<cn>12

<ct>Researching the emergent technologies of state control

<st>The courts-martial of Chelsea Manning

<au>Sarah M. Hughes and Philip Garnett

<bl>

* **Research objective**: This chapter has two objectives. The first is to critically analyse the multiple technologies by which state actors work to influence a narrative surrounding an event or process. The second is to attempt to ground this analysis within the context of leaked data, through the court-martial of Chelsea Manning.
* **Research puzzle**: This chapter helps researchers who want to navigate the challenges of working with state secrets that are leaked and therefore in the public realm, but which are technically still classified.

# <a>Introduction

<text>The number of high-profile cases of whistle-blowers in recent years presents a novel challenge for security researchers. What methods can be applied in order to research leaked state secrets that are now in the public realm? This chapter will help researchers who are confronted with the particular methodological difficulties associated with obtaining or publishing publicly accessible data that the state (or other organisations) may wish to obscure. Such data may be leaked, readily available on the Internet, and yet never have been declassified. The data may also have been released through Freedom of Information Act requests (FOIA) and be redacted or hidden on poorly implemented websites that are not easily searched. For this chapter we adopt an ethnographic approach to the research of these digital technologies, which include: large document datasets, website security certificates, search engine algorithms, and redacted FOIA documents.

Drawing upon our own research dilemmas whilst researching the court-martial of whistle-blower Chelsea Manning, in this chapter we map out a series of *obfuscating emergent technologies of state control*, (the difficulties that surround accessing publicly ‘available’ data via poorly constructed FOIA reading rooms, redactions and files downloads) and we comment upon the implications of these for security researchers in this field. Our ethnographic approach to the digital technology in the context of state secrets allows us to map our encounters with the inconsistent and emergent actors involved within the obfuscation of this data. We therefore detail to other researchers the challenges we faced, and the methods we arrived at to critically interrogate public access to information about Chelsea Manning’s court-martial.

This chapter therefore engages with the following questions:

<bl>

* What ethical, practical and technological challenges do researchers face when they wish to use leaked materials for their research?
* What tools can researchers use to map secrecy through an attention to technologies of state control?
* What methodological challenges face researchers who aim to access public data that the state wishes to hide?
* How can researchers navigate such a complex, ethically and politically charged field?
* What strategies can researchers deploy to avoid paranoia when researching secret state technologies?
* How can, or should, researchers publish their findings from this data?

|  |
| --- |
| <box\_head>**Box 12.1 Terminology**  <box\_bl>   * *Emergent technologies of state control:* We understand the state to be multifaceted and inconsistent (Gill 2010; Mountz 2013), continually performed through the dynamic interplay of multiple actors. Therefore when exploring the technologies of state control, we see these systems, procedures and programs in the context of an always-already incoherent and emergent state persisting beyond the duration of the actors that comprise it. * *Obfuscation*: A clouding over, a procedural darkness and/or a lack of clarity over the access to legally available data. Obfuscation differs from obstruction, as there may be no singular point or moment of refusal, rather a series of emergent practices that arise through an assemblage of state actors. |

# <a>The court-martial of Chelsea Manning

<text>Private Chelsea Manning was arrested by the US government in May 2010, charged with leaking classified military material to Wikileaks. Intelligence analyst Manning was later convicted in 2013 of a series of offences, including violating the 1917 Espionage Act and stealing government property. Initially sentenced to 35 years in military prison, Manning was released on 17 May 2017 after her sentence was commuted to time served in the final days of the Obama presidency. Between January and May 2010 Manning leaked approximately 750,000 documents to WikiLeaks. Among this material was the 2007 Baghdad airstrike video showing the killing of two Reuters correspondents (which has subsequently been termed ‘collateral murder’), the 2009 Granai airstrike in Afghanistan, and 400,000 documents that came to be known as the Iraq War Logs (James 2014). Constituting one of the largest ever data leaks in the military/security realm, over a million documents. These documents ranged in classification from UNCLASSIFIED up to SECRET/NONFORN (not to be shared with foreign nationals) (US Department of Defence 2011). No TOP SECRET information was released. These documents, including state department diplomatic cables, provide evidence of the officially sanctioned cover-up of rape and sexual torture (including of children) by military contractors, and the indiscriminate shooting of Iraqi civilians and those attending to their injuries.

Manning was convicted by courts-martial; under military rather than civilian law (the Uniform Code of Military Justice). This is important to consider methodologically as the proceedings of courts-martial are not routinely published; and although the judge has some discretion to release records it is the prosecution that is responsible for the release of information. Therefore, for full access it is necessary for the media to be physically present to report on trial proceedings, for which they need accreditation from the military before entering the court room. In the case of Chelsea Manning, one journalist, Alexa O’Brien, took and published detailed notes of the proceedings online (O’Brien 2017). She was able to file over 100 FOIA requests for official documents and transcripts of the court-martial, which have been uploaded to the US Army’s FOIA reading room. However, many challenges remain for the researcher in accessing this unclassified data on the trial which is now ‘publicly available’, and yet obfuscated through a series of emergent technologies of state control which we will continue to unpack later in this chapter.

|  |
| --- |
| <box\_head>**Box 12.2 From the Pentagon papers to WikiLeaks: leaked data in an Internet age**  <box\_text>One of the most famous large scale leaks of the twentieth century was the Pentagon Papers in 1971 (Ellsberg 2003); a 47 volume largely ‘Top Secret’ report produced by the United States Department of Defense as a history of the US’s political and military involvement in Vietnam from 1945 to 1967. In order to leak the documents US military analyst Daniel Ellsberg manually photocopied all 7000 pages, a process that took weeks to complete (Ellsberg 2003).  Since the Pentagon Papers, the advent of the Internet has fundamentally changed the scale and nature of document leaks. The digitisation of state processes has significantly changed the conditions through which data is released, as (access permitting) it is possible to make perfect digital copies of documents and other materials. Further, this data can be disseminated via online platforms, including the WikiLeaks website, a cryptographically secured leaks platform that takes advantage of this relative ease with which documents can be copied and transported electronically (WikiLeaks 2015). Leakers anonymously access the ‘dark web’ service submission website using The Onion Router (TOR) (Dingledine, Mathewson, and Syverson 2004), and deposit files for WikiLeaks to publish.  We can assume that the WikiLeaks dark web submission point was how Chelsea Manning was able to transfer 750,000 files from two databases to Wikileaks. A leak on this scale would have been practically impossible in 1971, as it would have taken months to photocopy 750,000 pages of documents, and physically moving them would be challenging. In contrast, Manning was able to copy an entire database onto a single CD-ROM, marked Lady Gaga, and walk out with it in a portable CD player (Leigh 2010).  The Internet brings further opportunities and constraints for disseminating leaked data. As the Pentagon Papers were classified, the *New York Times* and later the *Washington Post* had to go through the courts to publish with them. To further safeguard the possibility of public debate about the content of the papers then US Senator Mike Gravel asked Howard Zinn and Noam Chomsky to produce an edited portion of the papers (United States Department of Defense et al. 1971). This resulted in 4,100 pages of the papers being entered into the record of his Subcommittee on Public Buildings and Grounds (Gravel 1972); the full 7,000 pages were only declassified by the US Government in 2011 (“Pentagon Papers” 2016). In contrast, all the data leaked by Manning remains intact and available, if somewhat in limbo; it remains classified and is accessible on the WikiLeaks website. However, as we have written elsewhere (Garnett and Hughes 2019) it is not entirely clear how easy it would be to publish with the data which has not been declassified.  The recent Paradise and Panama Papers released by the International Consortium of Investigative Journalists (ICIJ) are different again in their scale (11.5 million and 13.4 million documents respectively). Impossible to photocopy, and significantly beyond the capacity of CDs, and most flash drives, these datasets present additional challenges to researchers with respect to access, raising questions of how to effectively approach, analyse, publish data of this scale. |

# <a>Research design and methodology

<text>Our research emerged from a recognition that Manning’s court-martial, and the data that she leaked to Wikileaks have received scant attention within the academy (see Garnett and Hughes 2019). This is, however, important to explore, in the context of claims reported by Julian Assange that: “the ISA has banned the single most significant US foreign policy archive from appearing in its academic papers...” (Assange and Others 2015). We were not interested in ‘testing’ Assange’s claims here; instead we focused upon the politics of knowledge curation in the context of an ambiguous and incoherent state.

We therefore draw a distinction between the two *forms* of data concerning state secrets that are relevant here: first, data that has been leaked by a whistle-blower and has not been declassified; second, data that the state has been forced to release, but otherwise would not have done so (e.g. through a FOIA request). In the case of Chelsea Manning, both forms of data are relevant here; the files that were leaked to Wikileaks, and the subsequent FOIA requests regarding her court-martial and treatment by the US military. This distinction is important; whilst both state secrets that are now in in the public realm, the technologies of state control used to obfuscate access to, or publishing on this data are different.

With this in mind, we depart from mainstream approaches for engaging with the state in security research. The information is publicly accessible; it is just not readily so. Indeed, we understand ‘the’ state to be emergent, and comprised of multiple actors (also Dijstelbloem and Pelizza this volume). There are many US government actors enrolled into Manning’s case including: the military tribunal staff at Fort Leavenworth; staff at the FOIA request department and website maintenance staff. Individuals people the state (Medby 2016). In addition, the state is also comprised of multiple material actors. These lively, agentic materials exceed and extend the spaces of politics beyond the traditional sites of the state. For example, the contents of the US army’s FOIA reading room cannot be picked up by a search engine, providing additional challenges for the security researcher. Splintering the definite article of ‘the’ state reveals an emergent and inconsistent assemblage that cannot be determined *a priori*. For security researchers attempting to access publicly available state secrets, this means starting from an acknowledgement that there is no singular point of refusal. In short, questions about ‘access’ raise important epistemological, ethical and political questions about the place of research in, on and with public state secrets. The state has obfuscated aspects of the production and release of this data and therefore the research is approached *obliquely*. By framing this research as oblique we are not claiming that access would a give a researcher a ‘full view’, for in some way most research is from an oblique angle (see Belcher and Martin, this volume).

We therefore adopted an ethnographic approach (including interviews, observation and autoethnographic reflections) to researching Manning’s court-martial. We chose this methodological approach to allow for a commitment to an inductive and iterative epistemology and to align with our understanding of an emergent state. Ethnographic methods can be considered more of an approach to research rather than a specific set of methodological practices. We conducted an autoethnography of our own interactions with state technologies and semi-structured interviews with actors involved within Manning case. This aligns with the framing of this research process as oblique; in the knowledge that we were encountering fragments of ‘the’ state which were already obfuscated. An ethnographic approach allowed us to these map obfuscating practices as they emerged and were encountered.

In the following sections, we unpack how these approaches played out during our research, and make suggestions for future researchers encountering the emergent technologies of state control. We look at this through the nuances of access to the US Army’s FOIA Reading Room website.

## <b>Example: access to the US Army’s FOIA Reading Room website

<text>As previously mentioned, when courts-martial are undertaken by the US military there is no public record of the trial; the prosecution can decide what is released. This does not mean, however, that there is no way for a researcher to access a transcript, for requests in the US can be made under FOIA. It is important for researchers to note, however, that FOIA requests have to be very specific (e.g. asking for documents that are known to exist) to avoid being rejected for being too broad. This requires a clear and detailed understanding of the form of the materials requested (e.g. in the US you usually require the subject, timeframe, individuals involved and a reason why that department will have that information). As a journalist who had attended the trial submitted 25 FOIA requests for access to the court-martial transcript specifically, and more than 100 requests for the proceedings as a whole, we did not submit our own FOIA requests. It is standard practice with US FOIA requests that the data that was permitted to be released was redacted to protect state secrets before being uploaded to the US Army’s FOIA Reading Room website.

Our ethnographic research on encountering technologies of state control, identified a tension between democratic public accountability and obfuscating practices in our attempts to access the US Army FOIA website. At the time of writing this chapter, we note that there are elements of the construction of this website that make it appear risky for the researcher (or any member of the public) to access. We documented this as part of our autoethnographic research methods. When arriving at the website, the visitor is warned of a lapsed certificate with an alert stating that “Your connection is not private” and an additional warning that there is the possibility that the site may be being used by ‘attackers’ to steal the visitor’s information and potentially their identity (see Figure 12.1)[[1]](#endnote-2).

**<FIGURE 12.1 ABOUT HERE>**

<caption>Figure 12.1 Screenshot of attempt to access the US Army's FOIA website [28 November 2018]

<text>This warning, we suggest, is likely to encourage many users to leave the site, nor attempt or know how to go any further. Previously, when using Chrome to get beyond this warning the user had to select the ‘advanced’ button, which is concealed on the left-hand-side of the alert message and greyed out. After selecting this ‘advanced’ option could user create a security exception and accept the expired security certificate, however this was accompanied by an additional warning about the potential hazards of proceeding to the site (Figure 12.2, Garnett and Hughes 2019). Only then can a user proceed to the website and the location of the documents. At the time of writing however, it has not been possible to access the US Army’s FOIA Reading Room via Chrome[[2]](#endnote-3) for at least six months (see Figure 12.3).

**<FIGURE 12.2 ABOUT HERE>**

<caption>Figure 12.2 Screenshot of attempt to access US Army's FOIA website [24 November 2016]

**<FIGURE 12.3 ABOUT HERE>**

<caption>Figure 12.3 Screenshot of attempt to access US Army's FOIA website [23 May 2018]

<text>The FOIA website itself has a clear layout and information on the documents filed there (e.g. the title, filename and some metadata). Yet attempting to download documents on the website reveals further difficulties; whilst the website does list individual documents that can be searched from within the site, the functionality is limited, for the searchable metadata (such as keywords) is restricted. Additionally, many of the documents (although, not all of them) are stored in ZIP files that are frequently in excess of 1 gigabyte. The files do not report their size to the web browser, which means that a visitor is unable to determine how long the download will take, nor the final size of the download (see Figure 12.4). When downloaded the files are redacted and difficult to search, for they are frequently images embedded within PDFs. We suggest that some visitors may consider abandoning the download due to the previous warnings cultivating a fear that the files are somehow corrupted.

**<FIGURE 12.4 ABOUT HERE>**

<caption>Figure 12.4 Screenshot of file downloading from the US Army's FOIA website [24 November 2016

<text>Our autoethnographic reflections on attempting to access the US FOIA website, are an example of where our reflections on government (in)actions could be labelled as aligning with conspiracy. However, as this is a website where the US Army disseminates information released in response to a FOIA request, it is not unreasonable to make the assumption that this is information that they would not willingly release. Perhaps it is in their interest to obscure access to this information; to make it harder for interested parties to research this data? Clearly, making their website easily accessible is not a high priority; for this has been the case since at least March 2016.

Importantly, however, that does not necessarily mean that these difficulties in accessing the files have been *intentionally* created. For example, the website’s security certificate may once have been valid, and when it expired its renewal may have been caught between the multiple actors comprising an (in)coherent bureaucratic assemblage. Similarly, the large ZIP files may be a reflection of the amount of time the creator of the content was willing to spend on building the database. This is therefore not likely to be a deliberate attempt to put people off downloading the files, for to create metadata for and upload every file individually would be a significant task. Perhaps therefore the state of the website reflects convenient neglect. As consequence of this complication, however, access to this data becomes *obfuscated*.

|  |
| --- |
| <text>**Box 12.3 Researcher in practice: on feeling like a conspiracy theorist**  <box\_text>From our experiences, the work of researching technologies of state control over publicly available data can make you feel paranoid. The lack of clear refusal of access, the delays, lack of responses and bureaucratic confusion can be helpfully understood through an understanding of ‘the’ state as inconsistent and emergent. However, this did not necessarily negate our concerns of being labelled as ‘conspiracy theorists’, joining dots into phantom shapes to make unsubstantiated claims about state practices.  We follow Hyndman (2001: 265) who argues in her feminist critique of traditional conceptions of Geographical fieldwork, that “there is value in working through the messiness, engaging in fieldwork in a careful manner, rather than writing it off as too fraught with difficulties and dangers. Imperfect engagement is better than no engagement, or a paralyzing angst”. In recommending that researchers remain with this discomfort and unease, we are not arguing for grand claims about illicit state practices, but instead suggesting the value in making these moments of obfuscation and confusion visible. This is important, first, because it is through encounters with state actors that researchers can come to learn about the technologies of state control and secondly, as it is through making this visible that we can hold democratic public institutions to account (Belcher and Martin 2013). |

# <a>Implications and suggestions for security researchers: politics, ethics practicalities

<text>What the above example from our research process reveals about researching the emergent technologies of state control is that an outright refusal of access, or a clear path of obstruction would likely be identifiable and therefore easier to write about. In contrast, the obfuscating practices that we were both researching and experiencing are emergent; they arise from encounters with facets of the state and its technologies. It is only through asking that you do not get a reply; only when attempting to access a website that you find difficulties. Technologies of state control are emergent, for they only arise when the researcher rubs up against, challenges or encounters aspects of the state apparatus. This makes these technologies hard to identify *a priori* and to capture through the research process.

In addition, and importantly for the academy, the data that Manning leaked has never been declassified. This raises a series of additional dilemmas for security researchers regarding the place of such data within academic journals. This is further complicated in the context of a series of claims made by Julian Assange, editor-in-chief of WikiLeaks that: “... the poverty of coverage in American international relations journals appears not merely odd, but suspicious.” (Assange et al., 2015, p. 10), leading others to observe that “[t]here has been an effective embargo on the use of those materials for research by US academics who fear sanctions by US authorities if they as much as access them” (Mair, 2016). We have written elsewhere on the relative lack of attention given to Manning’s case within International Relations and Political Geography and the possible reasons for this (Garnett and Hughes 2019). However, the *International Studies Association (ISA)* have responded to wider claims of this nature noting:

<ext> It has been discussed among the ISA journal editors in the context of any legal issues related to materials used from WikiLeaks. That discussion centered on the implications of publishing material that is legally prohibited by the US government … But no policy has been made and the issue has not been widespread in journal submissions.

<source>(Boyer, in Norton 2015)

There have been cases of high profile US universities activity discouraging students and staff from engaging with the materials; a leaked email from Columbia University’s School of International and Public Affairs (SIPA) advised the below (see Figure 12.5).

**<FIGURE 12.5 ABOUT HERE>**

<caption>Figure 12.5. Email from Columbia University’s SPIA

<credit>(Gustin 2010)

<text>This further demonstrates the relationship between the academy and the state; for this took the form of warning students that the use of leaked material might bring into question their suitability for handling government materials, and therefore by implication suggesting that they might damage their future employability (Figure 12.5). This advice, including the email from Columbia University’s SPIA, was retracted soon after it was released [(Gustin 2010)](https://paperpile.com/c/ErdNiY/C4Vf). In short however, there is a lack of clarity for researchers as to the methodological possibilities and implications for research in this area that resonate beyond the specifics of this example.

## <b>Politics

<text>In the absence of any written guidelines on the publishing of publicly available classified material within academic journals, we got in contact with editors of Political Geography and International Relations journals to request whether they had any specific policies regarding this. For example, could a researcher publish a screenshot of the video of the Baghdadi airstrike ‘collateral murder’, which depicts the indiscriminate shooting of Iraqi civilians, Reuters’ staff, and two children by US military forces in an Apache helicopter, including the audio recordings from the cockpit? This video is widely available on the Internet; a simple Google search will bring up a Wikipedia page with a screenshot and link to the video. Yet this material is classified and is therefore still technically a state secret. What then is the role of the researcher, and the wider academy in response to this?

Of those journal editors who replied, most expressed that they did not have a particular policy on this, and that individual cases were dealt with by the editorial board as they arose. They all stated that this was not a problem they commonly came across (if indeed, they did at all), and therefore it is likely that this situation does not merit a journal policy. One editor commented that they had not received a paper dealing with leaked material, but compared this discussion around the ethics of classified data to a conversation they had had regarding the (re)publication of the cartoon of Prophet Muhammed that had originally appeared in the Danish newspaper *Jyllands-Posten*.

## <b>Ethics

<text>There are significant ethical implications to consider when attempting to engage with, or publish on leaked data. Those potentially impacted by this include: the whistle-blower, publisher of the leaked data, those named in the leaked data, the researcher, their research team, institution and colleagues. This is not to say that security researchers should not engage with leaked data, for this is a critical part of holding the state to account, yet this research is located within a constantly changing politically and ethically charged field.

What this means is that it becomes challenging to deploy a pre-existing ethical framework to work with leaked data (see in this volume Hoijtink; Amicelle, Badrudin and Tanner). Instead, we find it helpful to follow Butler’s account that “ethics requires us to risk ourselves precisely at moments of unknowningness” (2005: 136). Ethics, Butler argues, begins at the edges of sensibility; it is only by acknowledging our own incoherence, the impossibility of being able to give an account of ourselves, that we can begin a “conception of ethics, and indeed, responsibility” (2005: 19). When framed in this way, ethics emerges at the point where the research route becomes unclear, where the researcher takes a step into the unknown. In the context of working with leaked data, has implications for the practical steps that can be taken by the researcher.

## <b>Practicalities

<text>Working with leaked data requires starting the research with different and difficult questions. From our experiences with the Manning data, which cannot simply be extrapolated to other geopolitical contexts, we make the following recommendations for researchers intending to publish within this complex and political area of research:

<nl>

1. The researcher must approach the topic in the realisation that their work is part of a wider process of knowledge curation, that they are working from an oblique angle whereby many aspects of traditional research design, ethics, methods and dissemination cannot simply be applied. For example from our research on Chelsea Manning, we started from the assumption that the researcher will likely encounter incoherent fragments of a dispersed and disparate state.
2. Prior to engaging with the leaked material, it is – of course – imperative to research the context of the data leaks. Why was this data leaked? What have the implications of this been for the whistle-blower, those named within the data, and the state institutions that have been impacted? What are the potential political and individual implications of further scrutiny of this data in the academy? Whilst the need to hold states to account for their actions may be the rationale for some critical security research, the researcher must think through the possible implications of their research in this field.

<text>It can be challenging to conduct a project with the understanding that the research process is oblique. Further, it is hard to document the obfuscating technologies of state control whilst simultaneously recognizing that these technologies emerge and become visible as a result of the research process. We found that conducting autoethnographic research was beneficial for balancing this tension within the research design. In taking detailed, self-reflexive notes of our own thoughts and actions throughout the research process we were able to build up two research diaries that captured our own encounters with state technologies. We found this helpful to navigate what was at times a confusing and disorienting process. It was also useful to have a record of our own encounters with technologies of state control, for example the screenshots of website access.

Furthermore, as previously noted, the publication of classified data within academia books and journals is a grey area, both legally and ethically. Therefore, we suggest to future researchers who are aiming to publish their research, that they contact relevant journal editor(s) well before submitting. In particular, for those publishing classified data that has been leaked from non-democratic (or potentially hostile) states, we strongly recommend taking legal advice on the implications of this on your future travel, access and employment. In addition advice should be sought on the possibility of further reproductions on the leaker and those named in the leaks. Our advice here would be to consider whether you need to include the data within your work, or whether can you signal this to the reader to find themselves. This will depend, of course, upon the nature of your research, epistemology and methods used. In short however, whilst we do not think that critical security researchers should shy away from pushing the academy to have difficult conversations on the place of leaked data, the researcher must be proactive in taking measures to prevent the potential repercussions of this.

# <a>Reflections

<text>The last decade has been characterized by whistle-blowers, with large deposits of publicly accessible, and still classified, state secrets. At the same time, the online documentation of FOIA requests has resulted in further repositories for redacted data that the democratic state has been forced to release. In this chapter we reflected upon these two forms of data: leaked classified data that has entered the public realm, and data that the state has been required to make public.

We explored the technologies of state control that emerge to control, curtail and obfuscate access to this data. Drawing upon our own research into the attention that the court-martial of Chelsea Manning has received in the academy, we reflected upon the ethical, political and practical dilemmas that we encountered, to give advice to future critical security researchers working in this field. First, we identified that it can be helpful for work in this area to theorize the state as multifaceted and inconsistent, an assemblage of multiple, heterogenous actors. This is because when conceptualizing the *technologies* of state control an understanding of these systems, procedures and programs as fragments of an emergent ‘whole’ can assist the researcher in processing their experiences. Technologies of state control are emergent; they arise through a researcher’s interaction with disparate parts of the state apparatus. Second, we frame these emergent technologies as a form of *obfuscation*. By this we mean that the incoherent state does not act with a singular intention; there is no singular point of refusal of access to, or to publishing on this data. Instead, it is possible to map, or document these areas of procedural darkness to address the politics of the lack of clarity over the availability of this data for researchers.

We therefore adopted ethnographic methods, in particular autoethnography, as a means by which to chart these emergent technologies. We utilized autoethnographic reflections from our work attempting to access the US army’s FOIA Reading Room. Commenting upon a series of what we term obfuscating technologies of state control, we note the difficulties accessing the website, the lapsed security certificates, lack of metadata, undisclosed file sizes and documents saved as redacted JPEGs saved within pdfs, making it challenging for the researcher to search. We drew out the implications of this for the security researcher, discussing the merits of framing these technologies as emergent and the consequent value of autoethnographic work within this area. From this we moved to examine the ethics, politics and practicalities of publishing classified data that has been leaked to the public. Utilizing our experiences and discussions with journal editors around the place of classified material within the academy, we advised future researchers to place their research within wider discussions of knowledge curation, to critically interrogate the context of the leaked data and to seek clarification from journal editors and – if necessary – lawyers before moving to publish in this field. We end by noting that mapping the emergent technologies of state control in the context of *publicly available* state secrets is a new and unchartered terrain. In a digital age, the rise of mass data leaks is likely to continue to increase, posing urgent and as-yet unaddressed challenges for critical security researchers.

# <a>Suggestions for further reading

<bl>

* Maillet, P., Mountz, A., and Williams, K. (2017) “Researching migration and enforcement in obscured places: Practical, ethical and methodological challenges to fieldwork.” *Social & Cultural Geography*, 21(7): 927–950.
* Michael, G. J. (2015). “Who’s afraid of WikiLeaks? Missed opportunities in political science research.” *The Review of Policy Research*, 32(2): 175–99.
* O’Loughlin, J., Raento, P., Sharp, J. P., Sidaway, J. D. and Steinberg, P. E. (2015) “Data ethics: Pluralism, replication, conflicts of interest, and standards in *Political Geography.*” *Political Geography*,44(1): A1–A3
* Steinberg, P. E. (2010) “Professional ethics and the politics of geographic knowledge: The Bowman Expeditions.” *Political Geography*, 29(8): 413.
* Suchman, L., Follis, K., and Weber, J. (2017) “Tracking and targeting: Sociotechnologies of (in)security.” *Science, Technology & Human Values* 42(6): 983–1002.

# <a>References

<ref>

Assange, Julian, and Others. (2015) *The WikiLeaks Files: The World According to US Empire.* London: Verso Books.

Belcher, Oliver, and Lauren L Martin. (2013) “Ethnographies of closed doors: Conceptualising openness and closure in US immigration and military institutions: Ethnographies of closed doors.” *Area*, 45(4): 403–410.

Butler, Judith. (2005). *Giving an Account of Oneself*. Oxford: Oxford University Press.

Digicert.com (2017) SSL & PKI Made Easy. *Digicert.* <https://www.digicert.com/> Accessed 6 December 2017.

Dingledine, Roger, Nick Mathewson, and Paul Syverson. (2004). *Tor: The Second-Generation Onion Router*. Washington DC: Naval Research Lab.

Ellsberg, Daniel. (2003). *Secrets: A Memoir of Vietnam and the Pentagon Papers.* Penguin: London.

Gill, Nick. (2010). “New state-theoretic approaches to asylum and refugee geographies.” *Progress in Human Geography*, 34(5): 626–645.

Garnett, Philip and Hughes, Sarah M. (2019) “Obfuscated semocracy? Chelsea Manning and the politics of knowledge curation.” *Political Geography.* (early edition)

Gravel, Mike. (1972). *The Pentagon Papers: The Defense Department History of United States Decision making on Vietnam. Critical Essays and an Index to Vol. 1–4*. Vol. 5. Beacon Press: Boston.

Gustin, Sam. (2010) Columbia University reverses anti-WikiLeaks guidance. *Wired* <https://www.wired.com/2010/12/columbia-wikileaks-policy/> Accessed 5 April 2018

Hyndman, Jennifer. (2001) “The field as here and now, not there and then.” *Geographical Review*, 91(1/2): 262–272.

James, Selma. (2014) “Chelsea Manning joins the army – of whistleblowers*.” QED: A Journal in GLBTQ Worldmaking*, 1(1): 47–51.

Leigh, David. (2010). “How 250,000 US Embassy cables were leaked.” *The Guardian*, 28 November 2010. http://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked.

Medby, Ingrid Agnete. (2016) “Peopling the state: Arctic state Identity in Norway, Iceland, and Canada.” Doctoral thesis. Durham University, 2017. <http://etheses.dur.ac.uk/12009/>. Accessed 25 May 2018.

Mountz, Alison. (2013) “Political Geography I Reconfiguring Geographies of Sovereignty.” *Progress in Human Geography*, 7(1): 1–13.

Norton, Benjamin. (2015) Assange: US Academia Helps the State Department. *Medium* <https://medium.com/@BenjaminNorton/assange-us-academia-helps-the-state-department-ac66b4276778 Accessed 5 April 2018>

O’Brien, Alexa (2017). Alexa O’Brien: Archive <https://alexaobrien.com/archive> Accessed 10 September 2017.

United States Department of Defense, Noam Chomsky, Mike Gravel, and Howard Zinn. (1971). *The Pentagon Papers.* (The Senator Gravel Edition.) *The Defense Department History of United States Decision-Making on Vietnam. vol. 5. Critical Essays.* Edited by Noam Chomsky and Howard Zinn, and an Index to Volumes One-Four. Beacon Press: Boston

“Pentagon Papers.” (2016). National Archives. 15 August 2016. <https://www.archives.gov/research/pentagon-papers>. Accessed 26 June 2018

US Department of Defense (2011) Final Report of the Department of Defense Information Review Task Force. <https://assets.documentcloud.org/documents/3868778/Wikileaks-Manning-Defense-Department-Damage.pdf> Accessed 6 December 2017.

Wikileaks (2015) “What Is WikiLeaks.” <https://wikileaks.org/What-is-Wikileaks.html>. Accessed 26 June 2018.

# <a>Notes

<note>

1. It is worth noting that a SSL certificate for a multi-domain site such as the US government webpages could be purchased for roughly $600 dollars a year (digicert.com 2017), so it is likely they have the capacity to install a valid certificate should they wish. [↑](#endnote-ref-2)
2. Similar situations play out – albeit with different wordings of the warning – in many other major browsers (e.g. Internet Explorer, Mozilla (Firefox) and UC Browser). [↑](#endnote-ref-3)