Scientific

OPEN SOURCING EVIDENCE FROM THE INTERNET- THE PROTECTION OF PRIVACY IN CIVILIAN CRIMINAL INVESTIGATIONS USING OSINT (OPEN-SOURCE INTELLIGENCE)

Leonore ten Hulsen[*]

ABSTRACT

This paper explores the relationship between open-source intelligence and privacy in the context of civilian criminal investigations. The existing legal mechanisms that could apply to open-source intelligence (OSINT) and civilian criminal investigations are discussed but a lack of suitable regulations is identified. Moreover, the legal, political and ethical implications of OSINT on the traditional privacy framework are discussed with the use of a case study. A paradoxical situation is identified, in which publicly available information is thought to be free from privacy concerns based on the fact that it is publicly available, although the information can be (sensitive) personal information and therefore inherently private. A theoretical solution is proposed to fill this lacuna in the law, consisting of a combination of Nissenbaum's theory on privacy as contextual integrity and Koops' theory on a new privacy proxy of a digital home right. This could provide legal privacy protection in civilian criminal investigations using OSINT, creating a just balance between investigation interests and privacy concerns. This research can serve as a guideline when drafting future privacy regulations regarding open-source intelligence and civilian criminal investigations.

Keywords: Open-source intelligence (OSNIT), civilian criminal investigations, vigilante justice, privacy, criminal investigations, publicly available sources, open source.

Introduction

The role of civilians in criminal investigations is changing due to our increasingly digitalized society.[1] The rapid technological developments create substantial disruptions, having an impact in every sphere of human activities.[2] The possibilities that computers and the internet hold are no longer reserved for a few, with over 98% of people in the Netherlands having access to the internet in 2018.[3] The internet and the World Wide Web have provided us with a platform to

---

[*] *Leonore ten Hulsen is a recent graduate of the LLM. in Internet, Intellectual Property and ICT-law programme at the Vrije Universiteit Amsterdam.*

[1] Eelco Moerman, 'Burgers in het Digitale Opsporingstijdperk' (2019) 94 NJB 1, 1.

[2] Marinko Maslarić & Svetlana Nikoličić & Dejan Mirčetić, '*Logistics Response to the Industry 4.0: The Physical Internet*' (2016) 6(1) Open Engineering 511, 511.

[3] Excluding the age group 65+, the percentage of internet users in that group is somewhat lower, at 86.4% in 2018. CBS, 'Internet Toegang, Gebruik en Faciliteiten' at:

share and gather information, which has fundamentally changed our relationship to accessing information and problem-solving. The internet has made vast amounts of data more accessible than ever before.[4]

This includes lots of publicly available data, also referred to as open-source information, which this paper defines in accordance with Klitou's definition as:

'anything publicly available, whether online or offline, such as blogs, tweets, information posted on social networking sites, videos, web chats or any other user-generated content, (online) news, websites, public data, geospatial data, books, academic papers, newspapers, magazines and even book or movie reviews'.[5]

These online data can be used for open-source intelligence (OSINT). OSINT is an intelligence gathering discipline which this paper defines in accordance with Best's definition as 'the retrieval, extraction and analysis of information from publicly available sources'.[6] Governmental, non-profit and business organizations alike recognize the value of open-source information as it provides strategic, fast and cost-effective intelligence sources, and OSINT has also increasingly been accepted as evidence in court.[7]

Where the police once held the monopoly on investigating criminal activities, the internet has opened up this possibility to many other interested parties. Civilians have the internet to use their voice and skills, enabling them to access data about crimes once only available to the police, empowering them to do their own research.[8] This research has been referred to as civilian policing or civilian criminal investigations, defined as 'forms of online collective action aimed at pooling resources to investigate online crime'.[9]

<https://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83429NED&D1=0,2-5&D2=0,3-6&D3=0&D4=a&HDR=T&STB=G1,G2,G3&VW=T> accessed 28 March 2019.

[4] Michael Glassman & Min Ju Kang, 'Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)' (2012) 28(2) *Computers in Human Behaviour* 673, 674.

[5] The terms publicly available data or information and open-source data or information will be used interchangeably throughout this paper; Demetrius Klitou, 'Privacy-Invading Technologies: Safeguarding Privacy, Liberty & Security in the 21st Century' [2012] Centre for Law in the Information Society, Faculty of Law, Leiden University 1, 61.

[6] Clive Best, 'Open Source Intelligence' in Françoise Fogelman-Soulié, Domenico Perrotta, Jakub Piskorski and Ralf Steinberger (eds), *Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining and Their Applications to Security* (IOS Press 2008), 331.

[7] Idem p. 332; Menno Sedee, 'Bellingcat-oprichter: 'Wij Helpen Degenen aan de Andere Kant' *NRC* (2 November 2018) <www.nrc.nl/nieuws/2018/11/02/bellingcat-oprichter-wij-helpen-degenen-aan-de-andere-kant-a2753704> accessed 27 March 2019; Hans Pool, *Bellingcat - Truth in a Post-Truth World* (VPRO 2Doc Documentary 2018)

[8] Eelco Moerman, 'Burgers in het Digitale Opsporingstijdperk' (2019) 94 NJB 1, 2.

[9] In Huey et al. the definition also contains 'and report information to law enforcement', but this paper will not focus exclusively on civilians seeking to assist the police and therefore leave this out of the definition. Laura Huey, Johnny Nhan and Ryan Broll, "Uppity Civilians' And 'Cyber-Vigilantes': The Role of The General Public In Policing Cyber-Crime' (2012) 13 Criminology & Criminal Justice 81, 83.

Use of OSINT by state authorities could pose privacy challenges, but less attention has been given to the potentially problematic privacy concerns posed by civilian criminal investigations by means of OSINT,[10] even though civilian investigators or "netizens", can also include internet vigilantes.[11]

Civilian policing of the internet is both relevant and prevalent in today's society,[12] and therefore civilian criminal investigations by means of OSINT will be the focus of this paper. Both civilian investigators aiming at aiding law enforcement and internet vigilantes or "digilantes"[13] creating their own version of vigilante justice through measures like doxxing[14] or online shaming, will be discussed.

Bellingcat

One of the private parties making use of OSINT is Bellingcat, a UK-based open-source investigation platform run by volunteering civilians who, in their own words, 'use open source and social media to investigate a variety of subjects, from Mexican drug lords to conflicts being fought across the world'.[15] Oftentimes they use crowdsourcing to aid their investigation, using the power of the crowd to their advantage instead of hiring specialists. Since its establishment in 2014, Bellingcat has gained global fame and acknowledgement, *inter alia* for its contribution to the MH17 research and its research on the suspects of the poisoning of the Russian ex-spy Sergej Skripal and his daughter in Salisbury in March 2018.[16]

Bellingcat is planning on setting up teams in various Dutch cities to research local issues according to the "Bellingcat Method".[17] This method entails looking through open-source

[10] Bert-Jaap Koops & Jaap-Henk Hoepman & Ronald Leenes, 'Open-Source Intelligence and Privacy by Design' (2013) 29 *Computer Law & Security Review* 676, 677.

[11] I define internet vigilantes, also called digilantes or netilantists, as internet users that engage in online activity including 'scam baiting, public shaming, distributed denial of service attack, google bombing, identity theft activism, anti-paedophile activism and counter-terrorism', see: Ramesh Palvai, 'Internet Vigilantism, Ethics and Democracy' (2016) 1 Anveshana's International Journal of Research in Regional Studies, Law, Social Sciences, Journalism and Management Practices 124, 124. This differs from a civilian criminal investigator, as the latter does not necessarily have to partake in online vigilante justice.

[12] Laura Huey & Johnny Nhan & Ryan Broll, "Uppity Civilians' And 'Cyber-Vigilantes': The Role of The General Public in Policing Cyber-Crime' (2012) 13 *Criminology & Criminal Justice* 81, 81-97.

[13] The terms digilantes and civilian criminal investigators will be used interchangeably throughout this paper.

[14] Doxxing is defined in this paper as the 'use of the internet to search for and publish identifying information about a particular individual, typically with malicious intent' in accordance with: Jeffrey Pittman, 'Privacy in the Age of Doxxing' (2018) 10 Southern Journal of Business & Ethics 53, 53.

[15] Bellingcat – 'About' (2019) at: <www.bellingcat.com/about/> accessed 26 March 2019.

[16] Hans Pool, *Bellingcat - Truth in a Post-Truth World* (VPRO 2Doc Documentary 2018) <www.2doc.nl/documentaires/series/2doc/2018/november/bellingcat.html> accessed 27 March 2019; Menno Sedee, 'Bellingcat-oprichter: 'Wij Helpen Degenen aan de Andere Kant' *NRC* (2 November 2018) <www.nrc.nl/nieuws/2018/11/02/bellingcat-oprichter-wij-helpen-degenen-aan-de-andere-kant-a2753704> accessed 27 March 2019.

[17] Gijs Beukers, 'Onderzoekscollectief Bellingcat komt naar Nederland' *De Volkskrant* at: <www.volkskrant.nl/nieuws-achtergrond/onderzoekscollectief-bellingcat-komt-naar-nederland~be070e83/> accessed 27 March 2019; Menno Sedee, 'Bellingcat-oprichter: 'Wij Helpen

information on platforms like YouTube, social media and Google Earth. These tools can be used to answer questions on who, what and where a certain bombing, attack or other event took place.[18] Interestingly, in comparison to traditional criminal investigational research by the police, Bellingcat publishes all of its methods and findings in detail online.

Shahin Gheiybe

On 19 March 2019, Bellingcat released an article on localizing a Dutch criminal called Shahin Gheiybe, who escaped prison in 2011 and has been a fugitive ever since. He had been sentenced to thirteen years in prison for two attempted murders and robbing the victims of 175.000 euro.[19] In March 2019, he was placed on the Dutch most-wanted list of fugitive criminals.[20] The case caught public attention after the police spread pictures and videos of him on a Dutch national TV-show and YouTube channel, asking the public for tips about his current location.[21]
Shahin Gheiybe seems to challenge the police by posting pictures on his Instagram with phrases like 'catch me if you can' and holiday pictures.[22] A week after he was placed on the Dutch most-wanted list, he uploaded a video stating people should not believe everything the media tell them and mocking the police. He continued by stating that he is going to enjoy his freedom and the nice weather, showing his belief that he is safe from being found.[23]

A week after the Dutch police asked for tips on Shahin Gheiybe's location, Bellingcat managed to track down his last known location based on his Instagram posts – over 170 pictures and videos – with the help of over 60 Twitter users.[24] Shahin Gheiybe himself confirmed that the house Bellingcat found was his most recent location, although it is unclear whether he is still residing there.[25] Even though the criminal himself cannot be arrested yet because of a lack of extradition

Degenen aan de Andere Kant' *NRC* (2 November 2018) <www.nrc.nl/nieuws/2018/11/02/bellingcat-oprichter-wij-helpen-degenen-aan-de-andere-kant-a2753704> accessed 27 March 2019.

[18] Menno Sedee, 'Bellingcat-oprichter: 'Wij Helpen Degenen aan de Andere Kant' *NRC* (2 November 2018) <www.nrc.nl/nieuws/2018/11/02/bellingcat-oprichter-wij-helpen-degenen-aan-de-andere-kant-a2753704> accessed 27 March 2019.

[19] Sebastiaan Quekel, 'Gezochte 'gangster' Schoot Zijn Zakenpartners Bijna Dood in Den Bosch: Wat Gebeurde er Tijdens de Deal?' *Algemeen Dagblad* (6 March 2019) <www.ad.nl/den-bosch/gezochte-gangster-schoot-zijn-zakenpartners-bijna-dood-in-den-bosch-wat-gebeurde-er-tijdens-de-deal-br~a4004741/> accessed 27 July 2019.

[20] Shahin Gheiybe 'Nationale Opsporingslijst' at *politie.nl* <www.politie.nl/gezocht-en-vermist/nationale-opsporingslijst/2019/maart/shahin-gheiybe.html> accessed 28 March 2019; 'Ontsnapte Gevangene Shahin Gheiybe (35) op Nationale Opsporingslijst' *Avrotros Opsporing verzocht* (5 March 2019) <https://opsporingverzocht.avrotros.nl/zaken/zaak/ontsnapte-gevangene-shahin-gheiybe-35-op-nationale-opsporingslijst/> accessed 28 March 2019.

[21] Ibid.

[22] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 28 March 2019.

[23] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 28 March 2019.

[24] Ibid.

[25] Twitter, account 'Henkvaness',

agreements between Iran and the Netherlands, this case shows the potential impact civilian criminal investigations using OSINT can yield.

This paper will use the case study of Bellingcat's research on Shahin Gheiybe to answer the following research question:

Do civilians' criminal investigations using OSINT impact the privacy of their suspects and if so, how can their privacy be protected?

This paper is structured as follows. Firstly, the legal framework of traditional and civilian criminal investigations is discussed, including when restrictions of privacy are granted. This is done in light of the changing landscape of criminal investigations and the emergence of digilantes and online vigilante justice with the aim of researching the privacy impact of OSINT, while focusing on civilian criminal investigations.

Afterwards, the horizontal direct effect of fundamental rights[26] is discussed in light of the case-study, to continue the evaluation of whether privacy violations occurred in Bellingcat's research specifically. This is important in light of the research question as it will exemplify, with the use of a case study, what the difficulty is in assessing whether civilian criminal investigations using OSINT impact the privacy of their suspects.

Subsequently, an analysis follows of the ethical and political desirability of the practice of OSINT, civilian criminal investigations and vigilante justice, as it is necessary to qualify the use of the practice before proposing methods to regulate it. Lastly, the political philosophical framework of privacy is elaborated upon and the influence that civilian criminal investigations have by means of OSINT on the privacy of their suspects. This includes discussing how public open-source information truly is or should be.

This paper argues that current regulations are not yet adapted to the privacy challenges posed by OSINT. A mixture between Koop's proxy of a digital home, specified on certain cyberspaces, and Nissenbaum's theory on privacy as contextual integrity is suggested, to ensure more effective privacy protection.

This paper aims to give coherent recommendations on a possible legal framework to protect privacy in civilian criminal investigations by means of OSINT, as well as ensuring the maintenance of an effective judicial system in a digitalizing society.

<https://twitter.com/henkvaness/status/1108679041274560512/photo/1?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1108679041274560512&ref_url=https%3A%2F%2Fwww.bellingcat.com%2Fnews%2Fuk-and-europe%2F2019%2F03%2F19%2Flocating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram%2F> accessed 28 March 2019.

[26] The horizontal direct effect of fundamental rights means that fundamental rights

I. The Legal Basis of Traditional Criminal Investigations

Before looking at civilian criminal investigations based on OSINT, it is necessary to make a distinction between governmental and civilian criminal investigations. To understand whether civilians' criminal investigations using OSINT impact the privacy of their suspects, firstly the current European legal framework on OSINT by police investigations is explained. Using this basis, the use of OSINT by non-public authorities can be assessed afterwards. It should be kept in mind that this legal framework is shaped by the traditional framework on privacy. Hence, this paper starts by explaining the traditional theories and principles on privacy and the legal basis of traditional criminal investigations using OSINT.

1. Traditional Theories and Principles on Privacy

Our traditional privacy framework is built around three principles: limiting surveillance of citizens and use of information about them by the government, restricting access to 'intimate, sensitive or confidential information' and imposing restrictions on places or spheres that are (more) private.[27] These principles are present in every approach to privacy protection.[28] The first principle refers to the more general balancing of powers and protecting citizens against governmental abuse.[29] As this paper focuses on civilian criminal investigations using OSINT, the latter two principles are most relevant.

The second principle, also referred to as information privacy, refers to the nature of information and how societal standards judge its level of 'intimacy, sensitivity or confidentiality'.[30] Following this second principle, the sensitivity or intimacy of information determines whether a privacy violation takes place, not the way it is collected or analysed.[31] This is why sensitive information is more protected under the GDPR, regardless of how it is analysed or collected.[32]

The third principle, which is specified as location privacy in this paper, refers to privacy connected to certain places, like one's home.[33] Depending on the privacy of a setting, the severity of the privacy violation is judged.[34] This principle stems from our common belief that certain private places should be guarded against unwanted interference[35] and can be found in most constitutions, including the Dutch constitution.[36]

---

[27] Idem p. 125.
[28] Idem p. 124.
[29] Idem p. 125.
[30] Idem p. 128.
[31] Idem p. 128.
[32] Article 6(4)(c), 9, 22(4), 27(2)(a), 30(5), 35(3)(b), 37(1)(c) and 47(2)(d) GDPR and preamble 51, 52, 53, 54, 71, 91 GDPR.
[33] Although the second and third principle can overlap somewhat, they are distinct principles. The principle of information privacy focuses on the value of the information at hand. The principle of location privacy focuses on the location of the information, when judging the severity of a privacy breach.
[34] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 129.
[35] Idem p. 130.
[36] Article 12 Dutch Constitution; Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 130.

In chapter five the implications of the changing legal landscape on the traditional privacy framework are discussed and a more contemporary conceptualization of privacy is set forth. However, first, the discussion of existing legal mechanisms will be continued and whether these mechanisms apply to OSINT in criminal investigations.

2. Privacy and European Fundamental Rights

The ECHR and the EU Charter and their respective courts, the ECtHR and CJEU, are the core of fundamental rights law in the EU.[37] Both the ECHR and the EU Charter contain the right to private life[38] and the right to protection of personal data.[39] Other relevant legislation for the discussion on traditional criminal investigations and OSINT includes the Law Enforcement Directive concerning the right to data protection and the Council of Europe's Cybercrime Convention (CCC) on cross-border OSINT. These various legal instruments will be discussed in the next few paragraphs, as these will provide us with an overview of OSINT regulations in governmental investigations. This existing framework will aid our research in possible privacy violations by civilian criminal investigators and provide us with possible ideas for regulation of civilian criminal investigations.

2.1. The ECHR and the ECtHR

Article 8 of the ECHR codifies the right to a private and family life, home and correspondence, including an implicit right to personal data protection.[40] The right to a private life is a derogable right, allowing for interference if it is in accordance with the law and if the inference is necessary in a democratic society to pursue one or more of the legitimate aims named in article 8(2) ECHR.

Member states have a margin of appreciation, to determine whether their measures are compatible with the right to a private life, albeit limited since the ECtHR has the final say on whether the measures are in breach of article 8 ECHR.[41] According to ECtHR jurisprudence, a two-stage test applies to assess whether a violation of article 8 ECHR has taken place.[42]

[37] Eleanor Spaventa, 'Fundamental Rights in the European Union' in Catherine Barnard and Steve Peers (eds), *European Union Law* (Oxford university press 2014), 226.
[38] Article 7 EU Charter and article 8 ECHR.
[39] The right to data protection is codified in article 8 EU Charter and implicit in article 8 ECHR.
[40] Emmanuel Salami, 'The Impact of Directive (EU) 2016/680 on the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and on the Free Movement of Such Data on the Existing Privacy Regime' (2017) SSRN <http://dx.doi.org/10.2139/ssrn.29124491> accessed 4 August 2019 1,1.
[41] Ursula Kilkelly, 'The Right to Respect for Private and Family Life. A Guide to the Implementation of Article 8 of the European Convention on Human Rights' (2003) 1 Council of Europe Human Rights Handbooks1, 6 – 7.
[42] Idem p. 8.

Firstly, an assessment will be made whether it concerns a right to private or family life, as laid down in article 8(1) ECHR. The applicant will argue which right he or she is seeking to protect under article 8 ECHR.[43] If it concerns a right protected by article 8(1) ECHR, the second stage consists of an evaluation of whether the interference with the right can be justified based on article 8(2) ECHR. This entails judging whether an infringement of the right to a private life has taken place, whether the interference was in accordance with the law, pursuing a legitimate aim that was necessary in a democratic society.[44]

'In accordance to law' requires the interference to have a legal basis in an accessible and foreseeable national law.[45] The law has to be sufficiently clear, precise and needs to protect against arbitrariness.[46] Moreover, a 'legitimate aim' is necessary to justify an interference with the right to privacy.[47] The state will have to argue which legitimate aim it is pursuing by the interference, although the aims are very broad and therefore interferences usually fall within the scope of the aim.[48]

Lastly, 'necessary in a democratic society' refers to a proportionality test and requires the interference to be appropriate and proportional to fulfil a pressing social need.[49] The aim of the interference, the factual situation in which the interference takes place, and safeguards like the restriction of data collection and time limits, are included in the proportionality test.[50]

The requirements aid in answering the question of whether there was a reasonable expectation of privacy. The latter is vital in ECtHR's privacy jurisprudence to establish whether a privacy breach has occurred.[51] Any specific remarks on the use of OSINT in the ECHR or the ECtHR case law cannot be found.

---

[43] Idem p. 10.
[44] Article 8(2) ECHR; Ursula Kilkelly, 'The Right to Respect for Private and Family Life. A Guide to the Implementation of Article 8 of the European Convention on Human Rights' (2003) 1 Council of Europe Human Rights Handbooks 1, 9.
[45] Nick Taylor, 'State Surveillance and The Right to Privacy' (2002) 1 *Surveillance & Society* 66, 68.
[46] Ursula Kilkelly, 'The Right to Respect for Private and Family Life. A Guide to the Implementation of Article 8 of the European Convention on Human Rights' (2003) 1 Council of Europe Human Rights Handbooks 1, 25.
[47] The justified intervention exceptions can be found in article 8(2) ECHR.
[48] Ursula Kilkelly, 'The Right to Respect for Private and Family Life. A Guide to the Implementation of Article 8 of the European Convention on Human Rights' (2003) 1 Council of Europe Human Rights Handbooks 1, 30.
[49] Nick Taylor, 'State Surveillance and The Right to Privacy' (2002) 1 *Surveillance & Society* 66, 68; Ursula Kilkelly, 'The Right to Respect for Private and Family Life. A Guide to the Implementation of Article 8 of the European Convention on Human Rights' (2003) 1 Council of Europe Human Rights Handbooks 1, 31.
[50] *Silver v. United Kingdom* App nos 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 and 7136/75 (ECtHR, 25 March 1983), ECLI:CE:ECHR:1983:0325JUD000594772 in: Nick Taylor, 'State Surveillance and The Right To Privacy' (2002) 1 Surveillance & Society 66, 68; Bert-Jaap Koops, 'Police Investigations in Internet Open Sources: Procedural-Law Issues' (2013) 29 Computer Law & Security Review 654, 656.
[51] Mark Feenstra, 'Opsporingsmiddelen in de Ontwikkeling: Openbronnen-Onderzoek als de Nieuwe 'Tap' (2018) 97 PROCES 367, 370.

2.2. The EU Charter and the CJEU

In comparison, the EU Charter encompasses the right to private and family life[52] and an explicit article on the right to personal data protection.[53] The EU's fundamental rights law is gaining in importance, especially in criminal law.[54] Fundamental rights law can limit Union actions and member state actions, when applying EU law, if fundamental rights are compromised or breached.[55]

In recent years there have been two landmark cases of the CJEU on privacy. The first landmark case is the *Google Spain SL v. Costeja* case, which introduced the right to be forgotten.[56] If information is 'inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased'.[57] Critics have argued that this decision can create censorship, as information on a person can no longer be found after removal.[58] Others have viewed it as a much needed addition to data protection.[59]

The second case is the *Schrems v Data Protection Commissioner* case, which became famous as it stopped the Safe Harbor agreement with the United States. The Safe Harbor agreement regulated the transferring of personal data from EU to the US.[60] It argued that review of claims of civilians on inadequate levels of data protection in third countries, that receive flows of personal data from the EU, should always be possible regardless whether it concerns an interference, sensitive personal information or adverse consequences. It is the interference itself that amounts to a breach of the right to private life.[61] The protection of personal data was later expanded in the GDPR.[62]

OSINT in criminal investigations is not specifically addressed in EU law and is therefore treated like any other investigative technique. EU law applies to assess whether or not an interference of the right to data protection occurred, based on the extent to which systematic collection and storing of files took place.[63] Systematic searches are considered an interference with the right to

[52] Article 7 EU Charter.
[53] Article 8 EU Charter.
[54] Eleanor Spaventa, 'Fundamental Rights in the European Union' in Catherine Barnard and Steve Peers (eds), *European Union Law* (Oxford university press 2014), 227.
[55] Idem p. 230 and 232.
[56] Case C-131/12, *Google Spain SL v. Costeja* CJEU 2014 ECR. 317, ECLI:EU:C:2014:317, paras 91-99.
[57] Idem para. 94.
[58] Edward Lee, 'The Right to Be Forgotten v. Free Speech' (2015) 12 I/S: A Journal of Law and Policy for the Information Society 85, 88.
[59] Idem p. 91.
[60] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* CJEU 2015, ECLI:EU:C:2015:650, paras 96– 98 and 103 – 106.
[61] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* CJEU 2015, ECLI:EU:C:2015:650, para 87; Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) Geo. L. J. 115, 127 and 128.
[62] This will be discussed in chapter II, paragraph 3 on the GDPR.
[63] Bert-Jaap Koops, 'Police Investigations in Internet Open Sources: Procedural-Law Issues' (2013) 29 Computer Law & Security Review 654, 656.

data protection and require a legal basis, regardless of the distinction between open-source information and other types of data.

This means that manual or non-systematic searches by public officials that do not include storing of information, do not amount to an interference with a person's right to data protection.[64]

3. Sub-conclusion

To summarize, the current European legal framework on criminal investigations lacks any specific regulations on the use of OSINT. OSINT is not specifically addressed the ECHR, ECtHR case law or EU law and is therefore treated like any investigative technique.

Governmental criminal investigations, with the use of OSINT, would pass the proportionality test of the necessity-requirement under article 8(2) ECHR, but the current legal status of open-source information and the use of OSINT in police investigations remains unclear. This lacuna in the law should be filled to consolidate legal certainty and prevent arbitrariness in police work. This is all the more important in light of the changing landscape of criminal investigations, which will be discussed in the next chapter.

II. The Legal Basis of Civilian Criminal Investigations

This paper now turns to the legality of civilian criminal investigations, to evaluate whether civilians' criminal investigations using OSINT impact the privacy of their suspects. In this chapter, the recent changes in the landscape of criminal investigations and justice administration are discussed to establish an awareness of the current state of affairs and explain the increased occurrence of civilian criminal investigations and vigilante justice. Subsequently, the GDPR and self-regulatory measures by private actors will be discussed in light of the case study of Shahin Gheiybe, which completes the overview of the current regulations on OSINT.

1. The Changing Landscape of Criminal Investigations

Technological adaptations have moved large parts of our communication to the online sphere. The digitalization of society causes datafication[65] of our online behaviour, as all our interactions and decisions are monitored and transformed into data.[66] When one scrolls through their

[64] Ibid.

[65] Datafication is defined in this paper as 'the transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis' in accordance with Viktor Mayer-Schoenberger and Kenneth Cukier, 'Big Data. A Revolution That Will Transform How We Live, Work and Think' (2014) 179 Oxford University Press in: José van Dijck, 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology' (2014) 12 Surveillance & Society 197, 198.

[66] Bert-Jaap Koops, 'Privacyconcepten voor in de 21e Eeuw' (2019) 68 Ars Aequi 1, 6 (this paper used the forthcoming version of this article sent by the author in April 2019).

Facebook feed, a software tracks not only what one posts but *inter alia* what one looks at, for how long and whether one comments on it. Combining these data allows for a detailed depiction of an individual as part of a group, useful for targeted profiling.

The traditional conceptualization of privacy is not adapted to this, as it often focuses on the individual, whereas targeted profiling concerns the privacy of an individual within a group.[67]

Moreover, through occurrences like the Internet of Things and 'smart' furniture, the physical world is intertwining with the digital world.[68] People can no longer expect to be most private in their homes, as digitalization and datafication have made technology become an ingrained part of our daily private life.[69]

For example, people bring their public and private life everywhere with them on their mobile phones. Sensitive information can be derived from these phones, by means of data mining and data analytics.[70] This is blurring the lines between the public and the private sphere and making it increasingly difficult to estimate the severity of a privacy breach beforehand. These blurring lines between the privacy of one's home[71] and one's communication[72] are challenging the classical investigative framework and need to be addressed.[73]

2. The Changing Landscape of Justice Administration

In today's society, most of the digital infrastructure and knowledge is in the hands of private parties. Many of these private parties are tech companies, but they can also include citizens, who are able to contribute both substantively to digital criminal investigations.[74] Digilantes[75] are growing in importance since the internet has created the possibility for the public to get involved.[76] The Dutch police have expressed their aim to include civilians more structurally in criminal investigations, harnessing the potential that civilian criminal investigations can yield.[77]

---

[67] İbid.
[68] Ibid.
[69] Bert-Jaap Koops, 'Privacyconcepten voor in de 21e eeuw' (2019) 68 Ars Aequi 1, 1 (this paper used the forthcoming version of this article sent by the author in April 2019).
[70] Commissie Modernisering Opsporingsonderzoek in het Digitale Tijdperk, *Regulering van Opsporingsbevoegdheden in een Digitale Omgeving* (s.l. 2018), 36.
[71] Art. 12 Dutch Constitution and article 8(1) ECHR.
[72] Art. 13 Dutch Constitution and article 8(1) ECHR.
[73] Commissie Modernisering Opsporingsonderzoek in het Digitale Tijdperk, *Regulering van Opsporingsbevoegdheden in een Digitale Omgeving* (s.l. 2018), 35.
[74] Commissie Modernisering Opsporingsonderzoek in het Digitale Tijdperk, *Regulering van Opsporingsbevoegdheden in een Digitale Omgeving* (s.l. 2018), 20.
[75] As mentioned in the introduction, the terms digilantes and civilian criminal investigators will be used interchangeably throughout this paper (see footnote 18).
[76] Johnny Nhan & Laura Huey & Ryan Broll, 'Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings' (2017) 57 *British Journal of Criminology* 341, 341 and 342.
[77] Harm Graat, 'Politie wil hulp van 'burgerrechercheurs' bij opsporing' *De Gelderlander* (25 August 2018) <www.gelderlander.nl/arnhem/politie-wil-hulp-van-burgerrechercheurs-bij-opsporing-br-br~a843f0f6/> accessed 28 July 2019.

For example, on the 1 June 2019, the Dutch police and the office of the public prosecutor launched a pilot app to help victims of theft track down the thief. The app will serve as a two-month trial in various parts of the Netherlands and aims to serve as a new platform stimulating collaboration between civilians and the police, aiding criminal prosecution.[78] It will give victims of theft the chance to start their own investigation.

The app allows civilians to perform all types of tasks, including interrogating witnesses, checking whether camera footage of the incident is available, uploading photos or videos as proof of the crime, conducting research in the neighbourhood and, importantly, conducting online research. The police argue it would only concern actions that civilians are allowed to undertake without legal permission.[79] The app will guide civilians through their investigation in accordance with the law, which could render evidence collected by civilians admissible in the courtroom.[80]

Another initiative trying to benefit from public action is the 'eyeWitness to Atrocities'-app, launched by the International Bar Association (IBA) and various human rights organisations.[81] This application aims to record information showing serious human rights violations. It checks metadata to verify the reliability of the evidence and sends it to a secure server for later use in court, while maintaining the anonymity of the users of the app.[82]

The increasing involvement of civilians in criminal investigations shows a change in the role of the police in society, from professional and independent, towards a more community focused security mechanism within a democratic participatory society.[83]

Increased involvement of civilians in criminal investigations could be a threat to fair and just criminal investigations, as civilian criminal investigations are not explicitly regulated in Dutch law. In contrast, one could argue that not having any safeguards against civilian criminal investigations makes sense as civilians might be able to use OSINT, but they cannot start a trial nor administer justice due to the public prosecutor's monopoly on tracing crimes, prosecuting crimes and monitoring the execution of the court's verdicts.[84] Civilians might be increasingly aiding criminal

[78] Politie, 'Politie en OM Lanceren App voor Burgeronderzoek' *Politie.nl* (27 May 2019) <www.politie.nl/nieuws/2019/mei/27/00-politie-en-om-lanceren-app-voor-burgeronderzoek.html> accessed 7 June 2019.
[79] NOS, 'Politie en OM Gaan Speurende Burger Met App Begeleiden' *NOS.nl* (27 May 2019) <https://nos.nl/artikel/2286469-politie-en-om-gaan-speurende-burger-met-app-begeleiden.html> accessed 27 May 2019; Politie, 'Politie en OM Lanceren App voor Burgeronderzoek' *Politie.nl* (27 May 2019) <www.politie.nl/nieuws/2019/mei/27/00-politie-en-om-lanceren-app-voor-burgeronderzoek.html> accessed 7 June 2019.
[80] NOS, 'Politie en OM Gaan Speurende Burger Met App Begeleiden' *NOS.nl* (27 May 2019) <https://nos.nl/artikel/2286469-politie-en-om-gaan-speurende-burger-met-app-begeleiden.html> accessed 27 May 2019.
[81] RELX, 'Eyewitness to Atrocities App Launched' *RELX.com* (08 June 2015) <https://www.relx.com/media/press-releases/year-2015/08-06-2015> accessed 27 October 2019.
[82] 'EyeWitness Project' at: <www.eyewitnessproject.org/> accessed 29 July 2019.
[83] Gary T Marx, 'The Public as a Partner? Technology Can Make Us Auxiliaries as well as Vigilantes' (2013) 11 *IEEE Security & Privacy* 56, 57.
[84] Article 124 of the Dutch law on the Judicial Organization ('Wet op de Rechtelijke Organisatie' (RO)).

investigations, but in the end the public prosecutor will decide what crimes will be prosecuted and which will not.

However, this view assumes that civilians cannot seek and administer their own kind of justice. A new type of justice has arisen with the growing importance of civilian investigators driven by private actors – also referred to as online vigilante justice – potentially due to the lack of regulations on digilantes.

For example, groups of civilians hunt down paedophiles online to submit them to a type of vigilante justice administration. These digilantes pretend they are under-age and schedule a meeting with the paedophile, where he or she gets beaten or humiliated, which is filmed by the digilantes and published publicly on social media to online shame the paedophile.[85] The goal is to create justice and awareness through the online shaming, while pointing out the lack of prosecution of paedophiles to law enforcement. Simultaneously, their vigilante justice offers some dubious entertainment to the viewers.

Online vigilante justice, administered by civilians or civilian organizations, can take shape in online bullying, online shaming[86] and doxxing[87], without being bound to rules.[88] Doxxing is a common example of online vigilante justice and can be used to supplement other types of online vigilante justice like online shaming. It is particularly difficult to prevent, considering that doxxing consists of putting together various pieces of seemingly innocent public information from different internet sources, to paint a bigger picture of one's life that goes beyond the individual pieces of information.[89] Doxxing provides information and entertainment to the public, but the publicity can also create notoriety or unwanted attention, which can lead to condemnation.

In a way, Bellingcat's vigilante justice is doxxing: they publish personal data of subjects of their investigations, retrieved from various public sources on their website. In the case of Shahin Gheiybe this includes information on his most recent location and his private pictures and videos.[90] Shahin Gheiybe is a convicted criminal, but especially when subjects of digilante justice

[85] Lennon Y.C. Chang, Lena Y. Zhong and Peter N. Grabosky, 'Citizen Co-Production of Cyber Security: Self-Help, Vigilantes and Cybercrime' (2016) 12 Regulation & Governance 101, 106.

[86] In this paper, online shaming is defined as 'spreading public information online', in accordance with: Mathias Klang and Umass Boston, 'On The Internet Nobody Can See Your Cape: The Ethics of Online Vigilantism' (2015) AoIR 1, 1.

[87] In this paper, doxxing is defined as the 'use of the internet to search for and publish identifying information about a particular individual, typically with malicious intent' (see footnote 19).

[88] Mathias Klang and Umass Boston, 'On the Internet Nobody Can See Your Cape: the Ethics of Online Vigilantism' (2015) AoIR 1, 1.

[89] For example, if one's postal code is publicly available online, and one's name, profession, age or phone number are also publicly available in separate online sources, the privacy violation would be more substantial if all this information would be doxxed together in the same place than if these facts would be doxxed separately, without connecting the various facts. A more complete image of a person's private life is revealed when you publish a person's name, profession, age, phone number and address all together in one place.

[90] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 28 March 2019.

have not yet been on trial in the judicial system, the image portrayed online and in media can have a substantial influence, even on decision making in various layers of the civil litigation system.[91] The need for regulation of vigilante justice is evident.

3. The General Data Protection Regulation: the GDPR

The need for regulatory measures to protect suspects of civilian criminal investigations and victims of vigilante justice has become clear. One of the available data protection mechanism to victims of digilantes using OSINT is the regulation (EU) 2016/679, also called the GDPR. The question is if the GPDR provides sufficient legal protection against OSINT.[92]

Open-source information consists of data and therefore the GDPR could be useful to protect civilians' data, without suggesting that privacy and data protection are the same.[93] Enforceable since the 25 May 2018, the GDPR is the most important data protection regulation of the EU, in part due to the high monetary sanctions.[94] It applies to the processing of personal data, either partly or fully automated, or as part of a filing system and has extraterritorial applicability, as the companies processing the data of the data subjects do not have to be located in the EU.[95]

According to article 13 and 14 of the GDPR, Bellingcat should provide the data subject with information about the data in question, including naming the source of the data and whether it came from a publicly accessible source,[96] unless the data subject already has the information[97] or if it is necessary and proportionate in a democratic society to not disclose the information to secure criminal investigations.[98] The latter seems relevant for digilantes and might serve as an exemption ground for digilantes to not have to inform the data subject on their use of his or her data.

Moreover, a digilante could otherwise also argue that notice has already been given to the data subject when it concerns open-source information from social media, as people permit further processing of personal data by agreeing to terms and conditions when using social media services. These terms and conditions often include the notion that further processing of personal data can occur for a purpose other than that for which the personal data were obtained, therefore notifying

[91] Jennifer K. Robbennolt and Christina A. Studebaker, 'News Media Reporting on Civil Litigation and Its Influence on Civil Justice Decision Making.' (2003) 27 Law and Human Behaviour, 5 – 27.
[92] As mentioned in chapter I, even though data protection and privacy protection are not considered being the same in this paper, this paper focuses on the possible ways in which civilians' rights are protected concerning OSINT in civilian criminal investigations. Therefore, exploring data protection mechanisms, like the Police Directive and the GDPR, are useful to gain an overview on the (lack of) legal protection and regulation of OSINT.
[93] The further in-depth discussion on the (lack of) overlap between data protection and privacy protection exceeds the scope of this paper (see footnote 99).
[94] Article 83 and 99 GDPR.
[95] Article 2 and 3 GDPR.
[96] Article 14(2)(f) GDPR.
[97] Article 13(4) and 14(5)(a) GDPR.
[98] Article 41(d) of the Dutch implementing law integrating *inter alia* article 23 GDPR, 'Uitvoeringswet Algemene verordening gegevensbescherming' (UAVG).

data subjects.[99] Apart from this, the use of OSINT, specifically in the context of civilian criminal investigations, is not regulated by the GDPR.

It should again be stressed that privacy and data protection problems are not the same. Finding a solution to a problem of data protection does not necessarily provide for a complete solution to privacy problems as well.[100] For example, if civilian investigators find a publicly available record of one's correspondence, which includes a nude photo, they might unlawfully process personal data if they save, analyse or use the personal photo. However, if they simply view the picture and describe it in detail to others, no data breach occurs but one's privacy can still be compromised.

Moreover, criticism has been expressed that the GDPR covers so many topics that it is at risk of becoming a focus point for compliance on paper, instead of implementing true privacy protection.[101] All in all, the GDPR does not seem to provide a comprehensive answer to privacy concerns caused by OSINT.

4. Self-regulation by Private Actors

Another possible protection method is self-regulation of privacy matters. Next to governmental initiatives there are also civilian investigators that adhere themselves to codes of conducts, engaging in a type of self-regulation.

Bellingcat uses the IMPRESS Standards Code for journalists that 'aims to protect the public from invasive journalistic practices and unethical news reporting'.[102] The Standards Code includes rules on privacy, the use of sources, transparency, accuracy and more. Article 7 of the Standards Code states that 'publishers must respect people's reasonable expectation of privacy', which can be judged on various aspects including their public profile,[103] and whether a person has voluntarily courted publicity on an aspect of their private life.[104] Its guidance remarks on article 7 provides for an in-depth description of the clauses and their application. It states:

> 'Information that is already in the public domain will not generally give rise to a reasonable expectation of privacy. However, private photographs or videos that capture intimate moments or images may still attract a reasonable expectation of privacy even though they have been previously publicised. This is because of the special quality of images and photographs. This does not mean that a publisher can deliberately reveal hitherto private information to argue that the

[99] Facebook, 'Data Policy' <https://www.facebook.com/about/privacy/update> accessed 1 November 2019.
[100] Bert-Jaap Koops, 'Privacyconcepten voor in de 21e Eeuw' (2019) 68 Ars Aequi 1, 7 (this paper used the forthcoming version of this article sent by the author in April 2019).
[101] Ibid.
[102] Bellingcat, 'Making a Complaint' <www.bellingcat.com/contact/> accessed 30 July 2019; IMPRESS, 'Standards Code' <www.impress.press/standards/> accessed 29 July 2019.
[103] IMPRESS, 'Standards Code', article 7(d).
[104] IMPRESS, 'Standards Code' article 7(e).

> information is now in the public domain. Information may still be regarded as being subject to a reasonable expectation of privacy where some people know of it, provided it is not generally known'.[105]

What a reasonable expectation of privacy is, will depend on the circumstances of a specific case and the many aspects named in article 7. IMPRESS ends its guidance note on article 7 stating that the clause is not breached if public interest outweighs privacy harm. Its guidance note seems in line to existing EU case law on privacy.[106] The benefit of this type of regulation is that companies are portraying their commitment to privacy protection and could therefore be likely to stick to it. Moreover, by creating their own regulations, companies can base it on their own experiences and come up with an effective privacy regulation.

However, simultaneously there is a risk that companies invent a privacy regulation that looks good on paper, but in practice provides little privacy protection. Moreover, the problem with non-governmental compliance schemes is that non-compliance with IMPRESS' Standards Code will have no legal consequences, as it is a voluntary regulation method. IMPRESS' Standards Code is recognized as an independent press regulator,[107] but becoming a member of its Standards Code is not mandatory.

5. Sub-conclusion

Digitalization and datafication of society, the blurring lines between public and private life, the increasing role of civilian investigators and the emergence of online vigilante justice are changing criminal investigations as we know them. This creates possibilities for different ways of investigating and justice administrating.

However, it is questionable whether vigilante justice truly administers justice or disguises behind the term, as no legal safeguards apply. Its use should, therefore, be restricted. Moreover, this chapter has shown that presently, no comprehensive, legally binding regulations on the use of OSINT in civilian criminal investigations exist. The GDPR does not address the use of OSINT specifically and self-regulation by private actors, like through the voluntary IMPRESS Standards Code for journalists, lack legal implications.

Referring this back to the research question, the lack of regulations on OSINT in traditional and civilian criminal investigations is problematic as it leaves open the question in which situations its use amounts to privacy breaches of suspects. Moreover, if a privacy breach would occur, the victims are not protected.

---

[105] IMPRESS, 'Standards Code' Guidance on article 7. The original text had a spelling mistake in it, which was removed in this quote.

[106] See chapter III for further information on the EU Court of Justice case law on privacy.

[107] IMPRESS, 'FAQ' point 11 at: <www.impress.press/about-us/faq.html#relationship-between-impress-government> accessed 30 July 2019.

Another possibility to assess whether civilians' criminal investigations using OSINT impact the privacy of their suspects is through the horizontal direct effect of EU Fundamental rights. Therefore, the next chapter will look at the horizontal working of the EU fundamental rights in light of the case study on Shahin Gheiybe.

III. The Horizontal Direct Effect of EU Fundamental Rights

The horizontal working of EU fundamental rights could provide for an answer whether civilians' criminal investigations using OSINT impact the privacy of their suspects, now the previous chapters have discussed the lack of specific regulations on the use of OSINT.

In this chapter, the case study of Shahin Gheiybe will be used to assess whether a privacy breach occurred and whether this outweighed Bellingcat's right to freedom of expression and information. Firstly, the horizontal direct effect of EU fundamental rights will be explained. Secondly, all relevant facts of the case study of Shahin Gheiybe will be discussed before evaluating Bellingcat's right to freedom of expression and information on the one hand and Shahin Gheiybe's right to a private life on the other hand.

1. Horizontal Direct Effect of EU Fundamental Rights Law

The EU Charter itself does not state explicitly that private parties can invoke its articles in horizontal relations but the EU Court of Justice has stated in case *Association de Médiation Sociale* that this is possible for articles of the EU Charter.[108] The previously discussed *Google Spain* case is an example of the horizontal effect of the EU Charter.[109] This case clarified that concrete legal obligations for private parties can be created based on fundamental rights protection in horizontal relations.[110]

To assess whether the EU Charter has direct horizontal effect in a specific case, a few steps have to be taken. First, the court will assess whether the EU Charter applies in a specific case.[111] Secondly, the court will examine whether it is a right or a legal principle that is called upon, with rights having stronger legal protection than principles.[112] Article 52(1) of the EU Charter states that limiting fundamental rights requires restrictions provided for by law that respect the essence

[108] Case C-176/12, *Association de médiation sociale*, CJEU 2014 ECLI:EU:C:2014:2, paras 41 – 43; J.M. Emaus, Rechten, beginselen en horizontale directe werking van de grondrechten uit het EU-handvest, 2015, NTBR 2015/10, 6 and 9.
[109] Case C-131/12, *Google Spain SL v. Costeja* CJEU 2014 ECR. 317, ECLI:EU:C:2014:317.
[110] Article 52(5) EU Charter; Jessy Emaus, 'Rechten, Beginselen en Horizontale Directe Werking van de Grondrechten uit het EU-Handvest' (2015) 10 NTBR 67, 75.
[111] Article 51 EU Charter; Jessy Emaus, 'Rechten, Beginselen en Horizontale Directe Werking van de Grondrechten uit het EU-Handvest' (2015) 10 NTBR 67, 75.
[112] Article 52(5) EU Charter; Jessy Emaus, 'Rechten, Beginselen en Horizontale Directe Werking van de Grondrechten uit het EU-Handvest' (2015) 10 NTBR 67, 75.

of those rights and freedoms. The evaluation of fundamental rights in horizontal relations consists of a proportionality analysis, balancing the various fundamental rights.[113]

Member states of the ECHR can also have a positive obligation to ensure fundamental rights in horizontal relations, which can include the adoption of protective measures. The doctrine of positive obligations was once developed in relation to article 8 ECHR to ensure effective protection under the ECHR.[114] This obligation is derived from the negative obligations of states to abstain from interference with fundamental rights. A responsibility to guarantee fundamental rights can therefore be evoked even if it concerns relations of individuals between themselves.[115]

The famous *Von Hannover* cases[116] are important in the development of ECtHR jurisprudence on the positive obligation of a state, weighing the right to privacy against freedom of speech. Although the cases were about the publication of pictures of public figures by the press, they gave rise to a general framework regarding the balancing between the right to privacy and the right to freedom of expression.[117] The essence of each right always has to be protected as fundamental rights should be treated with equal respect.[118] Therefore, a fair balance has to be found between the opposing interests.[119]

2. The Case Study of Shahin Gheiybe

On the basis of the ECtHR's *Von Hannover* jurisprudence, a conclusion can be reached on the present case study of Shahin Gheiybe. First, all relevant facts of Bellingcat's research into Shahin Gheiybe have to be stated.

Bellingcat used Shahin Gheiybe's Instagram content for OSINT to find his current physical location. His Instagram account contained over 170 pictures and videos at the time and was 'public' until somewhere in March 2019, when Shahin Gheiybe landed on the Dutch list of most wanted criminals. After that, he made his Instagram profile "private".[120] After Shahin Gheiybe's

[113] As codified in article 52(1) EU Charter.

[114] *Marckx v. Belgium* App no 6833/74 (ECtHR 13 June 1979), ECLI: CE: ECHR:1979:0613JUD000683374, para 31.

[115] ECtHR, 'Guide on Article 8 of the European Convention on Human Rights - Right to Respect for Private and Family Life (Council of Europe 30 April 2019) <www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 2 August 2019 1,8.

[116] *Von Hannover v. Germany* (No. 1) App no 59320/00 (ECtHR, 24 June 2004), ECLI: CE: ECHR:2004:0624JUD005932000; *Von Hannover v. Germany* (No. 2) App nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), ECLI: CE: ECHR:2012:0207JUD004066008.

[117] 'Global Freedom of Speech Columbia University' at: <https://globalfreedomofexpression.columbia.edu/cases/von-hannover-v-germany-no-2/> accessed 19 June 2019.

[118] *Von Hannover v. Germany* (No. 2) App nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), ECLI: CE: ECHR:2012:0207JUD004066008, para 106.

[119] *Von Hannover v. Germany* (No. 2) App nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), ECLI: CE: ECHR:2012:0207JUD004066008, para 99; *White v. Sweden* App no 42435/02 (ECtHR 19 September 2006), ECLI: CE: ECHR:2006:0919JUD004243502, para 20.

[120] An Instagram account is "public" when everyone that searches for your account can see you all your posts: pictures, videos and "stories" (which are small snippets of videos and photos that can be seen for

Instagram was made private, Bellingcat sent a follow-request. Shahin Gheiybe accepted the follow-request, giving Bellingcat access again to his personal content.[121] Especially one video of the 9 March 2019, depicting a house and Shahin Gheiybe talking about the ongoing investigations, was used by Bellingcat to find his last known location.[122]

Although it is not mentioned in Bellingcat's article, Bellingcat clarified through email that half of their OSINT research took place while Shahin Gheiybe's Instagram was public and half of it when it was private. It remains unsure whether the downloading of Shahin Gheiybe Instagram content took place before he put his Instagram account on private.[123]

Bellingcat downloaded part of Shahin Gheiybe's photos and video's through a Google Chrome plug-in called 'Downloader for Instagram', that downloads all materials in high resolution, including Instagram stories. Subsequently, Bellingcat included some of these pictures and videos in its article and uploaded some photos and videos on other websites and linked to those stable websites in their article on Shahin Gheiybe. This makes it possible for Bellingcat's readers to access the linked materials indefinitely, even if Shahin Gheiybe removes the content from his Instagram account.

The question arises whether or not Shahin Gheiybe's right to a private life was infringed and if so, how it balances against Bellingcat's right to freedom of expression and information.[124] In the next paragraphs, both sides of the argument will be considered.

3. Bellingcat's Right to Freedom of Expression and Information

Bellingcat could argue that Shahin Gheiybe's Instagram was publicly available at the time of their research, therefore making it a suitable open source for OSINT. No hacking took place nor were security measures circumvented. Since using publicly available data is a common occurrence on the internet and not illegal for civilians, this would only constitute a minor breach of privacy, if any.

---

24 hours and then disappear). If your Instagram account is public, anyone can see the content of your profile and 'follow' your account by just clicking on the follow-button. If you put your Instagram account on 'private', people that want to see your post will first have to send a follow-request to you. Only afterwards can they see the content of your profile. As the owner of a private Instagram account, you can accept or decline follow-requests and only your followers will be able to see your pictures, videos and stories. However, comments you put underneath other people's Instagram posts can still be seen by other Instagram users, especially if those accounts are public. If someone's Instagram account was first public and then made private, you keep all the followers you acquired when the account was public. If someone wants a follower to not see their posts anymore, you have to individually remove the follower(s).

[121] Email from Bellingcat contributor and author of Bellingcat's article on Shahin Gheiybe, Henk van Ess to author (23 July 2019).

[122] See chapter IV paragraph 1 on the reliability of OSINT, where this specific video will be discussed in more detail.

[123] Email from Bellingcat contributor and author of Bellingcat's article on Shahin Gheiybe, Henk van Ess to author (23 July 2019).

[124] Article 7 and 11 EU Charter.

For the other half of Bellingcat's research, when Shahin Gheiybe's Instagram was on private, Bellingcat clarified that Shahin Gheiybe had a 'rather welcoming door policy',[125] which meant that Shahin Gheiybe accepted Henk van Ess' Instagram follow request right away.[126] Shahin himself accepted the following request of Bellingcat contributor Henk van Ess, therefore clearly granting access to his profile and its content without violating Shahin Gheiybe's privacy.

Moreover, the ECtHR recognizes the importance of the right to freedom of expression, by stating freedom of expression is essential in a democratic society and necessary for an individual's self-fulfilment, even if ideas or information may offend, shock or disturb.[127] The press is a public watchdog protecting freedom of speech and has a duty to report on all matters of public interest. Bellingcat can be considered a public watchdog, being a civilian organization conducting OSINT and publishing on matters of public interest for the whole of society to read. Therefore, even if Bellingcat violated Shahin Gheiybe's privacy, this was allowed as it was done as part of Bellingcat's task of being a public watchdog.

Furthermore, the ECtHR has stated that it matters whether the information could amount to a factual debate or simply satisfy public curiosity, with the latter generally carrying less importance.[128] Bellingcat's findings amount to a factual debate and allow for fact-checking due to its transparency. Besides, Shahin Gheiybe's privacy seems to not be compromised in Bellingcat's research as his permission was asked once his Instagram account was no longer publicly available and no law was breached during Bellingcat's investigation. OSINT was used, which does not have a substantial privacy implication, if any, as it concerns public information.

It can, therefore, be argued that there is in fact no privacy infringement and Bellingcat simply used its freedom of expression and information to investigate a convicted criminal.

4. Shahin Gheiybe's Right to Private Life

Alternatively, Shahin Gheiybe could argue that his privacy was in fact compromised, contrary to the arguments given by Bellingcat. Turning to the scope of the right to privacy, the ECtHR stated in the *Von Hannover* cases that:

> 'the concept of private life extends to aspects relating to personal identity, such as a

[125] This means Shahin Gheiybe easily accepts people's follow-request for his Instagram account and therefore does not keep it very private, even though it is on private-mode. This is *inter alia* reflected in the fact that he currently has over 5.700 followers, making the account not very private, even though it is on private mode. See: Instagram, account 'shahin.mzr' <www.instagram.com/shahin.mzr/>, accessed 24 July 2019.

[126] Email from Bellingcat contributor and author of Bellingcat's article on Shahin Gheiybe, Henk van Ess to author (23 July 2019).

[127] *Von Hannover v. Germany* (No. 2) App nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), ECLI: CE: ECHR:2012:0207JUD004066008, para 101.

[128] *Von Hannover v. Germany* (No. 2) App nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), ECLI: CE: ECHR:2012:0207JUD004066008, para 114.

> person's name, photo, or physical and moral integrity and ensures the development, without outside interference, of the personality of each individual in his relations with other human beings. A zone of interaction of a person with others, even in a public context, may fall within the scope of private life'.[129]

This shows a broad scope of the right to privacy. Shahin Gheiybe could argue that the *Von Hannover* cases suggest that Bellingcat's use of his personal information on Instagram –which includes photos and videos – amounts to an infringement of his right to privacy, as even in a zone of interactions between people in a public context like Instagram, a person can have a realistic expectation of a private life.

Shahin Gheiybe accepted Bellingcat's Instagram follow-request, allowing Bellingcat to view the content of his profile. However, this is not the same as giving Bellingcat permission to download and doxx his personal information by means of a Chrome plug-in. It seems unreasonable to expect Shahin Gheiybe's permission to also cover the latter, especially if considered that Shahin Gheiybe otherwise collaborated in an investigation against himself without knowing it, which goes against the criminal law prohibition of a suspect unwittingly cooperating in his own conviction.[130]

Furthermore, different standards apply when the publication of one's private life concerns a person acting in a public context as a public or political figure or as a private person. According to the ECtHR, a private individual can request more protection of his or her right to privacy than a political or public figure can.[131] Shahin Gheiybe cannot be said to be a public figure as he is not famous. He should, therefore, be able to expect a reasonably high protection of his right to a private life.

Moreover, there would have been other ways for Bellingcat to use their right to freedom of expression and information, that would have infringed less on Shahin Gheiybe's right to privacy. For example, they could have accessed and analysed his Instagram account, without copying or doxxing its content on their own website(s).

Therefore, it can be argued that the infringements on Shahin Gheiybe's privacy are disproportional in relation to Bellingcat's right to freedom of expression and information.

5. Balancing the Fundamental Rights

[129] *Von Hannover v. Germany* (No. 1) App no 59320/00 (ECtHR, 24 June 2004), ECLI:CE:ECHR:2004:0624JUD005932000, paras 50 and 53 ; *Von Hannover v. Germany* (No. 2) App nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), ECLI:CE:ECHR:2012:0207JUD004066008, para 95.

[130] This principle follows from the right to a fair trial as codified in article 6 ECHR. In Dutch law this is translated into the Miranda warning or caution ('*de cautie*' in Dutch) as codified in article 29(2) of the Dutch Code of Criminal Procedure.

[131] *Von Hannover v. Germany* (No. 2) App nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), ECLI:CE:ECHR:2012:0207JUD004066008, para 110.

Having discussed both perspectives, the interests at stake will be reviewed, including whether essential aspects or fundamental values of private life are being compromised. In the end, a fair balance has to be found between these conflicting fundamental rights.[132]

There are five criteria in ECtHR case-law on the balancing of the right to privacy and freedom of expression and information, that should be taken into account:[133] whether the information would contribute to a debate of general interest, whether it concerns a well-known person, what the prior conduct of the person concerned is, whether consent had been given, what the form and consequences of the publication in question were and, lastly, what the circumstances were in which the information, or the photo, was collected.[134]

As all fundamental rights have equal weighing, the proportionality test evolves around the question of whether protection of one fundamental right can be achieved with the lowest cost possible to other fundamental rights in question.

If these five criteria are applied, it can be noted that Bellingcat's article on Shahin Gheiybe contributes to a debate of general interest, as Bellingcat found the location of a fugitive Dutch criminal. Moreover, Shahin Gheiybe is well-known by the government and the police, as he has been named a few times on TV-shows concerning his fugitive status. However, his fame seems too minimal to consider him a well-known public figure in the whole of society. If he continues to receive increasing attention in the media this may change.

Concerning his previous conduct, it can be noted that Shahin Gheiybe is a convicted criminal, sentenced to 13 years of imprisonment, who escaped from prison and publicly posted pictures and videos on his Instagram account, sometimes teasing the police by statements like 'catch me if you can'.[135] His online behaviour on Instagram is provoking and seems to call for the public's attention, which shows that his past behaviour is one of the reasons for the increased publicity and his decreased privacy.

When looking whether consent had been given by Shahin Gheiybe and the circumstances of the collection of his personal data, it could be argued that he implicitly agreed for his personal information to be publicly known, as he first had a public Instagram account. Moreover, even after Shahin Gheiybe turned his Instagram account into a private account he continued to have a 'rather welcoming door policy'.[136] Shahin Gheiybe explicitly allowed Bellingcat to access this

[132] ECtHR, 'Guide on Article 8 of the European Convention on Human Rights - Right to Respect for Private and Family Life (Council of Europe 30 April 2019) <www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 2 August 2019 1,8.
[133] *Von Hannover v. Germany* (No. 2) App nos 40660/08 and 60641/08 (ECtHR, 7 February 2012), ECLI:CE:ECHR:2012:0207JUD004066008, para 108.
[134] Idem. paras 109 – 113.
[135] This quote is the title of one of his Instagram posts on his private Instagram. See: Instagram, account 'shahin.mzr' <www.instagram.com/shahin.mzr/>, accessed 24 July 24 2019.
[136] See footnote 216 for the explanation of the 'rather welcoming door policy'; Email from Bellingcat contributor and author of Bellingcat's article on Shahin Gheiybe, Henk van Ess to author (23 July 2019).

information.

However, it seems unlikely that Shahin Gheiybe's intention was to actively aid Bellingcat in its research against himself. Moreover, Shahin Gheiybe did not explicitly give permission to Bellingcat to save, analyse and doxx his Instagram content. A follow request only entails a request to view the content and respond to it by posting comments or liking it. Giving permission to someone to view and comment on personal information is not the same as giving permission to save, analyse and doxx the same information.

The difficulty here is that giving someone permission to access one's personal photos and videos on Instagram, in practice, also entails giving permission to save and analyse this information, as it is simple to do so once one has access to someone's Instagram account. Because of the collected data from Shahin Gheiybe Instagram, Bellingcat had enough information to start a crowdsourcing campaign that led to Shahin Gheiybe's latest location. Moreover, the personal information on Instagram led to a publication on Bellingcat's website and other online media channels, giving Shahin Gheiybe photos, name and videos far wider exposure than they had previously, when they were only posted on his Instagram account.

This review reveals a mixed picture. On the one hand, it shows the importance and relevance of doing online research on a fugitive criminal and publish the findings, exercising the right to freedom of speech and information. Following this perspective, Bellingcat's right to freedom of expression and information prevails as Shahin Gheiybe is a fugitive criminal who simply created leads in his own investigation by being public on social media.

Contrarily, this case study portrays the image of a civilian that gave away more of his privacy than he could have reasonably expected. The fact that Shahin Gheiybe's last known location was found due to information he provided for himself on his personal Instagram account, seems to go against the legal prohibition of a suspect unwittingly cooperating in his own conviction.[137]

Whether or not Shahin Gheiybe consciously chose or should have been conscious of his choice to aid investigations against himself seems vital in deciding which fundamental right prevails in the scenario, which is difficult to prove in the context of OSINT.

6. Sub-conclusion

A large part of weighing up Shahin Gheiybe's privacy interests against Bellingcat's freedom of expression depends on the way OSINT is treated. On the one hand, one can view OSINT as a useful intelligence discipline based on publicly available data, which concerns information free from any substantial privacy concerns due to its public nature.

On the other hand, OSINT can be viewed as a method of investigation undermining the right to privacy, disguising itself as free of privacy implication, while some of the information used by

[137] See footnote 221.

OSINT is not necessarily information people wanted to become as public as it did. This means that people should be protected online against unwittingly giving away more of their privacy than they might want or think they are giving away.

It also means that once information is public, it should still be treated with care and its use should be regulated to protect people whose information is out there without their consent. Relating this to the case study, the question arises whether separate permission of Shahin Gheiybe should have been given to Bellingcat to download and doxx his personal data, or whether the fact that the data was publicly available meant that Bellingcat did not have to ask for permission.

The answer to this question is mainly dependent on the role society want to attribute to OSINT which will in turn largely depend on the usefulness of the practice of OSINT in investigations. The prevailing benefits or detriments of OSINT as a practice will determine whether future regulations will allow for more liberal use of publicly available information or more restriction. Ethical and political considerations indicate the direction in which the law will go.

Therefore, the next chapter will focus on the various ethical and political considerations on the use of OSINT, civilian criminal investigations and online vigilante justice. Subsequently, chapter five will discuss the possibilities of legally regulating OSINT to find a fitting legal approach to settle the problematic relationship between OSINT and privacy.

IV. Ethical and Political Considerations on Civilian Criminal Investigations

The changing landscape of criminal investigations has not only increased civilians' role in criminal investigations but also seen the rise of a new type of justice. This chapter looks at OSINT, civilian criminal investigations and vigilante justice arising from civilian criminal investigations from both an internal-legal perspective and an external-normative perspective.

The internal-legal perspective assumes 'sharing the perspective of judges, lawyers, legislators or citizens who engage in legal practice'.[138] The external-normative perspective includes the evaluation of these phenomena from both a moral and political point of view, to come to well-rounded recommendations. Combining these two perspectives enables more thorough review of OSINT's, civilian criminal investigations' and vigilante justice' benefits and detriments.

This chapter gives coherent recommendations whether these practices should be encouraged or discouraged, *inter alia* by means of the case-study on Shahin Gheiybe. Afterwards, chapter five will propose a regulation on the use of OSINT in civilian criminal investigations.

1. Reliability of OSINT

[138] See footnote 40.

First, the reliability of OSINT as a means of research is discussed. In the case study, the social media platform Instagram was the main source for OSINT. Bellingcat was able to answer the question whom Shahin Gheiybe interacted with and where he was residing by investigating his Instagram and tracing Shahin Gheiybe's interactions with other Instagram users.

By analysing a video on Instagram of 9 March 2019 – depicting a house and Shahin Gheiybe himself talking and mocking the police – Bellingcat was able to find his latest location at the time.[139] The flowers, the garbage can, the size of the well-maintained garden and the size and architectural style of the house, all depicted in the video, were cues in tracing his location. These cues would have never been found without his social media presence and were vital in locating Shahin Gheiybe. The case study is proof of the enormous knowledge that social media can yield in criminal investigations.

However, open-source information like social media posts, can also be deceptive. By either using a different geotag[140] than the real location of the photo or video, tagging other people than were present in the photo or by photoshopping a certain object or background, the audience can be tricked. Bellingcat tries to prevent this by looking at pictures and videos that include a clearly identifiable image of the subject of their research, or a distinctly recognizable object.[141] However, if a subject is aware of their research – which is not too difficult as Bellingcat posts its research method step-by-step online on their website – he or she could try to intentionally deceive Bellingcat, influencing its findings. It is dangerous that open-source information can be altered, depicting fake cues or the wrong people in pictures or videos. It seems necessary to let experts first consider whether open-source information is trustworthy before using it in research.

2. Transparency of OSINT

A key characteristic of OSINT is that it differs from more traditional knowledge gathering disciplines because it functions in full transparency.[142] Bellingcat's OSINT research is an example, as its methods and findings are explained precisely in the articles on its website. Its online audience can follow every step of the investigation process.[143] This transparency can work both ways.

[139] See chapter III paragraph 2 for an overview of all the facts concerning the case study of Shahin Gheiybe.
[140] Geotagging is putting GPS-coordinates of a certain location on online content, like a photo or a video, to show what someone's physical location is or was.
[141] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* at: <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 14 July 2019.
[142] Leonore ten Hulsen & Sophia Mard, 'Coding and Conceptualizing Technology in the Future of Law and Legal Practice: An Overview of the ALF Annual Seminar 2019' (2019) 11 Amsterdam Law Forum 76, 77.
[143] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* at: <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 28 July 2019.

A positive effect of the transparency of OSINT is that openness about online investigative methods and activities is known to generate trust. This trust is necessary to mobilize other civilians to contribute to investigations, of which crowdsourcing is an example.[144]

Another positive effect of the transparency of OSINT is that it allows other civilians to review the methods and findings of the civilian investigator, to check its credibility.[145] Nevertheless, considering the fact that most civilian criminal investigations using OSINT work on a voluntary basis, it is questionable whether there are sufficient means available to ensure proper reviews to verify other civilians' investigations.[146]

Bellingcat argues that its transparency is often the reason why it gets so far with its investigations. Shahin Gheiybe's last know location would never have been found without the help of over 60 Twitter users in a big crowdsourcing action on Twitter.[147] OSINT allows for distributed expertise and crowdsourcing serves as a communal focus on solving a problem by sharing knowledge between various internet users.[148] Where the police oftentimes have expertise within a certain field, like cybercrime, the public can consist of various experts in a variety of fields.[149]

Moreover, the public constitutes an undefined amount of people, not constrained to a location or time. They can serve as additional 'eyes and ears' to the investigators, although steering these eyes and ears in the right direction is vital for them to be useful.[150]

Besides, since people contribute in a civilian capacity they are participating on a voluntary, cost-free basis. Crowdsourcing as a method of investigation therefore saves time and money, while extending the research possibilities. Crowdsourcing could even prove useful in supporting the comparatively limited resources of the government.[151]

However, a strange property of crowdsourcing is the double identity civilians are attributed. On the one hand, civilians are the suspects being surveyed. On the other hand, they are the surveillance. An example of this double standard is the existence of various hotlines present in

[144] Leonore ten Hulsen and Sophia Mard, 'Coding and Conceptualizing Technology in the Future of Law and Legal Practice: An Overview of the ALF Annual Seminar 2019' (2019) 11 Amsterdam Law Forum 76, 77.
[145] Ibid.
[146] Idem p.76,78.
[147] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 14 July 2019.
[148] Leonore ten Hulsen & Sophia Mard, 'Coding and Conceptualizing Technology in the Future of Law and Legal Practice: An Overview of the ALF Annual Seminar 2019' (2019) 11 Amsterdam Law Forum 76, 77; Johnny Nhan & Laura Huey & Ryan Broll, 'Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings' (2017) 57 British Journal of Criminology 341, 348.
[149] Ibid.
[150] Idem p. 341, 357 and 359.
[151] Gary T Marx, 'The Public as a Partner? Technology Can Make Us Auxiliaries as well as Vigilantes' (2013) 11 IEEE Security & Privacy 56, 60.

most countries, to report all types of unwanted behaviour. This can bring caution and mistrust into a society, weakening social ties within a community.

Social media accounts can likewise serve as a means of surveillance, due to the personal nature of the cyberspace.[152] The line between civilian participation and civilian monitoring is delicate.

Another negative effect of OSINT is that it can be difficult to keep the lead in an investigation if the suspect can track the researchers' methods and findings. In the case study, Shahin Gheiybe could read on Bellingcat's website that his location was found, allowing him to relocate himself and to regain his anonymity.

Shahin Gheiybe himself also criticised Bellingcat's research on him and stated on Instagram that the Dutch newspaper AD and Bellingcat are 'throwing money away' by doing investigations into his last known location and publishing about it online. He states: 'I already put the location above the photo[153] that you [read: Bellingcat and the media] are referring to. Do not throw away your money for investigations like this. Just ask me or pay attention'.[154]

Bellingcat states that it sends the police 'even the tiniest leads' during its investigations to give them a head start, but it is uncertain whether this head start will be of any advantage. The police will need time to check the lead to see if it is trustworthy and accurate. By that time, Bellingcat's research might have been announced publicly on Twitter or Bellingcat's website, rendering the research outdated.

3. Effectiveness of OSINT

Next to reliability and transparency issues, OSINT lacks legal consequences when used in the context of civilian criminal investigations as civilians are not competent to prosecute or punish suspects. Concerning the case study, Bellingcat brought its research to the Dutch police but nothing happened afterwards. The lack of an extradition treaty with Iran prevented further legal steps.[155] Civilians might be able to hand over substantive proof regarding a crime, but in the end it is up to the authorities to prosecute or not. This shows that civilian criminal investigations on

[152] Ibid.

[153] The news article does not specify which photo Shahin Gheiybe is referring to exactly, but it concerns one of the pictures used in Bellingcat investigative research, see: Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 14 July 2019.

[154] Sebastiaan Quekel, 'Rosmalense 'Treitercrimineel' Gheiybe Blijft Voortvluchtig en Tart op Instagram Ook de Media' *Algemeen Dagblad* (19 maart 2019) <www.ad.nl/den-bosch/rosmalense-treitercrimineel-gheiybe-blijft-voortvluchtig-en-tart-op-instagram-ook-de-media~a6f4a988/> accessed 27 July 2019.

[155] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 14 July 2019; Sebastiaan Quekel, 'Crimineel Die Zich Bij Echtpaar Verstopte Tijdens Klopjacht Zegt 'Sorry'' *Algemeen Dagblad* (22 April 2019) <www.ad.nl/binnenland/crimineel-die-zich-bij-echtpaar-verstopte-tijdens-klopjacht-zegt-sorry~a6a910960/> accessed 27 July 2019.

itself lack the legal implications necessary to hold perpetrators accountable.

Moreover, civilian's participation is increasingly encouraged, and civilians' findings are even used in police investigations – for example through an app for civilians to aid criminal investigations – [156] without providing for any legal safeguards like proportionality, subsidiarity and objectivity. These safeguards are necessary for the judicial system to function fairly and reasonably. By delegating certain aspect of criminal investigations to civilians, the police are circumventing restrictions in the law aimed at protecting civil liberties, as civilian investigators are not bound by these restrictions.[157] This undermines the rule of law.

Furthermore, civilians do not receive any proper training in doing investigative work. This means they might act on biases or gut feelings, causing nuisance to innocent people, either online or offline. Because of the non-neutral nature of technology at large, it is important for investigators to be aware of their build-in biases and how these can affect their investigations.[158]

A lack of police guidance or feedback on civilian investigations can cause civilians efforts to be flawed or illegal, leading to a waste of time and resources on both ends, since the police will first need to check the material handed in by civilian investigators.[159]

Besides, there is a risk of justice becoming a scarce good, reserved for the few. If civilians are increasingly involved in criminal investigations, the unwanted consequence might be that victims with more knowledge, power or money can organize bigger, better or more thorough investigations.[160] Justice should remain accessible to everyone. The collaboration between civilians and the government should therefore be seen as an addition to traditional criminal investigations and not serve as a replacement of police investigations, necessary because of budget cuts or lack of capacity of the police to investigate.[161]

In light of the previous arguments, it seems evident that civilians' criminal investigations and their use of OSINT can have serious downsides. Legal safeguards should be implemented to ensure the rule of law.

---

[156] See chapter II paragraph 2 on the changing landscape of justice administration for more information on this app; Politie, 'Politie en OM Lanceren App voor Burgeronderzoek' *Politie.nl* (27 May 2019) <www.politie.nl/nieuws/2019/mei/27/00-politie-en-om-lanceren-app-voor-burgeronderzoek.html> accessed 7 June 2019.

[157] Gary T Marx, 'The Public as a Partner? Technology Can Make Us Auxiliaries as well as Vigilantes' (2013) 11 IEEE Security & Privacy 56, 60.

[158] Isabella Banks and Leonore ten Hulsen, 'Human Rights Weekend: Artificial Intelligence, Big Data & Human Rights: Progress or Setback?' (2019) 11 Amsterdam Law Forum 70, 72 and 75.

[159] Johnny Nhan, Laura Huey and Ryan Broll, 'Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings' (2017) 57 British Journal of Criminology 341, 353.

[160] Pim Lindeman, 'Burgers Die Zelf Misdrijven Oplossen Onontkoombare Trend, 'Als Ze Maar Niet Eigen Rechter Spelen'' *De Gelderlander* (19 April 2019) <www.gelderlander.nl/enschede/burgers-die-zelf-misdrijven-oplossen-onontkoombare-trend-als-ze-maar-niet-eigen-rechter-spelen~a46c3d76/> accessed 29 July 2019.

[161] Ibid.

4. Online Vigilante Justice

Online vigilante justice is increasingly present as a consequence of the lack of legal implications of civilian criminal investigations.

Previously, the surge of an alternative type of justice seeking and administrating was explained called online vigilante justice, but not yet its benefits and detriments to society.[162] Online vigilante justice can be beneficial to society. For example, there are websites run by volunteers that create blacklists of spambots, to keep an overview of real and automated online behaviour. Moreover, there are volunteer patrols of netizens on E-bay that check apparent frauds to protect consumers.[163] Especially in the shape of collaborations between government and civilians, types of online vigilante behaviour of netizens can contribute to the realization of public security goals.[164]

However, there are many problematic sides to online vigilante justice. Firstly, if subjective versions of justice are created and sustained, state legitimacy will erode. The belief that the government is incapable of providing security will be fuelled, in turn stimulating other initiatives of vigilante justice.[165]

One of the most problematic aspects of online vigilante justice might be the risk of wrongly suspecting, shaming or doxxing a person.[166] Vital principles of criminal law, like the presumption of innocence, proportionality, subsidiarity and objectivity, are easily disregarded when administering online vigilante justice.[167] Online vigilante justice opens up the possibility of administering justice when there is in fact no injustice taking place.[168] This can lead to troublesome situations, like when an American teenager committed suicide due to bullying, the wrong person was suspected of bullying her and his personal information was doxxed by the activist group Anonymous.[169]

Another example involves an undergraduate student who was wrongfully suspected of partaking in the Boston marathon bombings and whose identity and personal details were doxxed. His family received many letters and threats before it became public knowledge that the student was wrongfully accused of being one of the perpetrators.[170]

---

[162] See chapter II paragraph 2 on the changing landscape of justice administration for more information on the emergence of online vigilante justice.
[163] Lennon Y.C. Chang, Lena Y. Zhong and Peter N. Grabosky, 'Citizen Co-Production of Cyber Security: Self-Help, Vigilantes and Cybercrime' (2016) 12 Regulation & Governance 101, 103.
[164] Idem p. 104.
[165] Idem p. 108.
[166] Johnny Nhan, Laura Huey and Ryan Broll, 'Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings' (2017) 57 British Journal of Criminology 341, 353.
[167] Eelco Moerman, 'Burgers in het Digitale Opsporingstijdperk' (2019) 94 NJB 1, 4 and 5.
[168] Gary T Marx, 'The Public as a Partner? Technology Can Make Us Auxiliaries as well as Vigilantes' (2013) 11 IEEE Security & Privacy 56, 56.
[169] Johnny Nhan, Laura Huey and Ryan Broll, 'Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings' (2017) 57 British Journal of Criminology 341, 342.
[170] Idem p. 341, 354 and 358.

There is in fact little legal protection for victims of online vigilante justice. In case of faulty accusations by civilian investigators, a victim has far fewer legal remedies than a suspect in a criminal law case.[171] In case of doxxing, a victim will have to go to the civil law judge to argue his or her case and the judge will have to assess the case based on a horizontal weighing of the fundamental rights involved.[172] Most often the victim would want to stop the wider spread of the personal information, which can be close to impossible in a digital context.

In some cases, like in the example of paedophiles,[173] the victims of online digilante justice will most likely not even report the act of vigilante justice to the police because of the consequences this can have for themselves. Digilantes often have compromising evidence that could lead to prosecution of the paedophiles and therefore acts as a safeguard that their victims will keep quiet.[174]

Lastly, if civilians take justice into their own hands, they can frustrate ongoing investigations by tainting with evidence or leaking sensitive information as part of their online vigilante justice, which could lead to the failure of an investigation.[175]

All in all, online vigilante justice risks jeopardizing many legal safeguards, creates legal uncertainty and destabilizes the rule of law which is necessary in a democratic society. Therefore, it should be clearly regulated and restricted to prevent unnecessary harm.

5. The Need for Regulation

In November 2018, a Dutch politician called Chris van Dam advocated in parliament to establish a guideline on civilian criminal investigations, referring to troublesome behaviour of civilians in neighbourhood watch-apps.[176] He argued that clear rules have to be created that civilians must adhere to when participating in criminal investigations.

Currently, there is only one right that civilians have when it comes to criminal investigations: to arrest perpetrators in the act,[177] which is insufficient considering the increasing tasks of civilians in criminal investigations. Van Dam suggested that the government should offer a short training

[171] Eelco Moerman, 'Burgers in het Digitale Opsporingstijdperk' (2019) 94 NJB 1, 4.
[172] See chapter III on the horizontal effect of fundamental rights for more information.
[173] See chapter II paragraph 2 on the changing landscape of justice administration for more information on the emergence of online vigilante justice and the example of the paedophiles.
[174] Lennon Y.C. Chang, Lena Y. Zhong and Peter N. Grabosky, 'Citizen Co-Production of Cyber Security: Self-Help, Vigilantes and Cybercrime' (2016) 12 Regulation & Governance 101, 106.
[175] Idem p. 109.
[176] Pim Lindeman, 'Burgers Die Zelf Misdrijven Oplossen Onontkoombare Trend, 'Als Ze Maar Niet Eigen Rechter Spelen'' *De Gelderlander* (19 April 2019) <www.gelderlander.nl/enschede/burgers-die-zelf-misdrijven-oplossen-onontkoombare-trend-als-ze-maar-niet-eigen-rechter-spelen~a46c3d76/> accessed 29 July 2019.
[177] Article 53 Dutch Code of Criminal Procedure.

in addition to the to-be-established guideline, that civilians have to partake in before contributing to criminal investigations.[178]

In the US, a federal law on doxxing has already been introduced in Congress. The proposal aims to 'criminalize disclosure of personal information with the intent to cause harm'.[179] Even though it seems like a promising step for victims of doxxing, it is questionable whether enforcement of this law will be feasible, as anonymity online is easily reached. Moreover, once information is public online, it will be difficult to remove. This is often illustrated by the saying 'the internet never forgets'.

To protect civilians against the detriments of civilian criminal investigations and online vigilante justice, legally binding measures are needed. An option for desirable use of civilian criminal investigations could be to create evidence standards for civilians, which can filter wrong suspicions, unlawful evidence and can ensure legal safeguards in the investigation. Another measure could be aimed at redefining OSINT and legally regulating its privacy implications.[180]

Alternatively, the police could give more direction to civilian investigators, by requesting or describing the type of help they need, narrowing the public's efforts in the right direction.[181] The police could also focus on encouraging civilians to send their efforts to the police and discourage civilians to engage in their own type of vigilante justice online.[182]

6. Sub-conclusion

Private parties can contribute to filling in voids in criminal investigations, inter alia through the power of crowdsourcing, to reach the common goal of providing security for all.[183] By stimulating collaboration between police and civilians, national security, investigation efforts and justice seeking can be democratized.[184]

Moreover, attributing legal implications to civilian criminal investigations can subsequently lower the need for types of online vigilante justice. Initiatives like the app by the Dutch police and the

[178] Pim Lindeman, 'Burgers Die Zelf Misdrijven Oplossen Onontkoombare Trend, 'Als Ze Maar Niet Eigen Rechter Spelen'' *De Gelderlander* at: <www.gelderlander.nl/enschede/burgers-die-zelf-misdrijven-oplossen-onontkoombare-trend-als-ze-maar-niet-eigen-rechter-spelen~a46c3d76/> accessed 29 July 2019.

[179] HR 3067 introduced in the House of Representatives (June 27, 2017), in: Jeffrey Pittman, Privacy in the Age of Doxxing (2018) 10 Southern Journal of Business & Ethics 53, 55.

[180] One-way privacy can be protected from digilantes is by implementing the digital home right as a proxy for privacy combined with the theory of privacy as contextual integrity. This will be discussed in chapter V.

[181] Johnny Nhan & Laura Huey & Ryan Broll, 'Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings' (2017) 57 British Journal of Criminology 341, 359.

[182] Gary T Marx, 'The Public as a Partner? Technology Can Make Us Auxiliaries as well as Vigilantes' (2013) 11 IEEE Security & Privacy 56, 60.

[183] Eelco Moerman, 'Burgers in het Digitale Opsporingstijdperk' (2019) 94 NJB 1, 5.

[184] Isabella Banks and Leonore ten Hulsen, 'Human Rights Weekend: Artificial Intelligence, Big Data & Human Rights: Progress or Setback?' (2019) 11 Amsterdam Law Forum 70, 75.

eyeWitness to Atrocities-app should therefore be encouraged,[185] while online vigilante justice on itself should be restricted as much as possible.

The occurrence of vigilante justice has proven to be an inappropriate replacement for our governmental system of justice. It is important to ensure legal safeguards throughout civilian criminal investigations and justice seeking. Civilian criminal investigations require regulation to protect investigations and suspects against reliability, transparency and effectivity issues.

In conclusion, OSINT on itself and civilian investigators are useful additions to the existing means of criminal investigations as long as potential suspects receive legal protection. This will be taken into account in chapter five, which will discuss the possibilities of legally regulating OSINT in civilian criminal investigations.

V. Alternative Theories on Privacy in relation to OSINT

The previous chapters have tried to grasp in what ways civilians' criminal investigations using OSINT impact the privacy of their suspects. This chapter focuses on the subsequent part of the research question, namely, how to protect the privacy of suspects in civilians' criminal investigations using OSINT.

The previous chapter concluded that OSINT can be a useful tool for aiding criminal investigations. The aim of legally regulating OSINT in civilian criminal investigations should therefore be to protect privacy of potential suspects, without restricting the use of OSINT in its entirety.

Firstly, the challenges posed by the changing landscape of criminal investigations to the traditional conceptualization of privacy are discussed. Secondly, this chapter will propose a theoretical solution, by redefining parts of privacy in the public sphere.

By following Nissenbaum's approach to privacy as contextual integrity and combining it with Koop's proposed new privacy proxy of 'the digital home', a different approach to OSINT is argued for, allowing for effective legal regulations of privacy in civilian criminal investigations. This way, substantive protection of privacy can be given to those who are subject to OSINT in civilian criminal investigations.

1. The Problems with the Traditional Three Principles of Privacy

[185] Politie, 'Politie en OM Lanceren App voor Burgeronderzoek' *Politie.nl* (27 May 2019) <www.politie.nl/nieuws/2019/mei/27/00-politie-en-om-lanceren-app-voor-burgeronderzoek.html> accessed 7 June 2019; 'EyeWitness Project' <www.eyewitnessproject.org/> accessed 29 July 2019.

The first chapter elaborated on the traditional principles of privacy, inherent in every theory on privacy protection.[186] Now, the difficulties of applying them to situations which concern new technological developments will be discussed.

Firstly, it is difficult to define the boundaries of traditional privacy principles as they depend largely on a specific culture and time.[187] These principles are portrayed as universal, whereas in reality they can differ substantively depending on their context.

In a recent court case in the Netherlands, the Supreme Court created new rules on searching a smartphone,[188] putting emphasis on whether or not a complete image of a person's life can be formed by searching the smartphone to judge the severity of the breach of privacy. If a more or less complete image of certain aspects of a person's life can be created based on a digital medium like a smartphone, the search can be found unlawful, if it lacks a specific legal ground.[189] This case exemplifies a changing perception of the boundaries of privacy and shows a combined approach to privacy based on informational and locational privacy.[190]

Moreover, the traditional principles are not suited to situations of surveillance in public, in which new technologies play a role.[191] An example of such non-applicability arises in the case of OSINT. OSINT extends the possibility to observe, gather and analyse information about people and their behaviour.

According to the principle of information privacy,[192] OSINT should not pose any privacy problems if it does not include sensitive personal information. However, this ignores the potential detailed picture that can be created of someone's personal life after analyses of seemingly non-private information, like metadata. Metadata can be more revealing than content, allowing for a detailed picture, including relationships, political views or sexual preference.[193] Such practices violate people's privacy. According to the principle of location privacy,[194] information retrieved from publicly available sources does not lead to a privacy violation, as the information is located in a public zone.

However, when a person creates a complete image of someone's private life based on OSINT, it can be intrusive to one's privacy, even if the information is not sensitive personal information

[186] See chapter I paragraph 1 for the traditional theories and principles on privacy; Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 124.
[187] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 132.
[188] HR 4 April 2017 *Smartphone-arrest*, ECLI:NL:HR:2017:584.
[189] Ibid.
[190] See chapter I paragraph 1 for more background information on the traditional theories and principles on privacy.
[191] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 134.
[192] As explained in chapter I paragraph 1, information privacy refers to the nature of information and how societal standards judge its level of 'intimacy, sensitivity or confidentiality'.
[193] Yves-Alexandre de Montjoye and others, 'Unique in The Crowd: The Privacy Bounds of Human Mobility' (2013) 3 Scientific Reports 1, 1 and 4.
[194] As explained in chapter I paragraph 1, location privacy refers to privacy connected to certain places, like one's home. Depending on the privacy of a setting, the severity of the privacy violation is judged.

and located in a public sphere. The traditional principles of privacy do not offer an explanation for this as they are unable to adapt to new dimensions of time, location and cultural influence.[195]

Moreover, the sole option of dichotomies in the traditional three-principle framework – like the choice between the public and private sphere – does not allow for flexibility in an age where the lines between public and private life are blurring.[196] This shows the need for a more modern, technology-adapted, principle, which Nissenbaum provides in the shape of contextual integrity.

2. Privacy as Contextual Integrity

To solve the difficulties that the right to privacy faces with the emergence of technological developments, this paper focuses on combining a proposed proxy to privacy with the theory of privacy as contextual integrity.

The theory of privacy as contextual integrity is based on the idea that everything always has a context and no area of life is inherently free from privacy concerns.[197] Contextual integrity acknowledges these varying contexts and argues that these each have their own 'set of norms, which governs its various aspects such as roles, expectations, actions and practices'.[198]

These contexts cannot all be made explicit, but are rooted in common beliefs, common experiences and literature.[199] The norms governing information about people in certain contexts can be divided into two types: 'norms of appropriateness' and 'norms of flow or distribution'.[200] Whenever either type of norm is violated, the contextual integrity is violated and a privacy breach occurs.[201]

2.1. Norms of Appropriateness

Norms of appropriateness refer to norms that govern whether it is appropriate, fitting or even expected to reveal certain information about people in a certain context.[202] Every place and context is governed by these norms, both private and more public spheres. The fact that information distribution in one context can seem appropriate, does not mean that the same information distribution will always be appropriate, when the context changes.

An example is sharing information on one's love life with their friends, but not their family. If information is appropriated from one context to another, a violation of the norms of

[195] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 136.
[196] See chapter I paragraph 1 on the changing landscape of criminal investigations.
[197] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 137.
[198] Ibid.
[199] Ibid.
[200] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 138.
[201] Ibid.
[202] Ibid.

appropriateness occurs.[203] Another example would be sharing personal information with a friend in private messages on Facebook and that information becoming public knowledge at work. Following this theory, being active online in a (semi-)public sphere like social media should not preclude one from having any reasonable expectation of privacy.

2.2. Norms of Flow or Distribution

Norms of flow or distribution[204] refer to norms that govern whether the transfer of information between parties is appropriate or fitting, depending on the context. The norms of distribution differ from norms of appropriateness as the latter focus on the appropriateness of sharing information in a certain context, whereas norms of distribution focus on whether the distribution of that information respects contextual norms like confidentiality, free choice, discretion, need, entitlement and obligation, amongst others.[205]

For example, if someone shares information with a friend and tells her to keep it a secret but she tells their parents, she violated the contextual norm of confidentially, which functions as the norm of information distribution.

On the internet, the norms governing the exchange of information depend on the platform and online context. On Facebook Messenger or Instagram, one might expect a norm of discretion concerning the exchange of the information one posts, whereas on Google or Wikipedia the norm regulating the distribution of information is the free choice to post and entitlement to use, copy or analyse the information. The first information one considers more personal, whereas the latter information one considers free, public knowledge.

It is important to note that the violation of these norms could still be justified by weighing the right to privacy against other rights, like freedom of speech and right to information.[206] Freedom of speech, free press and security are often named to argue for free flows of information and a justification of privacy violations.[207] Whether or not a justification applies, will have to be judged on a case-by-case basis.

3. OSINT, Contextual Integrity and Privacy Protection

The theory of contextual integrity gives an explanation for the prevalence of privacy in public settings and is, therefore, relevant in relation to OSINT. In many digital settings, including on social media, social norms and social practices are in fact the only mechanisms governing privacy.

[203] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 140.
[204] Hereinafter these norms will be referred to as the norms of distribution.
[205] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 141 and 142.
[206] Ibid p. 151.
[207] Ibid p. 147.

To a large extent, the problem with OSINT is that it concerns information in a public sphere, which brings with it the assumption of it being freely accessible, whereas it can also contain information that people want to keep private. This in itself causes a privacy paradox: the information is publicly available and accessible for all, therefore inherently not private, but at the same time, the information is often (sensitive) personal information and is therefore inherently private.

Some argue that there is no paradox, because people themselves have uploaded the information, or given permission for the information to be put online and subsequently have given up their privacy. According to this view, sharing information online is an individual responsibility.[208] Once people post their personal information online, they give up their privacy consciously and make the information publicly accessible.

According to this view, it is one's own fault if their personal information becomes public, if it gets used in a way that the concerned individual does not approve of or when he/she experiences negative effects from posting information online, like doxxing.

This view of privacy as an individual responsibility is a widely shared approach to privacy both online and offline, even though it amounts to a type of victim-blaming. It portrays privacy as something one will only need if a person has 'something to hide'.[209]

This approach unfairly favours personal choice and overvalues one's ability to estimate privacy implications over other factors that can cause personal information to be publicly available. For example, the structure of social media provides companies with an insight into one's social connections and interactions with others without that person consciously or actively sharing it.[210] Other information people share subconsciously includes the use of third-party apps, advertisement interactions, clicking behaviour and screen time.[211]

The way social media platforms like Facebook are built, tricks people into sharing information by leveraging trust.[212] Social media platforms are based on human social needs and are designed to nudge users to disclose.[213] Information is gathered by constant monitoring of the platforms with the unwanted consequence that the information can end up somewhere online, potentially

[208] Alice Marwick, Claire Fontaine and Danah Boyd, '"Nobody Sees It, Nobody Gets Mad": Social Media, Privacy and Personal Responsibility Among Low-SES Youth' (2017) 3 Social Media + Society 1, 1.
[209] Ibid.
[210] Wouter Stol and Litska Strikwerda, 'Online Vergaren van Informatie voor Opsporingsonderzoek' (2018) 17 Tijdschrift voor Veiligheid 8, 8.
[211] Screen time refers to the amount of time that someone looks at something online, like an add or a video, before one scrolls further, which shows, for example, whether someone found content (not) funny or interesting.
[212] Ari E Waldman, 'Privacy, Sharing and Trust: The Facebook Study' (2016) 67 Case Western Reserve Law Review 193, 193.
[213] Ibid.

publicly available, without a person wanting it to.[214] This means that users can be tricked or mislead into sharing information and blamed for it afterwards.

It is problematic that people think they are in control of their personal information, while the control is *de facto* also in the hands of others. This deficiency in privacy protection can be addressed by applying Nissenbaums' framework.

Firstly, because the theory of contextual integrity does not work with dichotomies, rendering a situation as black and white as the privacy paradox impossible. Everything always has a notion of privacy and the context will decide whether or not privacy concerns should prevail. This counter the idea of privacy as an individual choice or responsibility that can be disposed of.

Moreover, contextual integrity asks us to look at the governing norms of a situation, making generalizations like the proposed paradox above inapplicable to real life environments. By focusing on the norms governing the appropriateness of information in contexts and norms of distribution governing information transferring, the victim-blaming can be countered. Now that the potential application of contextual integrity for general OSINT has been explained, the case study will show its use in a specific context.

4. The Case-study of Shahin Gheiybe through the Lens of Contextual Integrity

The use of Shahin Gheiybe's social media account on Instagram will be analysed to see whether it amounted to a breach of privacy through the lens of privacy as contextual integrity. Firstly, the norms of appropriateness will have to be considered. In the case of OSINT, this means that organizations like Bellingcat have to answer the question whether the information that they want to publish is appropriate in the context of where they want to publish it. The deciding factor is not whether the information is already available or whether the subject uploaded the information himself or herself.

The pictures of Shahin Gheiybe's Instagram account, including photos of holidays and Christmas celebrations, seem inappropriate to the public website of Bellingcat.[215] These pictures are fitting to the context of Instagram, where people post personal pictures of family and friends all the time, but less suitable for a public website of an international civilians' collective.

Secondly, the norms of distribution should be taken into account, governing the context of an information transfer. Social media platforms like Instagram have a norm of discretion or confidentiality as it concerns an online sphere used mostly for personal interactions. The level of discretion or confidentiality depends on factors like the amount of 'friends' of followers one

[214] Ari E Waldman, 'Privacy, Sharing and Trust: The Facebook Study' (2016) 67 Case Western Reserve Law Review 193, 194.
[215] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 21 July 2019.

has on the platform and whether the account is publicly available or on 'private'.[216] Whether the transfer of the information respects norms of distribution, does not depend on online information being already publicly available or not.

Shahin Gheiybe's Instagram is no longer public, but due to his "rather welcoming door policy'[217] he has over 5.000 Instagram followers, making the profile seem less private than a private account would suggest, arguably diminishing the norm of confidentiality.[218]

Nevertheless, Bellingcat's action of accessing, downloading and analysing all the photos of Shahin Gheiybe's Instagram, seems inappropriate because of the contextual norm of confidentiality that surrounds personal Instagram accounts. Even if Shahin Gheiybe accepts follow requests easily, exposing his private Instagram account, allowing someone to access one's Instagram content is not the same as allowing someone to download and doxx the content of one's Instagram account.

According to social norms, Shahin Gheiybe should have had a choice in the further distribution of his personal pictures outside of Instagram. Therefore, the norms of distribution were violated when Bellingcat downloaded and doxxed Shahin Gheiybe's Instagram as part of its research, without consulting Shahin Gheiybe on it. The fact that Shahin Gheiybe's Instagram was public at the time of acquiring his personal information and the fact that Shahin Gheiybe accepts follow requests easily, giving access to his Instagram account, cannot negate the norm of confidentially for further distribution of his personal information.[219]

It would be unreasonable to expect Shahin Gheiybe to take into account the possibility of a civilian organisation downloading and analysing his personal data for investigative research against him, to consider the consequences of this research and possible findings and the impact these might have on his privacy. Even if Shahin Gheiybe recognized Henk van Ess' name as a Bellingcat contributor when he accepted Henk van Ess' follow request, it is unlikely that Shahin Gheiybe meant to give Bellingcat indefinite access to his account, which is effectively what happened now as Bellingcat downloaded all his Instagram content and doxxed a part of it on Bellingcat's website.

It can, therefore, be concluded that no privacy violation concerning the viewing and analysing of Shahin Gheiybe's Instagram took place, as Shahin Gheiybe first had his Instagram account on public and later gave permission to a Bellingcat contributor to view his private Instagram account. However, Bellingcat violated the norms of appropriateness and distribution in the context of their investigation into Shahin Gheiybe by downloading and doxxing his personal Instagram account. This constitutes a violation of Shahin Gheiybe's privacy.

---

[216] If someone's Instagram account is on 'private' mode, only their followers can see their posts and live stories.

[217] Email from Bellingcat contributor and author of Bellingcat's article on Shahin Gheiybe, Henk van Ess to author (23 July 2019).

[218] Instagram, account 'shahin.mzr' <www.instagram.com/shahin.mzr/>, accessed 24 July 2019.

[219] Like Bellingcat did by means of doxxing and publishing their article on Shahin Gheiybe's last known location in Iran.

The situation does potentially allow for a justification of the privacy breach, as Bellingcat acted in pursuit of investigative research on a convicted violent criminal, therefore aiding international security and public interest. Especially considering Shahin Gheiybe's Instagram was vital in Bellingcat's effort to localize him, the publication of some of the personal content of Shahin Gheiybe's Instagram can be considered relevant for Bellingcat's article.

4.1. Mrs. Nasiri

In Bellingcat's efforts to trace Shahin Gheiybe, information was also accessed and collected concerning the people aiding Shahin Gheiybe in his fugitive lifestyle. Some additional remarks can be made on Mrs. Nasiri who is named a few times throughout Bellingcat's article.[220]

The house that Bellingcat identified as Shahin Gheiybe's last known location, belongs to a certain Mrs. Nasiri. Bellingcat did not release her full name in their article, but they did reveal the exact coordinates of the house and posted a link to her Instagram account in their article. Moreover, Bellingcat revealed that Mrs. Nasiri works as a lawyer and recently married Shahin Gheiybe's best friend[221] – which wedding Shahin Gheiybe attended – clearly showing that research into her private life had also taken place in Bellingcat's search for Shahin Gheiybe's last known location. Bellingcat fulfils a role as a public watchdog informing the public on the whereabouts of a fugitive – possibly dangerous – convict, but it seems uncertain what the importance is of Mrs. Nasiri's profession and marital status to the research on Shahin Gheiybe or their role as public watchdog.[222] However, Mrs. Nasiri's Instagram account was on private-mode and her Instagram profile picture did not depict a recognizable picture.[223] Moreover, quick searches on other social media or internet channels did not lead easily to more personal information on Mrs. Nasiri.[224] Therefore, it remains questionable whether the information Bellingcat published, is personal enough for a breach of the norms of appropriateness to have taken place.

Assessing whether the norms of distribution have been violated is more difficult in the case of Mrs. Nasiri as Bellingcat's article does not state everything they could have found, accessed and analysed, nor how they researched her. This makes it difficult to assess whether it was a confidentiality norm governing the personal informational or another norm.

---

[220] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 2 August 2019.

[221] Bellingcat does not release his full name either in their article, see: Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 2 August 2019.

[222] Henk van Ess, 'Locating the Netherlands' Most Wanted Criminal by Scrutinizing Instagram' *Bellingcat* (19 March 2019) <www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/> accessed 2 August 2019.

[223] Instagram, account 'Mrs. Nasiri's' <www.instagram.com/mrs__nasiri_/> accessed 14 July 2019.

[224] Based on the author's own Facebook, LinkedIn and Google searches (14 July 2019).

5. The Legal Conceptualization of OSINT: Proxies of Privacy

Social norms, like the norms of appropriateness and distribution, can be a useful means to assess privacy breaches in an online context. However, in order for legal protection of privacy to take place, transposition into law is necessary. Otherwise, other types of justice will be evoked such as types of vigilante justice, which can be skewed, disproportionate or unfair in their application.[225] A possible legal framework should aim to counter this and create a reasonable, fair and foreseeable regulation on privacy breaches caused by seeking, downloading, analysing or doxxing seemingly public information by civilians.

Many of the theories on privacy are not directly translatable into law.[226] The focus on social norms and practices of appropriateness and distribution can serve as a theoretical solution, but due to its normative nature it would create legal uncertainty if the theory were to be literally transposed into a legal regulation. Therefore, it needs to be translated into workable legal definitions. To do so, the law uses proxies of privacy as a means to protect it legally.

Proxies do not encompass privacy as a whole. Instead, they symbolise parts of privacy in order for privacy to be more tangible and effectively protected.[227] These more concrete aspects of privacy are protected in the law. There are three different approaches to shape these proxies, focusing on either the protection of the container of privacy, the substance of privacy, or the protection of certain personal contacts.[228]

An example of a container as a proxy of privacy is one's home.[229] The substance of privacy as a proxy would be the protection of someone's correspondence[230] or personal data.[231] The third category refers to privileges like the functional privilege between a lawyer and his client, but this third category is less relevant for the discussion on OSINT.[232] The general privacy protection regime embodied in the right to a private life[233] serves as an overarching protection mechanism, useful for situations in which the privacy proxies do not apply.[234]

---

[225] See chapter II paragraph 2 on the changing landscape of justice administration and chapter IV paragraph 4 on the benefits and downsides of online vigilante justice.
[226] Bert-Jaap Koops, 'Privacyconcepten voor in de 21e Eeuw' (2019) 68 Ars Aequi 1, 8 (this paper used the forthcoming version of this article sent by the author in April 2019).
[227] Ibid.
[228] Ibid.
[229] As codified in article 8(1) ECHR; Article 12 Dutch Constitution.
[230] Ibid Article 13.
[231] As codified in the GDPR. See also: Bert-Jaap Koops, 'Privacyconcepten voor in de 21e Eeuw' (2019) 68 Ars Aequi 1, 5 (this paper used the forthcoming version of this article sent by the author in April 2019).
[232] Article 165(2)(b) Dutch Code of Civil Procedure.
[233] Article 8 ECHR; Article 10(1) Dutch Constitution.
[234] Bert-Jaap Koops, 'Privacyconcepten voor in de 21e Eeuw' (2019) 68 Ars Aequi 1, 5 (this paper used the forthcoming version of this article sent by the author in April 2019).

The current proxies present in the law are based on the traditional principles of privacy protection,[235] and are therefore ill-equipped to deal with a digitalizing society. This is reflected in the fact that there are no suitable proxies present in the law which embody the specific privacy paradox inherent in OSINT.[236]

It is useful to focus on the sources of OSINT, the containers, as a proxy of privacy. Focusing on the substance of privacy as a proxy could also be useful, but in a context of civilian investigations, it will arguably be too difficult to regulate this inherently normative concept. Civilians do not have the same type of training that governmental investigators receive, hence it is desirable to create a clear and simple regulation on the use of publicly available sources by civilians.

Focusing on a container of privacy is more concrete and seems, therefore, more fitting. In the next paragraph a new legal proxy of privacy, as proposed by Koops,[237] is analysed to see whether it is fit for our contemporary society. Moreover, its relation to OSINT will also be discussed.

6. A New Proxy of Privacy: The Digital Home

A revised version of the 'home' as a container of privacy has recently been introduced by Koops, called the digital home.[238] Just like our physical home is protected in law, our digital home would likewise be secured. It would give every individual the right to decide who can access his or her personal cyberspace. Personal cyberspace can be defined as the cyberspace that one has agency over.[239]

Personal social media accounts, including those which are public, would therefore fall within this personal cyberspace. One's house is a depiction of one's privacy expectation at home and likewise is someone's personal social media account a portrayal of their private sphere and personal identity online. To create some nuance in the privacy expectations, without creating legal uncertainty, the exact privacy expectation attached to one's social media account should depend on clearly determined factors.

These factors should be based on the norms of appropriateness and distribution of contextual integrity. In practice, this should include factors like whether one has a public or private social media account, the number of followers or friends one has and whether a person uses the account for commercial or personal purposes.

[235] See paragraph 2 of this chapter for more background on the traditional principles of privacy protection and the difficulties in applying them to our contemporary society.
[236] As discussed in this chapter in paragraph 3 on OSINT, Contextual Integrity and Privacy Protection.
[237] Bert-Jaap Koops, 'Privacyconcepten voor in de 21e Eeuw' (2019) 68 Ars Aequi 1, 10 (this paper used the forthcoming version of this article sent by the author in April 2019); Bert-Jaap Koops, 'Digitaal huisrecht' (2017) 3 Nederlands juristenblad, 183 – 187.
[238] Ibid.
[239] Ibid.

For example, a social media influencer with a public social media account that makes money displaying (aspects of) her personal life online, uses social media professionally and therefore has a different expectation of the distribution of her personal information and privacy, in comparison to someone who uses social media in a purely private manner.

Following this reasoning, a non-professional, personal social media account in private-mode, with a definite number of followers or friends that one knows in real life – for example less than a few hundred – should receive the most privacy protection, as this person intended to put personal content online only for his or her friends to see.

This combination of the privacy proxy 'the digital home' and contextual integrity to fill in the requirements provides for a tangible framework which can be used to judge online privacy violations. However, the problem with publicly available sources is that personal information can also be found on websites owned by other parties, sometimes leaving individuals with no means to allow or refuse access to the information at stake.

To solve this, the law could legally attribute agency to individuals over specific cyberspaces within the digital home, which will always contain personal information. A few examples of specific personal cyberspaces are social media accounts, game accounts and personal (public) blogs. By explicitly defining the cyberspaces individuals should have agency over, the power that platform providers, service providers and other internet companies can exercise over one's personal information will diminish. This interpretation of the digital home would not only protect the cyberspace that one has agency over but the cyberspace that one *should* have agency over.

Another challenge to the digital home is the control of access, even if one's agency over certain personal cyberspaces is legally protected. As soon as a person gives someone permission to access their personal information in a certain cyberspace, like a social media account, in practice it often seems to imply eternal access. It is possible to remove someone as one's friend or follower or even block them, but when someone has access to a person's personal cyberspace, they also have the opportunity to download or doxx the information, even if norms of distribution argue that permission for downloading or doxxing should be given separately.[240] To solve this, downloading or doxxing personal information without the permission of the subject involved should be made illegal by law, although in practice it will be difficult to oversee and keep track of this.

Notwithstanding, creating a right to a digital home is a useful proxy of privacy. Specific cyberspaces which generate mainly personal data, like social media accounts, could be named explicitly in the law. This will formalize the right of every individual to decide who can access, analyse, download or doxx personal information from his or her personal cyberspace.

Permission to access someone's personal information and permission to download or doxx someone's personal information should be requested separately. The law should also leave room

[240] As happened to Shahin Gheiybe, see paragraph 4 of this chapter on the case study of Shahin Gheiybe.

for protection of other, undefined personal cyberspaces that have yet to arise, so the right to a digital home can adapt to technological developments in the future.

Even though the monitoring of these rules will undoubtedly pose challenges of its own, this legal framework serves as a useful attempt to protect personal information online and provides more clarity on the use of OSINT in civilian criminal investigations.

7. Sub-conclusion

Contextual integrity as a concept is useful for the discussion on OSINT and privacy in a public context. The theory of privacy as contextual integrity argues that every aspect of information has some notion of privacy attached to it and therefore true 'open' sources or 'public' information, does not exist. Moreover, contextual integrity shows the importance of social norms and social practices.

Social norms and practices ought to be taken into account when creating legal regulations for privacy protection. In connection to the proposed digital home right, contextual integrity can be used to create nuances in the privacy expectation of one's personal cyberspace and to create tangible requirements to judge privacy violations. This legal framework serves as a first attempt to regulate OSINT in civilian criminal investigations.

VI. Conclusion

This paper aimed to answer the following research question: do civilians' criminal investigations using OSINT impact the privacy of their suspects and if so, how can their privacy be protected?

This paper found that the privacy of suspects of civilians' criminal investigations using OSINT is compromised due to a lack of specific regulations governing both traditional and civilian criminal investigations and their use of OSINT specifically. For civilian criminal investigations, no regulation is in the making on the systematic use of digital publicly available sources, even though the impact these investigations can have on someone's privacy is substantial. This is worrisome in light of the changing landscape of criminal investigations, which shows an increasing role for civilians in criminal investigations and the emergence of vigilante justice as an alternative for governmental justice administration.

Civilian criminal investigations can be an effective addition to traditional law enforcement as long as legal safeguards are in place to ensure sustainable use of investigative tools. However, vigilante justice should be avoided due to its arbitrary and often capricious nature. Civilians are unsuitable to administer justice due to their non-professional capacity. Civilians are untrained and lack impartiality. Moreover, no safeguards exist against unfair justice administrating by civilians, like our governmental legal system has built-in when administering justice in a courtroom.

It is important to prevent lawbreaking to detect lawbreaking. Civilians aiding in criminal investigations should therefore be allowed, or even encouraged, as long as the law is respected, and the trial takes place in a court instead of on social media platforms.

This paper suggests a combination of contextual integrity and the digital home right to protect the privacy of suspects in civilians' criminal investigations by means of OSINT. This would combat the privacy paradox and ensure fair use of OSINT in criminal investigations, allowing for a just balance between investigation interests and privacy concerns.

VII. For Further Research

Governance relies on the existence of clearly defined communities to exercise its power. Traditionally, sovereignty is exercised over physical areas, founded on agreements with the people themselves.[241] These rules and regulations are made by national governments, based on the power they exercise overland through physical borders.[242]

However, regulating OSINT in civilian criminal investigations, by means of the proposed legal privacy protection, will not serve as a perfect solution *inter alia* due to the transboundary nature of OSINT and the Internet in general.

[241] In democratic societies that is.
[242] Joel R. Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory L.J. 911, 913 and 914.

To ensure proper privacy protection in the digital sphere, one needs to look at transnational regulatory options to ensure privacy protection in civilian criminal investigations using OSINT. This goes beyond the scope of this paper, but further researched on this topic is undoubtedly needed.

VIII. Closing Remarks

In a working democratic society, civil society involvement is necessary, both to aid and to counter the power of the government and point out abuses in society. The power in criminal investigations should therefore remain balanced.

In an ideal society, citizens would balance between reporting relevant information to the police, about other civilians or the state, publishing information independently themselves and leaving room for traditional law enforcement, in the appropriate moments. It is useful to keep this ideal in mind when drafting legislation on OSINT's use in investigations. Summarized accurately, 'citizen responsibility must be responsibly done'.[243]

[243] Gary T Marx, 'The Public as a Partner? Technology Can Make Us Auxiliaries as well as Vigilantes' (2013) 11 *IEEE Security & Privacy* 56, 60.