Big Brother and the Fourth Estate

Source Protection in The Netherlands in an Era of Increasing Digital Surveillance

Job Boonstra
141624

This thesis has been submitted to comply with the regulations for the hbo bachelor in Journalism

Ede Christian University of Applied Sciences, 2019

A special word of gratitude to mum and dad.

Thanks for helping me transcribe my interviews. You did not know what you were getting yourselves into.

Thanks to Martina Piras and Jan-Wouter Dekker for proofreading my writing.
I owe you a drink.

Ede, The Netherlands
June 20, 2019 Job Boonstra

Table of content

i. Introduction

The importance of source protection for journalists cannot easily be understated. Dutch Minister of Justice and Security Ferd Grapperhaus recently stated that "source protection is a *sine qua non* for the free press as servant to our democracy. A journalist that cannot protect his sources is at risk of losing access to those sources and thus is no longer capable of carrying out his job" (Grapperhaus, 2018). His remarks came in the weeks after the gruesome murder on journalist Jamal Khashoggi in the Saudi consulate in Istanbul. The dangers that journalists face were not lost on Grapperhaus when he stressed the importance of a critical, independent press as a fundamental principle of a free and open society. Source protection for journalists has been sufficiently secured within the existing legal framework, according to Grapperhaus, but two high-stakes incidents of a breach of the privilege of source protection in The Netherlands have called that statement into question.

The first is the controversy surrounding the Public Prosecution Service obtaining the private phone records of a journalist writing for Brabants Dagblad. Journalist Jos van de Ven was reporting on the race between two candidates for mayor in the city of Den Bosch and had obtained secret documents through a source familiar with the appointment process (Haenen & Dupuy, 2018). The leaking of secret documents is illegal under Dutch law and the Public Prosecution Service put in a special request to obtain the phone records of the journalist in order to trace the leak, without obtaining a judicial warrant. Although it is not uncommon for governments to crack down on leaks and whistleblowers, obtaining phone records and communications of journalists directly opposes Grapperhaus' dedication to securing the right of source protection for journalists.

Another incident is that of journalist Joey Bremer, whose phone records were illegally obtained in October 2017 and February 2018 by the Public Prosecution Service as part of an investigation into an employee from the Rotterdam police department who was suspected of leaking information. After realizing their error Bremer's phone records were deleted and the investigation was reportedly halted, but Bremer told newspaper Algemeen Dagblad he was shocked and said "How should I explain this to my sources? Being able to provide source protection as a journalist is my greatest asset" (Rubio, 2018).

Finally, a point of concern that also calls Grapperhaus' views into question is the annual World Press Freedom Index, conducted by Reporters Without Borders (2018). The

Netherlands has consistently scored high ratings, ending up in the top five six years in a row, but concerns about a new far reaching law governing intelligence agencies are being noticed. “A controversial Intelligence and Security Services Act (WIV 2017), approved by Parliament in 2017, gives the security services increased powers to decrypt secure communication networks and to tap phones and Internet communication systems. Journalists fear that it could undermine protection of the anonymity of their sources”, the report states.

These past developments, including new legislation that allows Dutch intelligence agencies to intercept cable communications, beg the following questions; are journalists still able to provide their sources anonymity in times of increasing government surveillance? In a society where most of our lives leaves a trail of data, is it still possible to prevent the identity of a source from being revealed to authorities? This thesis aims to shed light on such questions by first examining the current legal framework under which intelligence agencies operate and how they apply surveillance techniques. Secondly, it discusses conflicts of interest between the government’s ‘right to classify’ and the general public’s ‘right to know’, as well as whether journalists are in a position to accurately assess the public’s interest in publishing confidential, highly sensitive material. Finally, this thesis explores what journalists see as a threat to their ability to protect a sources’ identity and what tools they have at their disposal to secure their communications with sources.

ii. Summary

The ability to anonymize sources is one of the most important tools that journalists have at their disposal. Without this, many sources might not dare to speak to reporters, hugely affecting journalists' ability to report on truth and hold power to account. But this privilege is under threat, with a number of known cases where as a result of far-reaching digital government surveillance the identity of a source was revealed. This has a detrimental effect on the credibility of a reporter and could mean that sources become hesitant to bring stories to light. This thesis explores the tensions between source protection and government surveillance by studying how the journalistic privilege is defined in legal terms, by looking into what government intelligence agencies are allowed to do under new Dutch surveillance legislation that went into effect in 2018, and how oversight of the use of special coercion tools within the legal framework is regulated. Furthermore, it seeks to outline the complicated relationship between a public's right to know, and a government's right to classify. Central to this is the question of whether journalists are able to accurately weigh their own interests of publishing sensitive information and the national security risks.

The second part of this thesis focuses on source protection in practice and how journalists feel about their ability to provide anonymity. The findings in this part are based on seven interviews with journalists and editors primarily reporting on the intelligence community, or on fields that are of special interest to Dutch security agencies like Islamic extremism and terrorism, or organized crime. Their experiences in talking to anonymous sources is of special interest to this topic.

Having defined the legal framework, and having explored practical experience from journalists in their day-to-day reporting using source protection, the final part of the thesis explores the importance of digital security for journalists and outlines different ways through which they can limit the chances of their sources being exposed.

iii. Methodology

The central research question in this thesis is to what extent journalists are capable of protecting the identity of their sources in times of digital government surveillance. The hypothesis that follows is that journalists often are not capable to guarantee source protection. I will address this issue by addressing the following questions:

1. How is source protection for journalists regulated and guaranteed within the existing legal framework?

2. How are mass surveillance techniques being applied by the Dutch government domestically and in collaboration with foreign partner services?

3. How does the principle of source protection compare to government claims of risks to national security?

4. How do journalists struggle when protecting the identity of their sources and how do their newsroom support them in this?

5. What security measures do journalists have at their disposal?

The findings in this thesis are based on two methods of research; literature reviews and expert interviews. Literature reviews have been used to answer research questions 1, 2, and 3. To investigate the last two questions expert interviews have been conducted. An answer to research question 1 is provided by examining existing legislation, mainly Dutch legislation on the intelligence and security agencies (WIV, Wet op de Inlichtingen en Veiligheidsdiensten) of 2017. The WIV 2017 replaces the previous legislation dating back to 2002. It includes significantly broader authority given to these agencies to perform wire tapes on persons of interest, potentially including journalists. This law, together with Article 7 of the Dutch constitution, Article 10 of the European Convention on Human Rights, historic legal cases like Goodwin v. United Kingdom (1996), and recent amendments to Dutch prosecution law forms the legal backbone of journalistic privileges and liberties.

For questions 2 and 3 scholarly material was used. One of the major sources is Mark Lowenthal's *Intelligence* (2000), one of the most comprehensive studies on the methods of operation of the American intelligence agencies. It also sheds light on the most widespread methods of intelligence gathering of the Dutch intelligence agencies. Other literature used includes a study by David Abramowicz (2008), and a study on media incentives and national security secrets published in the Harvard Law Review (2009). Furthermore Julie Posetti's study *Protecting Journalism Sources in the Digital Age* (2017) provides insight into the legal struggles surrounding source protection on a European level, while Julia Angwin's chapter on digital security for journalists in *Journalism after Snowden. The Future of the Free Press in the Surveillance State* (2017) by Emily Bell and Taylor Owen elaborates on the tools journalists can use to secure their data and communications.

Although heavily focussing on literature reviews, expert interviews produced useful qualitative data on the effects of previous and current surveillance legislature on the everyday work of journalists. Investigative reporters are an especially interesting case since they often find themselves reporting on issues that touch on sensitive security issues such as Russian meddling, Islamic extremism or criminal gangs. By examining cases about conflicts between government interests and source protection, these interviews provided essential qualitative data used in research question 4 and 5 to elaborate on the theory discussed earlier. Below is an overview of the respondents and their profiles.

Thomas Bruning, secretary for the Dutch Union for Journalists (NVJ), played an important role in crafting new legislation designed to better protect journalists in court. Given his legal background, he has provided valid insights in the workings and limitations of this new legislation. Joost Oranje and Lucas van Houtert are the editors-in-chief of Nieuwsuur and Brabants Dagblad, respectively. They have the role of supporting journalists in taking precautions to work safely and of spreading awareness related to security vulnerabilities when working with anonymous sources. Joost Oranje oversaw the publication of numerous high-profile reports like the Marco Kroon-affaire and the publication of successful attempts by the Dutch intelligence agencies to infiltrate a Russian hack group. Lucas van Houtert experienced first-hand the effect of revealing a journalists' sources to authorities when the phone records of one of his reporters were seized by the Public Prosecution Service. Janny Groen and Hassan Bahara both cover radical right-wing and Islamic extremism for De Volkskrant and as such are in regular contact with sources that might be of interest to intelligence agencies. Their experience with working with anonymous sources proved to be of value since they both have very different levels of experience with methods to secure data and as a consequence have a different focus when trying to protect

their sources. Huib Modderkolk also is a reporter for De Volkskrant and is one of the most skilled reporters covering the Dutch intelligence agencies. Together with Eelco Bosch van Rosenthal of Nieuwsuur, he reported on Dutch agencies infiltrating Russian hack group Cozy Bear. His knowledge of the Dutch intelligence community proved to be of huge value. Finally, Bart Mos offered useful insights. Together with colleague Joost de Haas he was taken hostage by authorities in 2006 for not revealing their source.

The choice for individual expert interviews as my methodology, as opposed to a survey amongst a larger sample group, is a deliberate choice in the definition of my qualitative research. Each of the journalists interviewed was chosen for their established reputation in the field of investigative journalism, relevance to the issue of source protection, and experience in working with anonymous sources. The standardized questionnaire survey used for this thesis has serious advantages in data comparability. The interviews were transcribed and subsequently categorized following an open coding approach using ATLAS.ti, clustering the interviews according to relevant themes from the first three research questions.

The disadvantages of applying these qualitative research methods, though, are not to be overlooked. Individual expert interviews yield highly interesting experiences from journalists in the field, but making sure that they represent as much of the journalistic spectrum is a challenge. For this reason interview candidates were picked based on different requirements, firstly by having a track record of working with anonymous sources as reporter or as editor-in-chief. Secondly, they were picked for their reporting on either intelligence agencies themselves, or on a field that is of great interest to those agencies like radical right-wing or Islamic groups. Finally, some candidates like Thomas Bruning, Bart Mos, or Lucas van Houtert were picked for their special relevance to the issue of source protection in journalism. The people interviewed work for three major national news outlets (De Telegraaf, Nieuwsuur, and De Volkskrant) and for the smaller regional Brabants Dagblad. They mostly represent print media and a small fraction of television, but the lack of more sources in television and radio does not have an impact on the data since the process of working with anonymous sources and guaranteeing source protection is not shaped by the platform reports are published on.

1. Source protection: a legal definition

How is source protection for journalists regulated and guaranteed within the existing legal framework?

With the signing of the WIV 2017 and amendments to existing prosecution law regarding a journalists' rights to hold the court in contempt there has been a change in the legal protections for journalists. This chapter seeks to outline the legal framework regulating the privilege of source protection for journalists, as well as authority given to the Dutch intelligence services, often proving to be the greatest challenger to journalists' rights. It outlines the articles of interest in the European Convention on Human Rights, Dutch constitutional law, the 2017 Intelligence and Security Services Act, and internal guidelines of the Public Prosecution Service (Openbaar Ministerie), hoping to give a clear understanding of the legal framework regarding source protection.

1a. European law and the Goodwin case

Rights, privileges and limitations for journalists when it comes to source protection are for the most part enshrined in European law, specifically Article 10 of the European Convention on Human Rights (ECHR). It ensures freedom of expression and information and has proven vital to journalists protecting the identity of their sources, something also secured in the Dutch Constitution (Article 7: Freedom of Free Speech and Information). In a landmark 11-6 decision in the case of Goodwin versus United Kingdom, the European Court of Human Rights (1996) argued that forcing a journalist to reveal the identity of a source is a violation of the right to freedom of expression under Article 10 of the ECHR.

The journalist in question, William Goodwin, was a trainee journalist writing for The Engineer magazine who, according to court documents, was contacted by a source he had worked with previously. The source gave him sensitive information regarding the financial state of a company called Tetra Ltd., from what turned out to be highly confidential reports of which there were eight copies. One had recently gone missing. After Goodwin called Tetra Ltd. to check the facts on the information in the documents, the company sued. The next day a judge granted an injunction barring the publishers of The Engineer to run the story, or publish any information derived from the confidential documents. Furthermore, the judge

also ordered the journalist to reveal the identity of the source and eventually was fined £5,000 for contempt of court under the 1981 Contempt of Court Act. After appealing the British court decision in front of the European Court of Human Rights (ECtHR), the judges in Strasbourg ruled that fining the journalist for not being willing to give up the identity of a source was a violation of Article 10 of the ECHR. Publication of the confidential information was already prohibited, and the court found that "no breach of that injunction had occurred." It went on saying that "a source may provide information of little value one day and of great value the next; what mattered was that the relationship between the journalist and the source was generating the kind of information which had legitimate news potential. This was not to deny Tetra's entitlement to keep its operations secret, if it could, but to contest that there was a pressing social need for punishing the applicant for refusing to disclose the source of the information which Tetra had been unable to keep secret."

In its argument the ECtHR goes further, highlighting the risks of undermining the rights of source protection for a free and open society:

> "Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest" (European Court of Human Rights, 1996).

The decision underlines the significance of source protection under European law and establishes a binding or persuasive precedent within its jurisdiction (Columbia Global Freedom of Expression, n.d.). To this day the case of Goodwin v. United Kingdom has had a lasting impact on European law and the protection of journalistic sources, having been cited in cases in European courts at least 22 times. In the cases of *Sanoma Uitgevers B.V. v The Netherlands* (2010) and *Telegraaf Media Nederland Landelijke Media b.v. and others v. the*

Netherlands (2012) the ECtHR upheld the notion of source protection under Article 10 of the ECHR. However, in 2014 the Court ruled that Dutch magazine Ravage could not invoke Article 10 to protest a police raid in its newsroom. The purpose of the raid in 1996 was to obtain a letter that was a possible lead towards identifying the suspects of a bomb attack on chemical company BASF in Arnhem, the Netherlands. The Court ruled that the author of the letter could not be seen as a 'journalistic source', and that not "every individual who is used by a journalist for information is a 'source'", further stating that "his purpose in seeking publicity through the magazine Ravage was to don the veil of anonymity with a view to evading his own criminal accountability" (Posetti, 2017, p. 44). The Court stressed the importance of the press as a watchdog for democracy, but deemed the public interest of finding the suspect of the bomb attack to outweigh the interest of the journalist to protect a source.

1b. Dutch constitutional law and the right to hold the court in contempt

However never formally acknowledged until the approval of new legislation in 2018, Dutch courts have established a long standing precedent on source protection under existing constitutional law. This precedent constitutes to a conservative view of journalists invoking the professional privilege of source protection, with the Supreme Court saying in 1977 that extending journalists the right to hold the court in contempt does serve the common interest of free news-gathering, but potentially undermines the courts' ability to seek truth. More importantly, claimants who have been the subject of false and harmful reporting should not be limited in their ability to seek justice before the court, an interest that the Supreme Court ruled more important than a journalists' wish to hold the court in contempt (Schuijt, 2006, p. 152). The Court concluded their legal opinion by saying that *in general* a legal right to hold the court in contempt for journalists could not be accepted, leaving the door slightly open for specific cases in which the right of free news-gathering did outweigh other interests, and essentially stated that journalists have no such right, except for specific exceptions.

This changed with the adoption of new legislation in 2018 granting journalists the explicit right to hold the court in contempt. Amendments made to existing prosecution laws that came into effect on October 1st, 2018, state that people who get paid for news gathering on a professional level now have the right to keep the court in contempt when they are asked to reveal the identity of their source (Staatsblad, 2018). This includes journalists working in newsrooms, freelance journalists, and publicists but also bloggers, cartoonists, photographers and videographers. This right, however, is bound by limitations to be interpreted by the Court. In situations where national security interests outweigh the

interests of an individual journalist, the journalist can be charged for holding the court in contempt, and a judge can order for the journalist to be taken hostage for a period of twelve days, which can be then extended for periods of twelve days.

The process of amending the existing legislation took the better part of two decades, and the discourse on a journalistic right to be in contempt of court traces back all the way to the first part of the 20th century (Schuijt, 2006, pp. 141-149).On a European level, the ECtHR –going as far back as the early 2000s– has repeatedly stressed the importance of provisions in Dutch law permitting a journalist to hold the court in contempt by not revealing their source (Posetti, 2017, p. 44). The new Dutch legislation uses a very broad definition of who is a journalist. Journalists, publicists, photographers, videographers, cartoonists and bloggers can all invoke the right to hold the court in contempt in matters relating to source protection (NOS, 2018, October 17). This makes questions of whether someone earns a living from their work as a journalist irrelevant, especially important in times of increasingly flexible contracts for journalists. After years of debate the amendments were finally passed by both houses of Parliament and implemented on October 1st, 2018.

1c. WIV: Intelligence and Security Services Act

The recently approved Intelligence and Security Services Act (WIV 2017) is the main legal framework concerning source protection in The Netherlands. Passed in 2017 by both Houses of Parliament it replaced the aging legislation on the intelligence and security services dating back to the 1990s. It partially came into effect on September 1st, 2017 and was fully in effect on May 1st, 2018. The WIV 2017 regulates what the General Intelligence and Security Agency (AIVD) and the Military Intelligence and Security Agency (MIVD) can and cannot do. Publicly dubbed 'sleepwet' (dragnet law), it created a large backlash as some found the far reaching provisions on data interception to be a privacy violation. A small group of students from the University of Amsterdam started a petition triggering a referendum on the new law, resulting in a majority of 49,5% voting against the 'sleepwet' (NOS, 2018, March 23). After small changes, the law went into effect May 1st, 2018 despite the protests.

The WIV 2017 includes sweeping and far-reaching provisions that allow for mass collection of digital communication data such as phone records, emails and browser data. Most important is the provision that allows for the untargeted monitoring of all data to or from an area that is seen as a threat to national security (*Wet op de Inlichtingen- en Veiligheidsdiensten 2017,* 2018). This can mean for instance that if intelligence agencies are monitoring traffic from De Schilderswijk, a neighbourhood in The Hague with a large population of young men with ties to Islamic radicals in Syria (with some of them actually

joining jihadist extremist forces), the agencies are allowed to monitor all data between De Schilderswijk and Syria without having to limit their investigation to a specific individual, phone number or IP-address, as mentioned in Article 48, 49 and 50 of the WIV 2017 (Referendumcommissie, 2018). Any encrypted data that is intercepted may be decrypted. Following the referendum, and after the WIV was sent back to the drawing board, Minister of the Interior Kajsa Ollongren and Minister of Defense Ank Bijleveld-Schouten informed Parliament of changes to the law, writing in a letter to Parliament that special methods of interception will be used as little as possible and only if there are no other ways in retrieving the data deemed necessary for an ongoing investigation (Ollongren, & Bijleveld-Schouten, 2018).

Rob Bertholee, the director of the AIVD, underlines this once more, vehemently stating that the image that the intelligence agencies are just wiretapping entire neighbourhoods is false. Bertholee: "When you look at the WIV you should not just look at this one article giving us the authority to perform these wiretaps, but you should also look at the article stating that the use of it is only allowed when absolutely necessary in an investigation and only as a last resort." He goes on adding that "it is not like we are sitting together on a Monday morning, thinking who we might wiretap today [...] There are checks and balances" (VICE Nederland, 2018). But critics of the WIV pointed out that these checks might not be enough. The secret services are required to get permission from an independent oversight commission called TIB (Toetsingscommissie Inzet Bevoegdheden), which consists of two former judges and a field expert in digital security (van den Dool, & Versteegh, 2018). Mariëtte Mousault, the committee's chairman said in the commission's first annual report that the TIB is approving approximately 95% of the requests for the use of these special methods of interception, only blocking 1 in 20. In the 2018-2019 period the number of blocked requests dropped to only 1 in 50 (Toetsingscommissie Inzet Bevoegdheden, 2018, p. 11). The Dutch Data Protection Authority fears that this oversight is too weak, mentioning a possible high workload, the likelihood that TIB-members do not feel free to oppose intelligence officials and citing a fear of the TIB becoming merely a stamping machine, trying to keep up with a large flow of requests and being unable to properly vet them. A fear shared by the Council of State, the highest advisory organ for the government (Hijink, van Lonkhuyzen, Pelgrim, & Versteegh, 2018). The importance of the TIB was shown nonetheless in commission's 2018-2019 annual report, where it revealed it had prevented either the AIVD or the MIVD from accessing the data of millions of users from an unnamed company in order to zero in on the data of a number of targets. The commission writes that this specific request did not meet the commission's privacy standards, adding that a "sizeable

percentage of [the requests] was denied as in these cases the use of coercion methods was not proportional" (Toetsingscommissie Inzet Bevoegdheden, 2018, p. 22).

The changes made to the WIV following the 2018 referendum mention specific provisions about the protection of journalists. If journalists are subject of so called 'special coercion methods' like searches of private property, the hacking of digital devices, targeted wiretapping or the seizure of phone records from telecom providers, a special warrant is needed from the Court of The Hague, as stated in Article 30, section 2 of the WIV 2017. Also, if data about journalists is scooped up as the result of untargeted surveillance, then this will not be shared with foreign (security) agencies (Ollongren, & Bijleveld-Schouten, 2018). However, ultimately these extra measures do not prevent a journalist's data being scooped up as a byproduct of a large untargeted government data hack, nor does it prevent the use of that data by security agencies.

1d. The Public Prosecution Service and their approach to journalists' sources

Much in the same way that the WIV 2017 limits intelligence agencies in their use of 'special coercion methods' when journalists are involved, the Public Prosecution Service is working according to special guidelines as well (Leijten, 2018). The guidelines were renewed after the implementation of the amendments to prosecution laws allowing journalists to hold the court in contempt (Aanwijzing toepassing dwangmiddelen en opsporingsbevoegdheden bij journalisten, 2018), and most of the guidelines are overlapping with the WIV 2017. They stress that "first and foremost special coercion methods are to be used sparsely against journalists who can claim the privilege of source protection." Furthermore, it states that when the use of special coercion methods is justified when concerning source protection, the prosecutor working the case needs to seek permission from the Chief Prosecutor. Also, the Board of Prosecutors General has to be informed before. In the case of the journalist from Brabants Dagblad, however, the prosecutor who had obtained the private phone records of the journalist had neglected to inform the Board, showing that these rules of engagement are not written in stone (Brabants Dagblad, 2018).

The main issue, as shown above, is that it is one thing to draft these rules, but it is another to actually live by them. Minister Grapperhaus has stressed numerous times the importance a free press has to society, but in the cases of Joey Bremer and the journalist from Brabants Dagblad, lower ranking officials from the Public Prosecution Service neglected to get the proper judicial clearance allowing them to either obtain the phone records or listen in on a conversation between a journalist and his source. This clearance most likely would not have been given since both the WIV 2017 and the guidelines from the

Public Prosecution Service clearly state that such measures are only allowed in the rare instances when the public interest far outweighs the journalists' interest.

1e. Conclusion

Source protection as a right has been enshrined in both Dutch and European law, and theoretically should work well in protecting a journalist from prosecution when refusing to reveal the identity of his source. Source protection is guaranteed in Article 10 of the ECtHR and further strengthened by Article 7 of the Dutch constitution. The WIV 2017 gives intelligence agencies extensive authority to perform untargeted dragnet surveillance, but it specifically notes the special privileges of journalists. The guidelines from the Public Prosecution Service, finally, reaffirm these privileges and safeguard them. But this is also the biggest bottleneck as seen in the aforementioned cases of Brabants Dagblad and the Amsterdam gang war, because journalists face the risks of these rights being violated when oversight is lacking and public prosecutors do not follow the rules.

Although journalists are now given the right under Dutch law to hold the court in contempt when they are forced to give up the identity of their source, it is hard to say if the legislation will prove successful in guarding the privacy of communications between a journalist and a source. The cases mentioned earlier also show that there still is a high likelihood that procedural errors in getting proper permission to perform the interceptions as well as a possible lack of oversight from TIB can lead to sensitive information on sources ending up in the hands of intelligence agencies through illegitimate ways.

2. The Dutch government and mass surveillance

How are mass surveillance techniques being applied by the Dutch government domestically and in collaboration with foreign partner services?

A lot is known about the methods and tools of operation of American and British intelligence services, not only because of whistleblowers like Edward Snowden and Chelsea Manning, but also because we can tap into a large database of academic research on the workings of intelligence agencies. In the case of the AIVD and MIVD there is a lot less academic research on the inner workings of the services, but reporting done by newspapers like NRC Handelsblad (Hijink, 2018) and De Volkskrant (Modderkolk, 2018) makes it clear that Dutch agencies use similar general methods and tools to collect intelligence and intercept global radio traffic. Because of this we can draw parallels between the Dutch secret service and considerations on the American services, for instance from Mark Lowenthal's *Intelligence* (2016), the academic standard on intelligence practices. By elaborating on the methods described by Lowenthal and comparing them to reporting on the Dutch intelligence agencies, this chapter aims to give a clear picture of how techniques of electronic surveillance are being applied by those agencies.

Although both the AIVD and MIVD are notoriously secretive about the frequency of use and success rate of their methods, Lowenthal gives us a lot of insight into the tools at their disposal. He categorizes five disciplines (INT's) of intelligence collection; open-source intelligence (OSINT), geospatial intelligence (GEOINT), human intelligence (HUMINT), signals intelligence (SIGINT), and finally, measurement and signatures intelligence (MASINT). OSINT and SIGINT in particular, are of interest when it comes to the question of source protection and journalism, since both of these disciplines rely on large quantities of data and the ability to intercept communications, as opposed to relying on satellite imagery, geospatial data, or human intel from field agents.

This chapter aims to show how Dutch intelligence services work together combining data from different agencies and what are the tools that they have at their disposal. Finally, it looks at how Dutch agencies are regarded in the international intelligence community and how they work together with foreign services.

2a. National intelligence gathering in the current legal framework

Dutch intelligence services retrieve their information from a myriad of sources, one of the most successful and effective ones being the Counterterrorism Information Box – CT Infobox in short (Versteegh, 2017). The Box originates from a coordinated effort between eight government services, including immigration services, the Ministry of Social Affairs and Employment, and intelligence agencies AIVD and MIVD. Each organization shares from its database and provides valuable information to track down potential targets. The method of collaboration, which came to be in the aftermath of the Madrid train bombings, has prevented attacks from happening and has proven to be hugely successful according to former employees and a number of independent research and oversight committees (de Poot & Flight, 2015). However, specific numbers on the exact success rate have not been made public due to security concerns. The Box is run by members from every related agency and institution and has become an enormous database of personal information. The Box is used for targeted surveillance: specifically, dossiers of persons of interest are made based on information that pops up through these different institutions. If an investigation on a specific individual is requested, each member starts looking for matches of that person's name in the database of their own agency. This information is then combined in one dossier that gives a highly accurate image of the subject in question based on financial information, criminal records, travel details and potential ties to radical organizations. The source of this information can range from intercepted communications to decrypted messages, although permission must be granted by the aforementioned TIB committee, and protections in the WIV limit the agencies from using their authority to include any communications with journalists, unless the public interest outweighs the personal interest.

JSCU

Another important source of information for Dutch intelligence agencies is the Joint Sigint Cyber Unit (JSCU), tasked – among others – with intercepting international satellite and radio communications and performing hacks in the interest of Dutch national security (Hennis-Plasschaert & Plasterk, 2014). Just how capable the JSCU is, was revealed last year when reporting by De Volkskrant and Nieuwsuur revealed that the cyber forces had successfully infiltrated a Russian hacking network called Cosy Bear responsible for breaching the Democratic National Committee (DNC) in the United States during the 2016 U.S. presidential campaign (Smeets, 2018). The JSCU has the mandate to gather and decrypt data from technical sources, meaning they are allowed to perform targeted hacks of phones, laptops and pc's, as well as deciphering encrypted messages found among the international

satellite and radio data gathered (Hennis-Plasschaert & Plasterk, 2014). The WIV allows the agencies to intercept all communications to and from a place of interest, for example enabling them to essentially intercept all communications from a specific neighbourhood to, say, Syria. Since it is not uncommon for journalists to seek contact with eyewitnesses for instance from a beleaguered Syrian city, there is a high chance of these communications ending up in the databases of intelligence services. Unclear remains what happens with communications between a journalist and his source, possibly revealing the identity of the latter, that is scooped up as bycatch.

2b. Foreign Intelligence collaborations

In the WIV 2017 specific mention is made about the exchange of data between AIVD and MIVD and their foreign counterparts. In these collaborations different types of data can be exchanged as mentioned in Article 88, 89 and 90 of the WIV 2017. This ranges from raw data that is not yet analyzed, to phone records, or even specific intelligence on persons of interest (*Wet op de Inlichtingen- en Veiligheidsdiensten 2017,* 2018). In the case of raw data that has not yet been analyzed, permission has to be granted by the Minister of the Interior before it can be shared with foreign partners, but no authority is required by the independent CTIVD (Supervisory Commission on the Intelligence and Security Services, appointed by Parliament). The Dutch intelligence agencies are mainly working together within bilateral intelligence partnerships like the NATO Civil Intelligence Committee (CIC), the European Union's EU Intelligence Analysis Centre (EU INTCEN), the Counter Terrorism Group (CTG), and the Club de Berne (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, 2009). American intelligence agencies like NSA and CIA are also important partners when it comes to bilateral and multilateral collaborations, and it is especially this relationship that proves to be problematic.

In an interview with Nieuwsuur (2015) and De Volkskrant, NSA whistleblower Edward Snowden, who in 2013 stole countless documents revealing the extent of government surveillance in the United States, said that American agencies see Dutch intelligence services as subordinates, saying that "the Dutch [agencies] as sort of the surveillance kings of Europe are obviously quite comfortable and quite close to the NSA. However [...] they do not have the same respect that other services might get. For example the French intelligence services are extraordinarily sophisticated. They are one of the only services that CIA officers operating in Europe actually fear in counterintelligence terms. They are very aggressive and very good. The Dutch services in comparison are seen more as subordinates." He added that the "U.S. intelligence services do not value the Dutch for their

capabilities. They value them for their access, they value them for their geography, and they value them for the fact that they have cables and satellites. [They value them] as a sort of a vantage point that enables them to spy on their neighbours and others in the region in a unique way. And by taking advantage of that the NSA can use their capabilities to a greater advantage relative to if they did not have that partnership." Snowden goes on saying that he suspects that the Dutch government in many ways is "being pressured by offices such as the Foreign Affairs Division (FAD) in the NSA and other partners in Europe to join [...] this Five Eyes method of operation", referencing the intelligence alliance of the U.S., Canada, the United Kingdom, Australia, and New Zealand.

Outside influences

Snowden also mentioned the existence and the role of the FAD within the NSA in a statement to the European Parliament, saying "lawyers from the NSA, as well as the UK's GCHQ (Government Communications Headquarters), work very hard to search for loopholes in laws and constitutional protections that they can use to justify indiscriminate, dragnet surveillance operations that were at best unwittingly authorized by lawmakers. These efforts to interpret new powers out of vague laws is an intentional strategy to avoid public opposition and lawmakers' insistence that legal limits be respected, effects the GCHQ internally described in its own documents as "damaging public debate" (Austin, 2015). An example of how this works, is given by journalist Huib Modderkolk in an interview with Rob Bertholee, director of the AIVD. When asked if the AIVD can legally request information about a Dutch journalist from British or American intelligence agencies, Bertholee answers in the affirmative. "But they will never say how they retrieved that information", Bertholee says (Modderkolk, Minkema, Kranen, Hogeling, & van der Wauw, 2016). This confirms a scenario in which the AIVD can get private communications data on a journalist through foreign agencies that it would not be allowed to retrieve under Dutch law, essentially evading WIV 2017 safeguards and checks about journalist surveillance.

The influence of U.S. intelligence services in particular raises the question of whether the Dutch government has a real grip on what digital data is given to foreign services, especially when realizing that the Minister of the Interior has to give personal approval for every single request of exchange of information, most likely a full time occupation in itself. This also includes data that has not been evaluated by Dutch intelligence services, as described in Article 89, section 2 of the WIV 2017. Considering the amount of data that is under surveillance, the apparent lack of independent oversight in deciding what can be shared, and the risk of the Minister becoming a stamp machine approving everything that

crosses his/her desk, the sharing of data with foreign agencies can be a danger to the safety of a journalists' private conversation and of source identity. The WIV 2017 prevents Dutch intelligence agencies from sharing information on journalists gathered through untargeted digital surveillance with foreign intelligence partners (*Beleidsregels WIV 2017*, 2018), but it does allow for the sharing of unevaluated data. In effect, this creates loopholes in which journalists cannot be wiretapped by Dutch services unless they were granted permission by the Court in The Hague, but agencies can provide foreign intelligence partners with data not yet analyzed – and vice versa –, possibly containing information revealing a journalists' source, essentially evading the safeguards for source protection and a free press.

2c. Conclusion

The Dutch intelligence agencies are highly efficient in analyzing the available data, working in a network of at least eight semi-integrated government databases (CT Infobox). Given the excellent geographical location of the Netherlands, with its high density of fiber optic cables, Dutch agencies have the unique ability to intercept and analyze enormous amounts of international radio and satellite communications. But although legislation on the Dutch intelligence agencies clearly outlines the limits of targeted surveillance of journalists and their communications within the borders, it is in the context of information exchange with foreign partner agencies that those safeguards seem to be inadequate. Snowden's remarks about the AIVD and MIVD being subordinate to the NSA and CIA raises concerns about the extent to which safeguards in the WIV 2017 can actually guarantee the right of source protection for journalists and reaffirm the importance of a free press according to democratic values in an increasingly global surveillance system.

3. Source protection versus national security

How does the principle of source protection compare to government claims of risks to national security?

One key aspect that cannot be overlooked when discussing the privilege of source protection is the tense relationship between a journalists' right to know and a government's right to classify. It raises the question of whether journalists can be trusted with sensitive government secrets, and equally whether the government has the right motives when it comes to classifying material. This chapter aims to answer the question of how a balance between right to know and right to classify can be found by discussing how journalists can accurately assess national security risks, and when the use of anonymous sources is warranted.

3a. Assessing national security risks

Both the WIV 2017 and the recent amendments to Dutch prosecution law are clear when it comes to defining a journalist's right to invoke the privilege of source protection, at the same time clearly outlining its limitations. In the case of public interests like national security outweighing the interest of a reporter to protect his sources, it becomes a challenge for journalists to assess if the government's concerns are valid and if indeed the public interest outweighs the right for the public to know the truth. As a 2009 study published in the Harvard Law Review put it, "some secrecy is essential to both national security and democracy, but excessive secrecy undermines democratic accountability and decision making, and sometimes national security itself", further saying that "neither the government nor the press can be trusted to strike that balance, for both have asymmetric incentives" (Harvard Law Review Association, 2009).

Case in point is the reporting by Siebe Sietsma and Karel Ornstein from Nieuwsuur who in early 2018 were investigating claims by Marco Kroon, an officer in the Dutch army, saying he was held hostage was submitted to torture by an Afghan civilian during a covert mission in Kabul. When he later accidentally met his abductor he claims to have shot and killed him (Kroon, 2018). Journalists Sietsma and Ornstein were able to report on details that could possible shed some light on the exact circumstances of Kroon's claims, but in a

rare move the Minister of Defense requested Nieuwsuur not to publish their story as it "contained government secrets. Lives will be endangered when the story is published. We strongly request not to publish the information. I am also informing you of the fact that the publication of classified information is illegal" (Oranje, 2018). The claims officer Kroon made were later repudiated by the Ministry of Defense (Righton, Feenstra, & Thijssen, 2018). In an interview with Nieuwsuur, Sietsma elaborates on the decision not to publish the story, saying "there are two parts to this. State secrets, that is a legal question. We could say that we are going to fight that battle and we will see where it leads us. The other element is human lives. We cannot entirely see behind that, but we cannot ignore it. It begs us to question what story is worth a human life" (Nieuwsuur, 2018).

It is extremely hard, if at all possible, for journalists to be fully aware of the possible consequences of publishing sensitive, classified information, simply because they cannot be expected to understand the full scope of the possible risks and dangers since there is a clear knowledge gap that exists between intelligence services and journalists trying to inform the general public on sensitive matters. Possible overclassification by government agencies (Harvard Law Review, 2009) without real national security risks makes it even harder for journalists to assess government claims of threats of national security. Quoting the 2009 Harvard study: "while optimally we might judge a publication decision by identifying the disclosure's potential for harm to national security and its potential for benefit to public knowledge or accountability and balancing the two, such bottom-line balancing is basically unworkable." Even though journalists cannot be expected to strike a fair balance between accountability and the classification of sensitive information, according to the ombudsman of the Dutch broadcasting agency (NPO Ombudsman, 2018) this should not stop journalists from being able to investigate anything they deem of interest to the general public. "The press has to inform the public so that it is able to make well-informed decisions. In order to do this, the press has to be able to investigate anything. It is only after that that the importance or risks of publishing can be accurately determined." The opinion of the Ombudsman is in response to a complaint by an unknown individual against Nieuwsuur for using classified material in the aforementioned case of Marco Kroon. The Ombudsman goes on pointing towards known examples of governments using the term 'classified' in a very liberal fashion. "Not wanting to categorise the Dutch government in that way, the Ombudsman is of the opinion that the justification for classifying information can only be assessed after thorough investigation."

3b. Warranting the use of secret sources

Just as the limits to the privilege of source protection, the use of confidential sources has limits too. It is a journalists' job to inform the electorate on matters that help them make a decision at the ballot box, but there are inherent risks to working with source confidentiality that might be a threat to public trust in journalists and that warrant more scrutiny of journalistic methods. In *Media Incentives and National Security Secrets*, the aforementioned 2009 study published by the Harvard Law Review, three inherent risks are described. The first is the fact that journalists enjoy significant personal gain – awards for outstanding journalism, like De Tegel – when they break major stories. In line with this concern lies the second risk, namely the fact that reporters have incentives to report secrets that generate short-term scandal and public attention. The third point is based on the business model of most newspapers, in that they are driven by financial profit. This point is less true for Dutch media in general, since a large part of media platforms is government funded and does not have to rely on revenue from subscriptions sales.

Another study, by David Abramowicz (2008) and published in the Columbia Law Review, investigates the public interest served by the use of anonymous sources and source protection. It finds that one of the biggest risks are fabricators who can use their protected status to harm the credibility and accuracy of reporting. Also, the study finds that although ideally used to protect the weak from the powerful, it can also be used to shield sources whose information has proven to be false from accountability. The provided example is of a Newsweek story of guards at Guantanamo Bay desecrating copies of the Quran. The report was cited to anonymous sources. The reporting sparked riots that left sixteen dead, and later Newsweek retracted the story, saying that their source was not sure if the incident had happened. Since Newsweek kept its promise of confidentiality, the source could not be held accountable for the deaths that followed his false statements (Abramowicz). Finally, the study points out that sources always have their own motives that lead them to provide information or leak classified documents. Some motives might put the information ascribed to an anonymous source in a very different light if the identity of the source was made public.

To combat these risks that are associated with confidentiality and the use of anonymous sources, Abramowicz suggests that journalists should try to limit themselves from using these tools, unless it is impossible to use a source otherwise. He describes it as a tool of last resort, and points towards policies that require reporters to resist requests for confidentiality. He also says that those "policies [should] seek to limit what journalists cite to confidential sources to information that is 'important', not 'trivial, obvious or self-serving'." Another important aspect are internal newsroom guidelines stating that at least one editor

needs to know the identities of the sources used, a measure aimed at stripping reporters of their "unilateral powers to grant confidentiality" and preventing them from becoming "agents of their confidential sources". The last important argument Abramowicz makes when addressing the inherent risks to using confidential sources, is the need for transparency. Although the identity of the source cannot be revealed, many details that establish the reliability and knowledge of the source about a specific subject can be provided, giving a clearer image of the level of knowledge of that source and inspiring trust among readers.

3c. Conclusion

As both the 2009 study published in the Harvard Law Review and the 2008 study by David Abramowicz conclude, neither the government nor the press can accurately strike a balance between the right to know and the right to classify, for both have diametrically opposed incentives. Journalists cannot be expected to understand the full scope of potential consequences of publishing sensitive material that might put people in harm's way, but the importance of not damaging one's reputation and credibility is vital for journalists and is one incentive that could keep them from misusing their fourth estate power. Journalists are however susceptible to other motives such as personal gain when breaking major stories, or a general tendency to report on news that generates short-term scandal. The press ultimately is not in a position to accurately assess the larger public interest when it comes to reporting on classified material that might have national security implications. In order to not damage the public's trust in the press, journalists should keep in mind the limitations of the use of anonymous sources by only using it as a tool of last resort, by sticking to guidelines aimed at establishing editorial oversight on the sources receiving confidentiality, and by striving for transparency towards readers on the use of confidential sources.

4. Guaranteeing source protection in real life

How do journalists struggle when protecting the identity of their sources and how do their newsroom support them in this?

Regardless of the legal framework within which journalists try to protect the identity of sources, the biggest responsibility lies with journalists themselves and with the methods and tools they use in their day-to-day reporting. Based on interviews with seven reporters, editors-in-chief, and field experts, this chapter seeks to investigate the challenges that journalists feel threaten their ability to protect sources and aims to shed light on the role of newsrooms and editors in assisting their reporters in this matter.

4a. What do journalists see as risks to their ability to keep the identity of their sources confidential?

There are two main issues that journalists experience as developments that make it more complicated to work and communicate with anonymous sources. Firstly, they point towards digital footprints that are the result of devices leaking metadata possibly exposing sources' identity. The second issue concerns the Public Prosecution Service, that in the past two years has repeatedly overstepped its mandate when dealing with journalists.

Data trails and digital footprints

Every device that connects to the internet leaves an online data trail. Whether browsing on the web, downloading a PDF file, or checking our route on Google Maps, our online behavior can reveal a lot more about us than we might think. Journalists should be very aware of this, according to Huib Modderkolk. His reporting for De Volkskrant on the Dutch intelligence agencies has led him to an understanding of the risks that journalists face when communicating with sources. "Our phones and computers leak information in many ways. To companies, to organizations. An example are debit card transactions. Let us assume that you are a source and I were to pay here, that transaction will be stored somewhere. This could reveal that I was on this location at this time. If you compare this data to other data, then this could lead to you to know with whom I have been here. Technology is putting

pressure on a source protection through digital transactions, number plate registration, CCTV. Journalists have to think harder about what they are doing because of these technological advancements." Modderkolk argues that on the one hand special provisions in the new legislation on the intelligence agencies shield journalists from surveillance, but on the other hand warrants allowing for the interception of fiber optic cables also create risks for journalists. "Because of these large-scale cable interceptions, our data, or a journalists' data, could pass through a 'filter' [looking for certain keywords or patterns in communications] from an intelligence agency, increasing the chance that that data ends up in the agencies' systems." [...] "Back in the day you knew that the agencies could not just place a tap on those cables. So it could sometimes be safer to call from a landline from the newsroom. Those calls were hard to trace because you had to know exactly which phone at De Volkskrant the call was made from. All those phones have different numbers, which creates a bit more security. I would say that since wide scale cable interception there is less security."

Bart Mos, who together with his colleague Joost de Haan was held hostage in 2006 for refusing to reveal his sources to authorities (De Volkskrant, 2006), underlines the point Modderkolk makes. Their explosive reporting of a corruption scandal, involving career criminal Mink Kok who paid millions to bribe police officers and got his hands on information regarding criminal investigations, got them in serious legal trouble when a judge ordered them to reveal the identity of their source. They refused and were subsequently taken hostage by authorities for a number of days (NOS, 2012). Mos: "I do not think the new legislation on source protection is going to have a big impact on whether or not sources will come forward. What is going to have an effect, however, are all the technical means that enable you to zero in on a source. That already causes sources to think twice before approaching a journalist. Back in the day you had to do that with surveillance teams, then you could tap a phone or see where it was located based on cell tower data, but that technology has advanced at such a pace that it is even more important to not use any digital means to communicate with your sources when reporting on highly sensitive matters."

"It makes you become increasingly more cautious because you know that there are a lot of smart boys and girls within extreme right wing groups who are very good at hacking", says Hassan Bahara. As an investigative reporter for De Volkskrant he focuses mainly on radical Islamic groups and extreme right wing groups. "Let us put it this way, even the most experienced journalists have such a lack of knowledge on how vulnerable our communication systems are. We really have a long way to go in that area. My colleague Annieke Kranenberg and I are lucky in that we are dealing with highly sensitive material, making us automatically

focus more on digital security. But I know a lot of colleagues who are communicating with their sources in ways…" He makes a sigh of frustration. "If anyone knows their way around a computer, they can do a lot of damage."

Janny Groen, an investigative reporter for De Volkskrant has had similar experiences with digital security. She reports on radical Islam, and has written a book on the wives of the members of the Hofstadgroep, a radical Islamic terrorist organization active throughout the early 2000s. Her book was based on confidential information from these women, undoubtedly of interest to intelligence agencies. "Maybe it is paranoia, but when my co-writer and I were writing our book at the same time at different locations, we once lost entire chapters for a moment. We called in technical support, but they could not find anything. Both computers at the same time!" Although stressing the fact that it is impossible to retrace the origin of the glitch, she says it made her rethink her methods to protect confidential material. "I am sure we made some really amateuristic agreements with these women from the Hofstadgroep. We would meet in 'the canteen' and then only we would know where that spot was." She goes on saying that "this was also because we knew that these women were under surveillance by the AIVD. We would make an appointment and they knew they were being followed and we could see them like this…", waving her arm under the table. "We knew we had to leave."

The Public Prosecution Service

Three cases of the Public Prosecution Service overstepping its mandate have put a focus on the role of the organization in their relationship to journalistic source protection. In Den Bosch prosecutors requested the phone records of journalist Jos van de Ven in search of a source who had leaked information on the appointment process of a new major (Haenen, & Dupuy, 2018). In a second case prosecutors in Rotterdam had retrieved phone records of journalist Joey Bremer from MediaTV (NOS, 2018, July 5). The local prosecutor neglected to inform the Board of Prosecutors General –a mandatory step when using special coercion methods on journalists– and later admitted that it had been a mistake retrieving the phone records of the journalist. The third case involves a photographer who had taken photos of a fight between a NATO officer and a civilian. The photographer Chris Keulen was taken to the police station and put in jail for two hours after not complying with a police order to give his camera and SD-card (RTL, 2018). For journalists these cases can create a feeling of uncertainty and raises the question to what extend the protections for journalists in the new legislation are effective in the real world. Bart Mos: "I think the leadership of the Public Prosecution Service is very much aware [of these protections for journalists], but that the

people in the workforce, whose main focus it is to catch criminals, do not always think about source protection and the surveillance of journalists and how to deal with that." Huib Modderkolk agrees with this point of view, stressing the historical importance of the hostage incident of Bart Mos in 2006. "I think the problem of lack of oversight with law enforcement is much more serious than it is with the secret services. The Telegraaf incident [of the hostage situation involving Bart Mos] has been a lesson for the AIVD. But there is a serious mismatch between the amount of oversight on the AIVD –with oversight bodies like the TIB and CTIVD– compared to the amount of oversight on the police in matters involving journalists. The law enforcement apparatus is much bigger, especially looking at the number of wiretaps they are doing." Furthermore, he also mentions a crackdown on government leaks. "Even within the municipality of Amsterdam they send the national bureau of investigation (Rijksrecherche) for very minute leaks, like an email, or small documents. That is a powerful signal, especially for young government officials. They will think three times before talking to a journalist." Executive editor of Nieuwsuur Joost Oranje: "An affair like the one involving Brabants Dagblad, or the one involving the photographer in Limburg [Chris Keulen]... It is unbelievable that government officials pull stunts like that. And we have seen it more often these past years. I am not entirely sure why it happens more often. Maybe they are not thinking about source protection as much, or maybe they are lacking in education on this subject." Thomas Bruning of the union for Dutch journalists points to the lack of law enforcement education in this area. "We have addressed this point with the Board of Prosecutors General and asked them to put a greater emphasis on the need for a firm understanding of source protection in the education of prosecutors. You have to make them realize what they can and cannot do when dealing with this issue. Because wiretapping a journalist to get to someone who has committed a crime can be a very alluring short cut for prosecutors and can be way easier than getting suspects to confess."

Although data gathered through the illegal wiretapping of journalists will likely lead to the evidence being deemed unusable in court, it cannot stop sources from being exposed to authorities. Lucas van Houtert, the executive editor for Brabants Dagblad, elaborates on the tense relationship with the Public Prosecution Service after finding out about the illegal wiretapping of one of his reporters, saying that "at first they were denying that our reporter had been wiretapped, which in and of itself is a lie. But they argued that it was not the reporter who had been wiretapped, but the person whom he was calling. [...] Eventually we successfully demanded they delete all the phone records and scrap any conversation involving our reporter." But the damage was done and the identity of the sources had been revealed to authorities. Van Houtert: "we were surprised to learn that the justice department

was not going to drop the case against the two persons suspected of leaking classified information." He says that his level of trust in the Public Prosecution Service to faithfully abide by the rules concerning journalists and their privilege to protect sources has been severely damaged. "When we were protesting their illegal wiretaps of our reporter they were not too eager to admit their mistake. We had to threaten with legal steps thrice before they caved, but it clearly showed a lack of willingness. The minister would do good to seriously overhaul and address those practices, because that is where the real problem lies. It is cowboy behavior."

A final point that needs to be addressed is that most of the respondents did not feel that the amendments to the WIV 2017 concerning the special position of journalists' made them and their sources safer. When asked whether she felt protected after the introduction of this new legislation, Janny Groen says she does not; "not now, not back in the day [when reporting on the Hofstadgroep terrorist network]". Bart Mos agrees with her, saying that since the hostage affair in 2006 "it has become increasingly difficult to protect your sources." Hassan Bahara: "it has become more fragile, absolutely. Especially because of what people are revealing about themselves on the internet and on social media. A message of condolence ten years ago, just to name some. People are leaving so many traces about themselves."

4b. Assisting journalists in keeping the identity of sources confidential

The responsibility of providing source protection lies for a big part on the shoulders of a journalism medium. As Abramowicz (2008) notes: "the general principle is that when anonymity is granted, reporter and source must understand that the commitment is undertaken by the newspaper, not alone by an individual journalist". Hassan Bahara mentioned earlier the lack of understanding of security risks among his colleagues at De Volkskrant. Asking him how he experiences the technical support of his newsroom in helping colleagues protect their data who do not handle highly sensitive material often, he says that "that can be improved upon massively. [...] We can do a lot more in terms of educational courses, I have raised that point myself before. There should be a better understanding of how journalists can secure their online data in technical terms. Right now that is often seen as complex and hard to understand, but we can do a lot better in that area. [...] I was in Russia to cover the World Cup in 2018. One would think that your employer prepares you for the digital dangers you face and teaches you how to protect your devices. Did not happen, sadly." Further support for this is given by Huib Modderkolk. He thinks journalists should think harder about how to handle sensitive issues, even when you are writing about agriculture. "You might think that writing about agriculture is not very sensitive, but there is

no way of knowing. You can never oversee the consequences for a source. Especially not if you really start digging."

When looking at his colleagues, Bart Mos does not entirely agree with Bahara and Modderkolk in their perception that there is a lack of understanding amongst colleagues in how vulnerable digital communications can be. "This newspaper [De Telegraaf] has been around the block and the people who work here have a good understanding of what is at stake when dealing with highly sensitive matters." But the affair in 2006 that resulted in him and his colleague being taken hostage has changed the way the newspaper deals with situations like those. "When the affair began we were invited to the national bureau of investigations [Rijksrecherche] to be questioned. The newspaper had not assigned a lawyer to support us and we had only consulted with the paper's in-house civil attorney, but not with a criminal defense lawyer even though at that point we were suspects. It took a long time for the paper to realize the magnitude of that situation. That naivety has disappeared, though. A couple of years later we had a similar situation with Jolande van de Graaf [who was a suspect in a case involving leaks within the AIVD. Her name was eventually cleared, (Bockting, 2012)], but the newspaper responded immediately and used every trick in the book."

Bos also disagrees with Bahara and Modderkolk on the notion that technical support from the newsroom can be better. "There is a good technical support at the newspaper. You have to ask for it yourself, but they offer tips and tricks, and even courses from security consultants. Shortly after the affair I even had training in how to lose people who are trailing you."

To help educate journalists to secure their date and help them become more tech savvy, the New York Times recently hired an experienced tech expert Runa Sandvik as Senior Director of Information Security, whose job it is to teach journalists how to protect their data by regularly changing their passwords, or using encryption tools (Kreling, & Modderkolk, 2017). "As a security practitioner I was once used to telling people that you should not click on the links you do not know, and you should be careful with email attachments. But you cannot give that advice to the newsroom. It is the newsrooms job to click on links and open attachments and communicate with people they do not know, because that is how they get their stories. So we are in a position to help them click on links securely, helping them open attachments securely" (OWASP, 2017). Asking Huib Modderkolk, who interviewed Sandvik for De Volkskrant, about the possibility for such a team at his newspaper, he answers in the affirmative. "But you have to look at scale. There are probably ten times more journalists working for the Times than for De Volkskrant, but of course I think it would be a good idea.

We do have a good CISO, Chief Information Security Officer, working for our parent company De Persgroep who actively thinks with us about implementing things like Tor [a highly secure internet browser]. I do notice change in that aspect over the course of the past four to five years. Back in the day when I wanted a Tor browser on my company computer, the technical desk would not allow it because everything was standardized out of security reasons." Most likely they were not eager installing software they were not entirely familiar with. "I understand their reasoning, but it is also a bit lazy." Modderkolk also stresses the fact that his newsroom is very supportive when it comes to replacing devices that might be breached. "I am the one who uses up the most phones and laptops. Most of the times because there are indications that really weird things are happening to them, and then they provide me with new ones." When asking him exactly what those indications are, he answers that he is not at liberty to say. "To not give anyone a clue."

When asking Joost Oranje about his role as executive editor in supporting his reporters in protecting their data, he says that for highly sensitive stories the board of editors is keeping a short leash. "Also to be able to give them feedback and advice, pointing at the risks they might run. Would it not be better to communicate through WhatsApp? Or is it better to meet in person? So you have this classified letter, but who gave it to you and what is his or her motive?" Those questions might also include legal questions, as Janny Groen points out. "When my colleague Annieke Kranenberg and I were reporting on the women of the Hofstadgroep we were given a CD-ROM by them with videos of beheadings that were shared within that terrorist network. We kept the CD-ROM in the newsroom and we made ourselves see all of the videos. The file was highly sought after by the government and Pieter Broertjes, our editor-in-chief at the time, made the decision that we had to get rid of it as fast as possible. 'Otherwise they will come and get it, it might be evidence.' So we watched it in its entirety one more time and then gave it back to those women."

Despite the series of events that exposed the identities of two confidential sources to law enforcement officials, executive editor Van Houtert from Brabants Dagblad does not plan a serious overhaul of standard newsroom practices. "I rarely get requests from reporters for more help in protecting sources. Maybe also because journalism is a bit of a lonely profession. [...] We have the legal department from our parent company De Persgroep that we can rely on when things go wrong, but I have no reason to assume we will be wiretapped again. It is only when you realize you are entering a place where we could be targeted that you start worrying about encryption, and communication over the phone."

4c. Conclusion

There are many developments that journalists experience as a challenge to their ability to protect sensitive material or the identity of their sources. One of them is everyday technology. Although it enables journalists to access enormous amounts of information through the click of a button, it also presents a risk of becoming the subject of targeted or untargeted digital surveillance that can limit journalists in their ability to protect their sources' identity. Many devices leak information that only very few users are fully aware of, and this is true for journalists as well.

A second concern journalists point at is the Public Prosecution Service repeatedly having overstepped its mandate when it comes to using special coercion methods on journalists. Three incidents in the past two years of prosecutors knowingly violating source protection and a harsh response towards leaks within government organizations can have a chilling effect on sources and whistleblowers coming forward, and in the case of Brabants Dagblad has led to two legal cases against sources who have been exposed as a consequence of illegal wiretapping.

Newsrooms have a special responsibility in assisting journalists in helping protect their sources, as the commitment to anonymize is finally undertaken by the medium, not the journalist himself (Abramowicz, 2008). The reporters interviewed mention educational courses on digital security, and material support in case of possible breaches. However, some also point to the general lack of consideration of security risks among colleagues who do not often handle sensitive materials. The New York Times is combating this by hiring a Senior Director of Information Security, but such big investments might not be feasible for smaller newspapers like Brabants Dagblad.

5. A journalist's toolbox

What security measures do journalists have at their disposal?

In 1972, at the height of the Watergate scandal and around the time of President Nixon's re-election to the White House, two reporters were secretly meeting a source in an underground parking garage, just across the Potomac River in Arlington, Virginia (Bernstein, & Woodward, 1974). The source, who was called by the name of Deep Throat, helped Carl Bernstein and Bob Woodward of the Washington Post piece together the story of a lifetime. The identity of the source remained a secret until 2005, when former Associate Director for the FBI Mark Felt admitted to being Deep Throat. By comparison, it took NSA officials just 48 hours to single out Edward Snowden as being the leaker of a huge trove of classified material (Angwin, 2017). In over four decades journalistic practices have changed drastically and the amount of data that reporters feel could leave a trail and expose the identity of their sources has greatly increased, as shown in chapter 4. This chapter, however, focuses on the security measures that journalists can take to better secure their data.

5a. A journalists' digital security toolbox

There are a myriad of solutions to help protect and secure a digital footprint, but the question regarding which methods are most effective depends on how much time and effort are at hand to build up an arsenal of tools, according to Julia Angwin. Angwin is a senior reporter at ProPublica and led a privacy investigation team for the Wall Street Journal. She advises journalists to firstly take basic security preparations, like updating software, using a password protector that can store and generate highly complex passwords, and not clicking on suspicious links in emails. Huib Modderkolk stresses the same point, saying that "if you have a new iPhone and you keep the software up to date, then a Zero-day exploit can easily cost a million euros." Zero-day exploit means using code to exploit a security hole not yet known by the developer of the product in order to plant a virus or other malware (Zetter, 2014). "I do not believe that secret services are willing to pay a million euros to be able to see my communication data. There are easier ways to get to that. So I am not too afraid of having my phone hacked." But Angwin (2017) also points to the fact that different sources require different security approaches, advising journalists to make a threat assessment outlining the

strategic goal, the threat itself, and tactics to be used. Two strategies are HEM, and ACE. The first one is especially useful to protect content and stands for Hide, Encrypt, and Mask, meaning to hide data in a secret physical, or digital compartment, encrypting it and finally making it look like an innocent file by masking its importance. The second acronym stands for Add Noise, Cloak, and Evade, and is used for securing metadata, information that describes or says something about digital communications. Add Noise means to add false connections or content to communications in order to confuse an observer. Cloak is meant to disguise metadata from communications by using another digital identity, or location. And finally, Evade means to try to generate as little metadata in the first place. In the following paragraphs we will delve into what tools and methods journalists use for some of the different elements of HEM and ACE.

Encryption

Although it seems like encrypting data is something only done by tech-savvy users, many forms of our communication are already encrypted. Message platform WhatsApp already offers end-to-end encryption for all messages sent through the app. But there are concerns about the existence of backdoors in the software enabling law enforcement to decode previously encrypted messages. More concerns exist about parent company Facebook's ability to scan the content of the texts despite the messages being encrypted (Ganguly, 2017). An alternative is Signal, which the journalists interviewed all confirmed to be using regularly. The app offers the same functionality as WhatsApp, including end-to-end encryption of texts, but due to the fact that it is based on an open source encryption protocol, the reliability of the safety features can be verified (Mora, 2017). Ofcourse, encrypting your messages is not everything, and journalists who handle sensitive information should look at an arsenal of tools that can encrypt hard drives (BitLocker), internet traffic (Virtual Private Network, VPN), or use a physical encryption USB-key that can protect your emails. Hassan Bahara, investigative reporter for De Volkskrant, says that he uses "Signal as much as possible. It is encrypted, so it is the most secure way to communicate. Besides that, I have taken a lot of precautions to shield off my email account by using two-factor authentication and I have ordered a USB-key that lets me further secure my emails."

It is however important to note that encryption is not a definitive answer in and of itself. Messages will still be readable on the devices of the participants in the chat. In a case involving former Trump campaign chair Paul Manafort, FBI officials obtained messages sent over WhatsApp through the devices of people who had received those texts. In another case law enforcement officials could access encrypted Signal messages sent by former US Senate

Intelligence Committee aide James Wolfe. As a Wired article (Newman, 2018) about the cases pointed out, it is unclear how the FBI got access to the messages, but it would not necessarily have to involve hacking and deciphering the encryption key.

Cloaking

One of the methods used by Janny Groen during her reporting on the Hofstadgroep, was to "not use our own phones. We had bought separate phones with a new sim card that we used to keep in touch with our sources." It is a method described by Angwin (2017) that is used to "mask metadata by using alternative identities or locations." When talking to sources, the actual conversation might not be that interesting to adversaries, but merely the fact that someone talked to a journalist can be reason to launch an investigation. Metadata can contain information like that, revealing for instance the time, place, or device a message was sent from. By using burner phones, setting up fake email addresses and sending texts from a different location, a sources' identity can be concealed. However, it is important to keep in mind that making a source use a fake email address while being connected to a company network might expose them to a high risk of their identity being revealed. Another important tool can be the use of Tor, a highly secure anonymous browser that bounces internet traffic to a large number of servers worldwide before delivering it to the receiver, so that it appears that the user is in a different location.

Evade

Journalists can try to fool observers into thinking they are someone or somewhere else, but it can be more effective to avoid metadata being collected all together. The most trusted method is by meeting sources at a previously disclosed location without discussing specifics through digital communications. Bart Mos, who was taken hostage for not revealing his source to a judge in 2006, says that when meeting a source, he and his co-worker would "...leave our phones at home. When we were meeting we would already set up the next meeting, and we would never communicate about that afterwards. Me and my colleague would also never speak on the phone about the case, only face to face in a special office in our newsroom". That could not prevent law enforcement agents from listening in, something which was revealed to them years later when lawyers of the suspects charged in the case were handed over the prosecutor's files. "They described a meeting with a source in a hotel in Noordwijk, a day after our initial reporting of the case. It said that a team from the National Bureau of Investigation (Rijksrecherche) had placed microphones in our hotel room ceiling two hours before we had arrived. We were lucky, because apparently these things were not

working properly, so they had transcribed what they could hear, but that apparently was of no value." This anecdote goes to show that journalists have to be very certain about the safety of a meeting place. Another way could be meeting people at their home, something that could however potentially aggravate a source. Huib Modderkolk explains: "It often leads to complaints from employers or even sources themselves, but what I often do is to go to a sources' home address, knock on the door and introduce myself as a journalist from De Volkskrant. Many times that scares people, but in my opinion there is no other way. By the way, for this to work you should leave your phone in the car, make sure you are not being followed, and park your car a couple of blocks away."

One point of concern that journalists should always keep in mind, other than the methods outlined above, is that it is of vital importance to always make sure that files given by sources are scrubbed of information giving away the sources identity. Printers often leave traces known as Machine Identification Code, very fine yellow dots not visible to the naked eye, that reveal the printer's serial number, and when and where a document was printed. In 2017 25-year-old NSA-contractor Reality Leigh Winner was charged with "removing classified material from a government facility and mailing it to a news outlet" after yellow dots on documents published by The Intercept led the trail to her. The hunt for the leak took government agencies less than an hour (Collins, 2017). Bart Mos: "Those are matters I take into consideration when publishing documents. [...] Sometimes I print the documents again, or in the case of a pdf-file –which can always reveal the original owner– I will make an image of the document instead of using the actual pdf-file."

5b. Conclusion

Despite numerous vulnerabilities that journalists' feel threaten their ability to protect the identity of their sources, there a plenty of options that can help them decrease the risks of sensitive information being exposed. To be successful, journalists should make an individual threat assessment when working with confidential sources identifying potential risks and vulnerabilities, and outlining a method of communication. Popular methods for digital security are the encryption of messages, emails, and other data through Signal, VPN, or USB verification keys. Another method to disguise metadata is to use burner phones, secondary email addresses set up on not on a private or work computer, or the anonymous Tor browser. The most trusted way to communicate with sources remains to meet physically, while leaving phones at home and making sure that the location is not under surveillance. Finally, journalists should always keep in mind that physical and digital documents often contain

cues revealing the time and place it was downloaded or printed. When publishing potentially harmful or sensitive material, they should always make sure to scrub documents of those traces.

6. Conclusion

By researching the five main questions from the previous chapters, this thesis firstly finds that the reporters and editors-in-chief questioned for this research outline a number of developments they feel threaten source protection. These are primarily the vulnerabilities of digital devices such as phones, laptops, and smart home appliances. They collect more and more data, creating more and more risks of leaks for journalists who are trying to protect and anonymize the identity of their sources. It also makes journalists susceptible to leaving online data traces. This fear is fueled by the recent introduction of Dutch legislation allowing for mass-scale cable interception. It makes it more likely that a journalists' data can be intercepted by intelligence agencies, as shown in Research Questions 1 and 2. Although legislation outlining the limits of targeted surveillance on journalists seems adequate, safeguards built to prevent the excessive use of special coercion methods are not up to the task of protecting the press, as there are numerous loopholes ways around them (Modderkolk, Minkema, Kranen, Hogeling, & van der Wauw, 2016). A second factor that the respondents to this thesis mark as a threat to source protection, are the actions of the Public Prosecution Service. It overstepped its mandate in 2018 in three separate cases, violating rules aimed to protect journalists' position, as shown in Research Question 4. In the case of Jos van de Ven from Brabants Dagblad this led to the name of his source to become known to law enforcement through an illegitimate way. The third and final threat respondents point to is the number of their coworkers in the newsroom that are inexperienced in applying even the most basic security measures to protect their data and who fail to outline possible risks their sources face as a result of a lack of understanding of digital security concerns.

Second, this thesis also finds that in order to minimize the risks to source protection mentioned above, journalists need to invest more time and energy in securing their communications in order to be able to protect their sources' identity. As mentioned in the previous paragraph, journalists themselves are not always equipped to accurately assess digital security risks. Respondents questioned for this thesis note that many of their colleagues are running unnecessary risks and fail to take basic steps to improve their digital security, like using more complex passwords for their email. This makes them and their sources vulnerable to exposure. It is absolutely vital that journalists who regularly use anonymous sources for their reporting invest in digital security, but a basic level of

protection is needed for every journalist, just as it is for every private citizen. Newsrooms have a responsibility in educating their staff about digital security, since ultimately they as an institution guarantee a source anonymity (Abramowicz, 2008). However, investments in security measures can be costly, especially for small newsrooms. While the New York Times can appoint a Senior Director of Information Security, a small regional newspaper like Brabants Dagblad might not have the funds, nor feel the need and urgency to invest in digital security. This finding is supported by the remarks of Lucas van Houtert, the editor-in-chief of Brabants Dagblad. Despite the fact that the phone records of one of his reporters were recently illegally obtained by the Public Prosecution Service, exposing the reporter's source, Van Houtert does not feel the need to focus on more security measures.

Third, this thesis finds that journalists do not feel that recently introduced legislation like the amendments to the WIV 2017 and the internal guidelines of the Public Prosecution Office aimed to protect a journalists' right to source protection makes them and their sources safer. They feel that it is becoming increasingly difficult to guarantee source protection and that recently implemented safeguards fail to make them feel protected in their day-to-day reporting. Some respondents note the complete lack of oversight of the Public Prosecution Office and their use of special coercion methods from the WIV 2017. This lack of independent oversight has resulted in at least three cases of the office breaking protocol and unlawfully obtaining private communications revealing the identity of the source. It has to be said that the provisions in Dutch prosecution law allowing journalists to hold the court in contempt are seen by many as long-overdue protections, but Bart Mos points out that journalists never had any other choice than to hold the court in contempt, as revealing a source's identity damages a reporters' reputation beyond repair.

In answering the central research question of this thesis, i.e., to what extent journalists are capable of protecting the identity of their sources in times of digital government surveillance, we can reach the conclusion that due to technological advancements and far-reaching mandates for Dutch intelligence agencies it becomes increasingly difficult for journalists to conceal the identity of their sources.

Recommendations

Following the answer to the central research question, it is recommended that journalists invest heavily in safeguarding communications and building up a digital security arsenal in order to be able to provide anonymity to their sources. Digital security can be a cat-and-mouse game and journalists should put more effort in keeping up with developments in this field, even with measures as simple as using a password protector, or

encrypted messaging services like Signal. Newsrooms play an important role in creating this awareness among their reporters and should invest heavily in setting up encrypted communication channels that enable potential sources to reach out to reporters. Furthermore, they should also assist their reporters in securing their data and communications. Investments in digital security could potentially have a return on investment for newsrooms as it instills trust in a source to come forward and could potentially lead to exclusive reporting.

Finally, the conclusions in this thesis result in a call for independent oversight on the Public Prosecution Service in their use of special coercion methods on journalists. While the Dutch intelligence agencies AIVD and MIVD are overseen by the TIB and CTIVD, there is a lack of independent oversight on the Public Prosecution Service and their use of special coercive methods concerning journalists. This has resulted in three known cases –Van de Ven, Bremer, and Keulen– where the prosecution has overstepped its mandate. Besides more oversight, a lot can be achieved by emphasizing the special position that journalists have in the education of prosecutors, a point that secretary of the Dutch Union for Journalists (NVJ) Thomas Bruning has previously stressed to the Board of Prosecutors General.

Reflection on the research

Source protection for journalists continued to be a relevant subject of inquiry throughout writing this thesis. I have been able to continually update findings with new reports of the oversight committees since the new legislation on the Dutch intelligence agencies went into effect and could draw on a number of recent cases of infringements of source protection with grave consequences for reporters and sources. The intelligence agencies and their conduct continued to be of interest to a number of Dutch journalists, allowing me to update my writing along the way drawing from their reporting.

Picking a relevant research topic has made writing this thesis a pleasant experience. The subject was noticeably relevant to the respondents who have been interviewed and they were eager to sit down and elaborate on their experiences. I have been able to draw on extensive interviews with reporters and editors who have first-hand experience with the subject of source protection, and this has yielded a large amount of valuable and useful date. In picking suitable candidates I have made use of personal recommendations by people who had been approached, leading to a less representative, but higher in-depth quality sample-size. This convenience sampling has some slight drawbacks, namely the fact that most of my respondents are from only two outlets: De Volkskrant and Nieuwsuur. This however only has a limited negative effect on the obtained data, since neither tone nor image of their medium is of importance, but rather the individual respondents' previous record of reporting. In selecting respondents I have made the choice for journalists and reporters with a clear relation to reporting on the intelligence agencies themselves, or to fields like Islamic radicalism and security. The latter are fields that the AIVD and MIVD have a special interest in, affecting the way reporters handle their sources. One element I regret not making a bigger effort for, is a better gender representation of the respondents. Of all seven respondents of this thesis only one is female. Even though a respondent's gender theoretically has no effect on their views regarding any one of the research questions, striving for better gender representation in academia is a cause of importance. Of the primary academic literature used for this thesis, however, a large part has been written by female academics, making the balance in the theoretical part of this research more even.

Using a method of open coding helped significantly when it came to processing and analyzing the results from the individual expert interviews. It helped sifting through the large

amount of answers and comments by the respondents and made it an uncomplicated effort to structure arguments and reach logical conclusions. A point of critique is that instead of producing a list of codes after having transcribed the interviews, it is better to begin the process of data gathering by figuring out the codes and basing the questionnaires on the preconceived codes. This way it is easier to stick to the structure of the research during the interview and not get distracted by information that is interesting, but not relevant. This issue, however, was circumvented by conducting the interviews using a topic list of themes relevant to the research and using that as a basis for producing a list of codes. Besides that, strictly sticking to preconceived codes laid out in advance and narrowly working down a list of standardized questions would not have worked, since it goes against common practices of journalism and makes it impossible to highlight topics raised during the interview. Straying from the topics every now and then has uncovered some interesting details during the interviews that proved relevant and useful in answering the research questions. Also, due to my own background studying journalism, I was able to relate to the challenges journalists face when reporting on complicated and secretive government affairs. Though not having used anonymous sources myself, I am familiar with governments and organizations not eager to talk about their secretive business through my experience working for BNR Nieuwsradio and the Washington DC bureau of Dutch broadcaster NOS.

Part of what helped me write this thesis is that the central research question has been sufficiently narrowed down, making it relatively easy to separate between what is and what is not of relevance to this topic. Together with a clearly defined research schematic, and a strict separation between the literature review in the first part and the data analysis based on personal qualitative interviews in the second part, it was significantly less complicated to stick to the essence of the matter. Worth mentioning is the effort of Drs. Timon Ramaker, senior lecturer in Journalism and Ethics at the Ede University of Applied Sciences, in helping me structure my thesis and thoroughly vetting my arguments. Finally, opting to write this thesis in English has been a wise choice, not only because of a personal preference in writing on academic topics, but also because a sizeable share of the available literature used for this thesis is in English. Interviews were conducted and transcribed in Dutch and translated when used to answer the research questions, so translation of data and sources would have been part of the process anyway when having opted to write this thesis in Dutch.

Due to the fact that the new legislation on the Dutch intelligence community, and regulations regarding source protection are both very recent, this thesis only serves as a starting point for future qualitative research when the long-term effects on journalistic practices become clear. This could be done by conducting similar research in five or ten years

time, based on further interviews and future reports by the commissions like TIB and CTIVD regulation the intelligence agencies.

To conclude: clearly structuring my work has helped me write a thesis that touches on a highly relevant question within the field of journalism and digital surveillance. The conclusion of this research produces useful recommendations for journalists in their everyday life on the newsroom and in their use of confidential sources. The thesis was clearly structured in advance and I was able to remain faithful to the outline throughout the process of gathering and analyzing the data, and writing the thesis.

References

Abramowicz, D. (2008). *Calculating the Public Interest in Protecting Journalists' Confidential Sources.* (Columbia Law Review, Vol. 108, No. 8): pp. 1949-1990

Austin, L.M. (2015). *Lawful Illegality: What Snowden Has taught Us about the Legal Infrastructure of the Surveillance State.* In Geist, M. (Ed.), *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (pp. 103-120). Ottawa; University of Ottawa Press.

Beleidsregels WIV 2017 (May 1, 2018) Retrieved on November 8, 2018, from https://wetten.overheid.nl/BWBR0040860/2018-05-01

Bernstein, C., & Woodward, B. (1974). *All the President's Men.* New York: Simon & Schuster

Bockting, B.J. (2012, March 30). Journalist ten onrechte beschuldigd. *De Volkskrant.* Retrieved on January 21, 2019, from https://www.volkskrant.nl/nieuws-achtergrond/journalist-ten-onrechte-beschuldigd~b36f9bfe/

Brabants Dagblad (2018, June 8). *OM door het stof na opvragen belgegevens BD-journalist.* Retrieved on January 3, 2019, from https://www.bd.nl/s-hertogenbosch/om-door-het-stof-na-opvragen-belgegevens-bd-journalist~a6c41fd6/

Collins, K. (2017, June 10). Computer printers have been quietly embedding tracking codes in documents for decades. *Quartz.* Retrieved on January 15, 2019, from https://qz.com/1002927/computer-printers-have-been-quietly-embedding-tracking-codes-in-documents-for-decades/

Columbia Global Freedom of Expression. (n.d.). *Goodwin v. United Kingdom.* Retrieved on November 11, 2018 from https://globalfreedomofexpression.columbia.edu/cases/goodwin-v-united-kingdom/

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (2009) *Toezichtsrapport 22a over de samenwerking van de AIVD met buitenlandse inlichtingen en veiligheidsdiensten*. Retrieved on November 21, 2018, from https://www.ctivd.nl/documenten/rapporten/2009/09/30/index

de Poot, C.J., & Flight, S. (2015). *Ruimte om te delen. De CT infobox tien jaar in werking*. Evaluation from Research and Documentation Centre (WODC) of CT infobox after ten years of operation. Retrieved on November 15, 2018, from https://www.wodc.nl/binaries/2482-volledige-tekst_tcm28-73660.pdf

De Volkskrant (2006, November 27). *Telegraaf-journalisten in gijzeling genomen*. Retrieved on January 10, 2019, from https://www.volkskrant.nl/nieuws-achtergrond/telegraaf-journalisten-in-gijzeling-genomen~b1ea3185/

European Court of Human Rights. (1996, March 27). *Case of Goodwin v. United Kingdom (Application no. 17488/90)*. Retrieved on November 11, 2018 from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57974%22]}

Ganguly, M. (2017, January 13). WhatsApp design feature means some encrypted messages could be read by third party. *The Guardian*. Retrieved on January 15, 2019, from https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages

Grapperhaus, F.B.J. (2018, October 17). *Toespraak door minister Grapperhaus bij het Symposium Bronbescherming Journalisten*. Retrieved on November 6, 2018 from https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/documenten/toespraken/2018/10/17/toespraak-door-minister-grapperhaus-bij-het-symposium-bronbescherming-journalisten

Haenen, M., & Dupuy, L. (2018, June 8). OM vroeg belgegevens journalist op. *NRC Handelsblad*. Retrieved on October 4, 2018, from https://www.nrc.nl/nieuws/2018/06/08/openbaar-ministerie-heeft-telefoongegevens-journalist-opgevraagd-a1605895

Harvard Law Review Association (June, 2009). *Media Incentives and National Security Secrets*. (Harvard Law Review, Vol. 122, No. 8): pp. 2228-2249

Hennis-Plasschaert, J.A., & Plasterk, R.H.A. (2014, July 3). *Convenant AIVD – MIVD inzake de Joint Sigint Cyber Unit*. [Letter to Parliament] Retrieved on November 15, 2018, from https://zoek.officielebekendmakingen.nl/blg-359723.pdf

Hijink, M., van Lonkhuyzen, L., Pelgrim, C., & Versteegh, K. (2018, July 12). Met een sleepnet door het internet op zoek naar terroristen. *NRC Handelsblad*. Retrieved on November 14, 2018, from https://www.nrc.nl/nieuws/2017/07/12/met-een-sleepnet-door-het-internet-op-zoek-naar-terroristen-6580813-a1544813

Hijink, M. (2018, December 12). Stilte graag, de geheime dienst wil afluisteren. *NRC Handelsblad*. Retrieved on January 3, 2019, from https://www.nrc.nl/nieuws/2018/12/12/geen-volwaardig-5g-netwerk-voor-noord-nederland-want-dat-verstoort-de-oren-van-de-mivd-a3060455

Kreling, T., & Modderkolk, H. (2017, September 8). Zij helpt journalisten zichzelf en hun bronnen te beschermen. *De Volkskrant*. Retrieved on January 14, 2019, from https://www.volkskrant.nl/cultuur-media/zij-leert-journalisten-zichzelf-en-hun-bronnen-te-beschermen~b31d5f3f/

Kroon, M. (2018, February 8). 'Het was op dat moment hij of ik'. *Algemeen Dagblad*. Retrieved on January 3, 2019, from https://www.ad.nl/binnenland/enlsquo-het-was-op-dat-moment-hij-of-ikenrsquo~a7445621/

Leijten, J. (2018, October 18). Mag OM dwangmiddelen inzetten tegen journalisten? *NRC Handelsblad*. Retrieved on November 20, 2018, from https://www.nrc.nl/nieuws/2018/10/18/mag-om-dwangmiddelen-inzetten-tegen-journalisten-a2637194

Lowenthal, M.M. (2016). *Intelligence. From Secrets to Policy*. (Rev. Ed.) Washington, United States: SAGE Publications Inc.

Modderkolk, H. (2018, January 26). Hackers AIVD leverden cruciaal bewijs over Russische inmenging in Amerikaanse verkiezingen. *De Volkskrant*. Retrieved on January 3, 2019, from https://www.volkskrant.nl/nieuws-achtergrond/hackers-aivd-leverden-cruciaal-bewijs-over-russische-inmenging-in-amerikaanse-verkiezingen~b32c6077/

Modderkolk, M., Minkema, M., Kranen, H., Hogeling, T., & van der Wauw, W. (2016). *Zo sluipt de geheime dienst bij u naar binnen*. Retrieved on November 25, 2018, from https://www.volkskrant.nl/kijkverder/2016/afluisteren/

Mora, J. (2017, August 17). Demystifying the Signal Protocol for End-to-End Encryption (E2EE). *Medium*. Retrieved on January 15, 2019, from https://medium.com/@justinomora/demystifying-the-signal-protocol-for-end-to-end-encryption-e2ee-ad6a567e6cb4

Newman, L.H. (2018, June 14). Encrypted Messaging Isn't Magic. *Wired*. Retrieved on January 16, 2019, from https://www.wired.com/story/encrypted-messaging-isnt-magic/

Nieuwsuur (2015, January 21). *Snowden: AIVD en MIVD zijn ondergeschikt aan de VS*. Retrieved on November 21, 2018, from https://nos.nl/nieuwsuur/artikel/2014570-snowden-aivd-en-mivd-zijn-ondergeschikt-aan-de-vs.html

Nieuwsuur (2018, February 23). Retrieved on January 3, 2019, from https://www.npostart.nl/nieuwsuur/23-02-2018/VPWON_1282936

NOS (2012, November 22). *Telegraaf wint zaak tegen de Staat*. Retrieved on January 10, 2019, from https://nos.nl/artikel/443508-telegraaf-wint-zaak-tegen-de-staat.html

NOS (2018, March 23) *Eindstand referendum: meer kiezers tegen sleepwet dan voor*. Retrieved on November 8, 2018, from https://nos.nl/artikel/2223978-eindstand-referendum-meer-kiezers-tegen-inlichtingenwet-dan-voor.html

NOS (2018, July 5). *Ook Rotterdamse OM in de fout met journalist*. Retrieved on January 14, 2019, from https://nos.nl/artikel/2240029-ook-rotterdams-om-in-de-fout-met-journalist.html

NOS (2018, October 17). *Hoe werkt bronbescherming journalisten?* Retrieved on January 28, 2019, from https://www.nvj.nl/nieuws/zo-werkt-wet-bronbescherming

NPO Ombudsman (2018, March 9). *Handen af van het staatsgeheim!?* Retrieved on January 29, 2019, from https://ombudsman.npo.nl/uitspraken-en-columns/handen-af-van-het-staatsgeheim

Ollongren, K.H., & Bijleveld-Schouten, A.Th.B. (2018, April 6). *Reactie raadgevend referendum Wet op de inlichtingen- en veiligheidsdiensten.* [Letter to Parliament] Retrieved on November 8, 2018, from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/04/06/kamerbrief-met-reactie-op-raadgevend-referendum-wet-op-de-inlichtingen-en-veiligheidsdiensten

Oranje, J (2018, February 23). 'Verantwoording over het niet-publiceren inzake onrust commando's'. *Nieuwsuur*. Retrieved on January 3, 2019, from https://nos.nl/nieuwsuur/artikel/2219122-verantwoording-over-het-niet-publiceren-inzake-onrust-bij-commando-s.html

OWASP (December 12, 2017). *Keynote - Runa Sandvik - Building a Culture of Security at The New York Times - AppSecUSA 2017.* Retrieved on January 14, 2019, from https://www.youtube.com/watch?v=_iCLs4jw_yo&t=1104s&index=12&list=WL

Posetti, J. (2017) *Protecting Journalism Sources in the Digital Age*. Paris: UNESCO.

Referendumcommissie (2018). *Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten*. Retrieved on November 8, 2018, from https://www.referendum-commissie.nl/binaries/referendumcommissie/documenten/publicaties/2018/01/18/samenvatting-van-de-wet-op-de-inlichtingen--en-veiligheidsdiensten-2017/ReferendumWiv_pdf4-samenvatting.PDF

Reporters Without Borders (2018). *Issues of national identity at the center of debates.* Report on press freedom in The Netherlands. Retrieved on November 6, 2018, from https://rsf.org/en/netherlands

RTL (2018, September 13). *Fotograaf de cel in na weigering camera aan politie te geven.* Retrieved on January 14, 2019, from https://www.rtlnieuws.nl/nederland/artikel/3036646/fotograaf-de-cel-na-weigering-camera-aan-politie-te-geven

Rubio, A. I. (2018, July 5). OM gebruikte zonder toestemming telefoongegevens Rotterdamse journalist. *Algemeen Dagblad.* Retrieved on January 21, 2019, from https://www.ad.nl/rotterdam/om-gebruikte-zonder-toestemming-telefoongegevens-rotterdamse-journalist~ad0f02d1/

Schuijt, G.A.I. (2006) *Vrijheid van nieuwsgaring*. Den Haag: Boom Juridische uitgevers.

Smeets, M. (2018, February 8). The Netherlands just revealed its cyber capacity. So what does that mean? *The Washington Post.* Retrieved on November 15, 2018, from https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/08/the-netherlands-just-revealed-its-cybercapacity-so-what-does-that-mean/?utm_term=.0e2226216553

Staatsblad, 2018 (264), 1-4. (2018) *Wet van 4 juli 2018 tot wijziging van het Wetboek van Strafvordering tot vastlegging van het recht op bronbescherming bij vrije nieuwsgaring (bronbescherming in strafzaken).* Retrieved on November 8, 2018 from https://zoek.officielebekendmakingen.nl/stb-2018-264.html?zoekcriteria=%3fzkt%3dUitgebreid%26pst%3dStaatsblad%26dpr%3dAlle%26spd%3d20181108%26epd%3d20181108%26jgp%3d2018%26nrp%3d264%26sdt%3dDatumUitgifte%26orgt%3dministerie%26planId%3d%26pnr%3d1%26rpp%3d10&resultIndex=0&sorttype=1&sortorder=4

Toetsingscommissie Inzet Bevoegdheden (2018, April 25). *Jaarverslag TIB 2018-2019.* Retrieved on June 16, 2019.

van den Dool, P., & Versteegh, K. (2018, November 1). 'De geheime diensten zijn regelmatig niet blij met ons.' *NRC Handelsblad.* Retrieved on November 14, 2018, from https://www.nrc.nl/nieuws/2018/11/01/burgercommissie-wilde-informatie-over-hackverzoeken-openbaren-a2753592

Versteegh, K. (2017, February 7). De TomTom van de terreurbestrijding. *NRC Handelsblad*. Retrieved on November 15, 2018, from https://www.nrc.nl/nieuws/2017/02/07/de-tom-tom-van-de-terreurbestrijding-6414571-a1544831

VICE Nederland (2018, March 1). *We spraken AIVD-baas Rob Bertholee over de sleepwet en wat de AIVD allemaal mag hacken*. Retrieved on November 8, 2018, from https://www.youtube.com/watch?v=JfhDXVRScrc

Wet op de Inlichtingen- en Veiligheidsdiensten 2017 (May 1, 2018) Retrieved on November 21, 2018, from https://wetten.overheid.nl/BWBR0039896/2018-05-01

Zetter, K. (2014, November 11). Hacker Lexicon: What is a Zero Day? *Wired*. Retrieved on January 15, 2019, from https://www.wired.com/2014/11/what-is-a-zero-day/