167/ghs.2016.090306>

Author Note

Jedidiah Anderson is a Visiting Assistant Professor at Furman University. He is currently preparing his book, *Sexual Intifada Now!*, an ethnography of LGBTIQ activists in Lebanon, Iraq, and Israel/Palestine for publication with Indiana University Press. His work focuses on minority groups and transnational identities in the Arab World. Correspondence regarding this article can be addressed directly to: jed.anderson@furman.edu.

Erik Skare is a PhD Fellow at the University of Oslo. He is currently preparing his dissertation on the Palestinian Islamic Jihad movement, its history and developments. He wrote his master's thesis at the University of Oslo on Palestinian hackers and their targeting of the Israeli cyber-infrastructure, which was published by Zed Books with the title *Digital Jihad: Palestinian Resistance in the Digital Era*, October 2016. Skare's research focuses on the Palestinian violent and non-violent resistance against the Israeli occupation. Correspondence regarding this article can also be addressed directly to: erik.skare@ikos.uio.no.

Courtney Dorroll is an assistant professor of Middle Eastern and North African Studies and Coordinator of the MENA Program (<http://www.wofford.edu/MENA/>) at Wofford College, a liberal arts institution in Spartanburg, SC. Courtney is currently the executive director of the Wofford/MENA Virtual Exchange which links Wofford students through social media and new communication technologies to students in Beirut and Cairo. Her research focuses on pedagogy, ethnography and new media. Correspondence regarding this article can also be addressed directly to: dorrollcm@wofford.edu.

This work was supported by the Aspen Institute under the Stevens Initiative.

Copyright 2018: Jedidiah Anderson, Erik Skare, Courtney Dorroll and Nova Southeastern University.

Article Citation

Anderson, J., Skared, E., & Dorroll, C. (2018). Nothing to hide, nothing to fear? Tools and suggestions for digital data protection. *The Qualitative Report*, 23(5), 1223-1236. Retrieved from <https://nsuworks.nova.edu/tqr/vol23/iss5/14>
