SECURITY AND HUMAN RIGHTS MONITOR

Open source intelligence and privacy dilemmas

Is it time to reassess state accountability?

Quirine Eijkman and Daan Weggemans

Quirine Eijkman (Phd) is a senior researcher / lecturer at the Centre for Terrorism and Counterterrorism (CTC), Leiden University-Campus the Hague. Email: q.a.m.eijkman@cdh.leidenuniv.nl.

Daan Weggemans (MSc.) is a researcher / lecturer at the Centre for Terrorism and Counterterrorism (CTC), Leiden University-Campus the Hague. Email: d.j.weggemans@cdh.leidenuniv.nl

DOI: 10.1163/18750230-99900033

Introduction

Providing for safety and security is a core task of the state. The rapid developmentof technology has, in many ways, affected the dynamics of this responsibility. Intelligence- and security agencies and the police increasingly rely on informationtechnology that facilitates the collection of Open Source Information (OSINF). OSINF forms the basis of Open Source Intelligence (OSINT), which is gathered through publicly available sources that are unclassified and include sources ranging from(foreign) newspapers, governmental reports, public data, maps, academic sites toblogs, social networking sites, apps and web-based communities.

With the evolution of the internet, a vast array of information has become retrievable with the click of a mouse. In addition to this accumulation of valuabledata, the internet also contains large quantities of personal information, often postedonline by people themselves through social networking sites, blogging or apps. Individuals regularly share personal information online, which is stored as digitaldata in databases or in the cloud. This, in turn, has led to new perceptions about how this personal data may be used for security and safety purposes. In many areasthe use of OSINF — e.g. the monitoring of different social networking sites, blogs or apps — is growing significantly. Several research centres and think tanks, both public and private, have been established solely with the aim to study, coordinate ordevelop new approaches to (the gathering of) OSINF and the acquiring of OSINT. Quoting one of the main themes of the '2010 Naked intelligence' conference; 'the gathering of knowledge in a see through world' has become a prominent aspect within the security and intelligence industry.[1]

New strategies for using OSINF are also designed to anticipate national security threats such as international terrorism. Although the chances are slim that aterrorist will post his or her selected target location online, these measures are helpful in monitoring violent extremist views. In 2012 this was confirmed by theDutch General Intelligence and Security Service (AIVD) 'Jihadism on the Web' report, in which the internet was labelled as the 'most important medium for the dissemination of these (jihadist) ideologies'.[2] Returning to the state's core task ofproviding safety and security for its citizens, we argue that gathering Open SourceInformation is a legitimate tool for security governance. As Ben Hayes stated, '(…)security services would be negligent if they didn't utilize information in the publicdomain to inform their work'.[3]

However, the legitimacy of the growing use of OSINF cannot be derived solely from the pursuit of security or safety concerns. (Side) effects for human rights should also be considered. In this article we therefore discuss challenges associated with the use of OSINF — mainly in relation to the freedom of internet andthe rights to privacy and data protection. From a human rights perspective, the gathering of OSINT demands proper checks and balances. This is especially important, when security — and intelligence agencies as well as private companies use and exchange information. In this article, we (re)assess the checks and balancesfor the use and sharing of open source intelligence by, and between, security — andintelligence agencies and law enforcement agencies. Even though laws, regulationsand policies in relation to OSINF may recognise the need for checks and balances including the value of the right to privacy, data protection or a fair trial, it is nevertheless important to review whether the gathering of OSINF online requires more (state) accountability. Henceforth, in this article we focus

1 The conference Naked Intelligence, 'Gathering Knowledge in a See Through World', origins from the collaboration of two private corporations in the field of Open Source intelligence production; Sandstone s.a. and Infosphere AB, 2010, Retrieved 27 January 2013, http://www.telestrategies.com/ni_10/index.htm.

2 General Dutch Intelligence and Security Service, 'Jihadism on the Web', 2012, p.3. Retrieved 27 July 2012, https://www.aivd.nl/@2872/jihadistisch.

3 B. Hayes, 'Spying in a see through world: The 'Open Source' Intelligence Industry', in *Statewatch Bulletin,* 2010, no. 1, p. 2.

on what dilemmasarise with the collection of open source information by security – and intelligenceagencies and to a lesser extent the police. We thus address the following questions:Have state accountability mechanisms been able to keep up with the rapidly increasing practice of open source information gathering and exchange? Are sufficient safeguards provided to protect human rights?

Open source information in context

After the 9/11 attacks the National Commission on Terrorist Attacks upon the United States recommended a greater role for OSINT within security agencies.[4] Thefollowing institutionalization of open source collection has been called 'one of themost high profile reforms (..) aimed at the preventing of terrorists attacks and avoiding intelligence failures'.[5] Meanwhile it is often stated that 'ninety percent ofintelligence comes from open sources'.[6]

The definition of open source information, which is at the base of this formof intelligence, is ambiguous. In this section we review some of the definitions and developments concerning the use of open sources for national – and public security purposes. Open source information is information that is publicly available.In other words; what is not 'confidential' and out there in the (digital) public domain. It is the information that anyone can 'lawfully obtain by request, purchase,or observation'.[7] Examples of open information sources include the media (e.g. radio, television, newspapers, websites, blogs), official (governmental) reports, academic sources (papers, conferences, seminars), commercial data and so called'gray literature' such as working papers, unofficial government documents and surveys.[8] In this article we focus on the increased availability of personal open source information on the World Wide Web ('www'). Not only online news pagesbut also 'weblogs', 'chat rooms', 'social networking sites' including Facebook, Twitter or Skype and 'apps' such as Whatsapp or WeChat, are perceived as potential valuable sources for intelligence - and security services and the police. Here, one can, through information technology find unique information about thelives of millions of (world) citizens.[9] Open Source Centre director Doan Naquinonce said 'We're looking at YouTube, which carries some unique and honest-to-goodness intelligence'.[10]

To acquire this Open Source Intelligence, OSINF (raw data) in the form of aninterview, a photograph, a tweet, etc. is 'analyzed, edited, filtered and validated'.Furthermore, the data is linked with different media sources (e.g. the internet, academic journals, official reports, newspapers, radio and television), in order to verify, complement and contextualize the collected information.[11] As is describedabove, an advantage of this data is

4 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 2004. Retrieved 25 August 2012, http://govinfo.library.unt.edu/911/report/index.htm

5 H. Bean (eds.), *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence*, Praeger, Santa Monica, CA, 2011, p. 12.

6 R.A. Best and A. Cumming, 'Open Source Intelligence (OSINT): Issues for Congress', Congressional Research Service, 2007, p. 7. Retrieved 2 July 2012, http://www.au.af.mil/au/awc/awcgate/crs/rl34270.pdf.

7 National Open Source Enterprice, Intelligence Community Directive 301, July 2006.

8 A. Sands, 'Integrating Open Sources into Transnational Threat Assessments', in J. Sims and B. Gerber (eds.), *Transforming US Intelligence,* Washington, D.C., 2005, pp.64-65.

9 For instance, Facebook had at the end of March 2012, 901 million active users. At the first quarter of 2012 an average of 3.2 billion likes and comments were generated by its users each day. See: Facebook, 'Key Facts', 2012. Retrieved 2 July 2012, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

10 D. Naquin, 'CIRA Newsletter, Remarks by Doug Naquin', in *CIRA Luncheon*, 2007, p.7. Retrieved 2 July 2012, http://www.fas.org/irp/eprint/naquin.pdf.

11 NATO, *NATO Open Source Intelligence Handbook,* 2001, p.2. Retrieved 4 July 2012, http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf.

that it has become widely available nowadays.Especially with the 'information explosion', which is the result of the rapid development of the internet, obtaining OSINF has become significantly cheaper.

Simultaneously, the frequent use of open sources by security – andintelligence and law enforcement agencies has been facilitated by legislation. TheDutch Intelligence and Security Services Act, for instance, states that first open sources need to be checked before any other methods can be applied.[12] Other countries, though sometimes implicitly, often demand similar approaches to information gathering.[13] In addition to the growth of available information, the number of public - and private organizations concerned with OSINF and OSINT haveincreased substantially. In the United States, the National Open Source Center (NOSC) was opened on 1 November 2005 with the goal to effectively collect available open source information. In Europe EUROSINT Forum was installed in 2007 to exchange knowledge and experiences between different professional OSINF analysts. Moreover, initiatives by universities, including the Open Source Intelligence Exchange at Fairmont State University, USA, or think thanks, such as Rand Cooperation, respond to the constant demand for new knowledge in this area.[14] But not only new public institutes, training courses or expertise were created. In addition, the increased outsourcing of information gathering, data mining and analyzing by private companies has been a major development withinthe security industry. This also affects intelligence gathering.[15] Various private entities are becoming more involved in national – and personal security. For instance, the privately funded company, the OSINT-Group was founded in 2007 and'utilizes in each case the best and most relevant sources to respond to established client needs with sensitive yet unique and important 'open source intelligence' rather than just 'information'.[16] Several other private companies like Stratfor, Infosphere AB and Sandstone AB have gained substantial OSINF-market shares as well.[17] Simultaneously, the rise of websites like Wikileaks or OpenLeaks,which facilitate the mass publication of classified information by whistleblowersfurther reflect this development.

Open source intelligence dilemmas

The benefits of OSINF are emphasized by security consultants, scientists, the mediaas well as the intelligence community. OSINF is cheap and more widely available than the traditional public information acquired by clandestine services. Moreover,it also provides extra information which sometimes cannot be gained by other intelligence sources (e.g. human intelligence). In addition, as a result of the wideavailability of (local) news coverage throughout the internet, the use of online opensources enables security – and intelligence agencies to be more up-to-date.[18] Simultaneously, online open sources may in times of crisis – e.g. a war – be a more reliable and safe way of acquiring intelligence than by polarized human intelligence. The large scale usage of (online) open sources has created new contexts and perspectives that assist intelligence – and security agencies to betterunderstand the complexity of certain security developments within local or nationalcontexts.

12 Wet op inlichtingen en Veiligheidsdiensten 2002 (The Intelligence and Security Services Act 2002), 2002. Retrieved 3 July 2012, http://www.st-ab.nl/wetten/0662_Wet_op_de_inlichtingen-_en_veiligheidsdiensten_2002.htm.

13 See for instance: The United Kingdom Intelligence Services Act 1994 or the Australian Intelligence Services Act 2001.

14 Hayes, p. 5 (see note 5 above)

15 S. Chesterman, 'We can't Spy… If we can't Buy!: The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'', in *The European Journal of International Law*, 2008, no. 5, p. 1057.

16 OSINT-Group, *Overview,* 2012. Retrieved 2 July 2012, http://www.theosintgroup.com/overview.html

17 Hayes, p. 3-5 (see note 5 above)

18 L. Pouchard, J. Dobson and J. Trien, 'A Framework for the Systematic Collection of Open Source Intelligence', 2009, p.1. Retrieved 29 July 2012, http://info.ornl.gov/sites/publications/files/Pub13152.pdf.

It enables intelligence – and security agencies to verify (classified) information with various open media sources and data. Finally, it has been arguedthat because in comparison to other sources online information is more widely available and less secretive, the use of OSINF for intelligence purposes has loweredthe threshold for sharing information between intelligence – and security agencies.[19]

Apart from information security, the (side) effects of the use of OSINF for security – and safety purposes have received little attention in the literature. In thissection we therefore introduce some dilemma's regarding data collecting, – processing, – mining and – sharing of open source information. Of course thereare many other dilemmas in relation to the use of OSINF by security – and intelligence agencies or the police. These include the construction of virtual personal identities by others[20] or the facilitation of more social control by the state.[21] In this article, however, we focus primarily on the collecting, processing, mining and sharing of open source information retrieved from social networking sites, blogs or apps.

Collection

Whether the wider range of available digital information will be considered a blessing or a curse remains to be seen. As a result of an information overload, theneed of intelligence – and security agencies and the police to be more critical about information has become more evident. As Hamilton Bean states 'the amountof available, and potentially useful, information for analysts to consider (…) (is) increasing to nearly unmanageable levels'.[22] The search of intelligence analysts inthe information jungle called the internet has become more difficult and requiresnew skills from open source analysts. This kind of expertise needs to be developedby intelligence – and security agencies and the police.[23]

A second obstacle is the multiplication of individual sources. This so called 'echo' effect occurs when a news-item that appears in one source (e.g. a website) is spread among a considerable number of other media sources.[24] The risk arises when a story is framed in differing ways by a variety of sources of which many only reflect a certain part of the story, sometimes in different ways. This may mislead OSINF analysts. Consider, for example, a two minute lasting YouTube filmof one man hitting another man on a street. A second film of the incident, which forthe sake of the argument lasted five minutes, showed that the man, who was hit onthe head, had kicked his girlfriend numerous times and subsequently she had begged for help, had not been posted online but was recorded by someone else on amobile phone. If journalists were to write about this incident, they would probablyfind the YouTube film and several references on social networking sites and maybe tempted to conclude that the first man was at fault. In turn this creates a reality ofits own and the echo effect could lead to the first man being labelled as the 'villain',whereas in reality the second man carries primary responsibility for the turn of events.

19 M.D. Cross, 'EU Intelligence Sharing & The Joint Situation Centre: A Glass Half-Full', *Meeting of the European Union Studies Association,* 2011, p.10. Retrieved 25 July 2012, http://www.euce.org/eusa/2011/papers/3a_cross.pdf.

20 E. Morozov, *The Net Revolution: How not to liberate the world,* London, 2010.

21 M. Hildebrandt, B. Koops and K. De Vries, 'Where Idem-Identity meets Ipse-Identity. Conceptual Explorations', in *Future of Identity in the Information Society,* 2008. Retrieved 26 July2012 http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP7-del7.14a-idem_meets_ipse_conceptual_explorations.pdf.

22 Bean, p.7 (see note 7 above)

23 See e,g, H. Minas, 'Can the open source intelligence emerge as an indispensible discipline for the intelligence community in the 21st century?', *Research Institute for European and American Studies*, 2010.

24 Best and Cumming, p.7 (see note 8 above)

Personal data: Processing, sharing, mining and storage

Further dilemmas arise with the collection, processing and storage of intelligenceby security – and intelligence agencies and the police. In 2009 the American Federal Bureau of Investigation (FBI) invested in a private company that specializedin monitoring social networking sites.[25] Similar developments have been reported about Europol.[26] It is not widely known that information from social networking sites is being gathered and monitored by intelligence - and security agencies and shared among national - and international actors, but there are many incidents that suggest this is the case. For example, when in 2012 two British tourists were detained and deported for tweeting that they were going to 'destroy America' during their holiday[27], it became clear that Twitter accounts were monitored.[28] Inthe same year Saudi journalist Hamza Kashgaru[29] was deported from Malaysia. With alleged support of Interpol he had been located there after he fled Saudi Arabia due to an 'insulting' tweet about the Prophet Muhammed.[30] A further expansion of this monitoring of social networking sites was indicated by an article in February 2012 that proclaimed the 'US seeks to mine social media to predict future'. More specifically, the development of new software was discussed which enables security - and intelligence agencies to mine informationof social networking sites.[31] In a response, Open Source Centre director Patrick O'Neill stated that 'we need to see social media as intelligence gathering very similar to spying'.[32]

An important dilemma with the processing of the information that is collectedfrom the social media relates to the storage of large datasets that contain quantitiesof digital personal information. Subsequently, 'data analysis tools (are used) to discover previously unknown, valid patterns and relationships'.[33] Data mining tools in relation to collected information from e.g. social networking sites can be used bylaw enforcement and security – and intelligence agencies to develop risk profilesand label individuals as potential security risks. For most people this profiling takesplace without the data subject even knowing that he or she is being profiled.[34] Thisdevelopment has led to significant concerns about privacy and data-protection aswell as the right to a fair trial. What if an angry ex-girlfriend posts a Facebook message that her former boyfriend is a 'hi-tech terrorist' and he is subsequently barred from entering the USA; Will he ever find out why?

---

25 N. Shachtman, 'Exclusive: U.S. spies buy stake in firm that monitors blogs, tweets', 2009. Retrieved 29 July 2012, http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm.

26 European Parliament, 'Parliamentary Questions, Subject: Wikileaks Global Intelligence files, Generalised data mining by the US and EU, profiling EU citizens', 2012. Retrieved 25 July 2012, http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2012-002428&format=XML&language=EN#def4.

27 Huffingtonpost, 'British Tourists Detained, Deported For Tweeting 'Destroy America'', 2012. Retrieved 2 July 2012, http://www.huffingtonpost.com/2012/01/30/british-tourists-deported-for-tweeting_n_1242073.html.

28 M. Hosenball, 'Homeland Security Watches Twitter, social media', 2012. Retrieved 10 August 2012, http://www.reuters.com/article/2012/01/11/us-usa-homelandsecurity-websites-idUSTRE80A1RC20120111 ; For other examples please see Huffingtonpost (2010),'Arrested over Twitter: 8 Tweets that got people BUSTED', 25 august 2010. Retrieved on 20 August 2010 via http://www.huffingtonpost.com/2010/08/25/arrested-over-twitter-8-t_n_693866.html#s130765&title=Man_Arrested_Fined

29 Not his real name.

30 Al Jazeera, *Malaysia arrests Saudi blogger over tweets*, 2012. Retrieved 5 February 2009, http://www.aljazeera.com/news/asia-pacific/2012/02/20122105349670993.html.

31 M. Wohlsen, 'US seeks to mine social media to predict future', *Associated Press*, 2012. Retrieved 1 December 2012, http://www.news.com.au/technology/us-seeks-to-mine-social-media-to-predict-future/story-e6frfro0-1226269477144.

32 P. O'Neill, 'Spies give way to 'sexy' social media', *Federal News Radio,* 2012.

33 J.W. Seifert,'Data mining and Homeland Security: An overview. CRS Report for Research', *Congressional Research Service*, 2007.

34 *Cf.* Hildebrandt *et al.,* p.24 (see note 23 above); Pouchard *et al.*, p.2 (see note 19 above)

By stating 'just because data is accessible doesn't mean that using it is ethical' Dana Boyd raises one of the major concerns regarding large scalepersonal data storage.[35] Consider, for example, a youngster who has expressed radical views about animal rights online and is confronted with this information ten years later during a job interview for an administrative position in a toy store.Would it be considered ethical if the employer asked her about it? Points of viewmay differ about this: What is in 'the public domain' has been redefined to 'accessible and available for any purpose under any circumstance'. According toBoyd we have 'stripped content out of context, labelled it data, and justified our actions by the fact that we had access to it in the first place'.[36]

People who are concerned with privacy and data protection in relation to data mining of open source information are not afraid, at least initially, of the lossof ownership over their – digital – personal data. They are primarily concerned that their data is disconnected from the context in which they intended it to be. Toquote Helen Nissenbaum[37], 'privacy is about expectations about the environment,and the norms that accompany this environment, in which your information is shared'. When people share information (e.g. about their health), they share it witha certain audience of people (a doctor), within a certain environment (the hospital)where certain norms apply (e.g. doctor-patient confidentiality). Different to this example is the environment of social networking sites, which deceivingly appearto be for a selected audience. In reality sites like these are often fully transparent with many people listing and reproducing your pursuits. We want to upgrade ourstatuses and 'like' certain pictures on Facebook so others can see who we are, butthis information is usually only intended for a specific audience. Boyd therefore stresses rightly that 'Making content publicly accessible is not equal to asking forit to be distributed, aggregated, or otherwise scaled'.[38] The data mining of social networking sites for security and intelligence purposes is therefore a violation of privacy.

In addition, the Council of Europe highlighted the risks of automatic data processing profiling.[39] When data for someone is produced based on the data of others, the data subject 'a priori cannot suspect the existence of correlation processes that might result in certain characteristics of other individuals being attributed to him or her on the basis of a probability calculation'.[40] For instance, when a certain person has been detained at an airport and deported because of hisalleged violent radical views. Other people who perhaps have updated their Facebook statuses with words that relate to the profile of the deported radical, may subsequently be treated differently by customs and border control or be blacklisted as risk passengers, which, in reality, does not correspond to their actual 'threat level'. In other words, in addition to its benefits, profiling also dilutes valuable information concerning implicit personal characteristics that may be crucial for detecting potential violent extremist. Stories and lives, which take place outside the realm of social networking sites are not taken into account and this may lead to the profiling of persons who in reality are no threat (false positives) - e.g. the case of the British tourists - or not identifying those who actually pose a threat (false negatives).

35 D. Boyd, 'Privacy and Publicity in the Context of Big Data', 2010. Retrieved 27 July 2012, http://www.danah.org/papers/talks/2010/WWW2010.html.

36 Boyd (see note 37 above)

37 H. Nissenbaum, 'Privacy as Contextual Integrity', in *Washington Law Review,* 2004, no. 1, pp. 101-139.

38 Boyd (see note 37 above)

39 Council of Europe, *The Protection of Individuals with Regard to Automatic Processing of Personal data in the Context of Profiling, Recommendation CM/REC(2010)13 and explanatory memorandum,* 2010, pp.28-32.

40 *Ibid.*

Hildebrandt, Koops and De Vries[41] also focus on the side effects ofprofiling. They state that the process of identity construction might be affected byprofiling based on data mining techniques. Accordingly, profiling may lead to a different treatment that could affect real-life opportunities. When people are unaware of being profiled or where their personal data is stored, they may changetheir behaviour after experiencing the negative consequences of this profiling. Thiscan be considered a privacy violation; at least when privacy is defined as the 'freedom from unreasonable constraints on the construction of one's identity'.[42]

Open source accountability

Open source information has increased the range of security tools at the disposal ofsecurity – and intelligence officials or police officers. Nonetheless, the side effectsof this new method of intelligence gathering should be balanced by a form of accountability, which is sufficient both in theory and in practice. To illustrate, in most Western societies there is strict legislation for phone – or internet tapping, however for social networking sites or apps this is less evident. Furthermore, manysecurity officials probably do not see the need for more accountability for OSINT.They may argue, for example, that social networking sites are part of the public domain and that therefore anyone is able to access it. Henceforth what is the issuewith monitoring by public – or private security analysts? And, why should they keep track of what kind of information they collect? The difference, however, between just anyone and a security official is that OSINT can indirectly or directlyaffect someone's private life or future opportunities. As mentioned before, the useof OSINF for intelligence purposes has real life consequences. From a human rightsperceptive these side effects should be balanced. Henceforth, state accountabilityfor the use of OSINF is reviewed in this section.

As a concept accountability has a normative aspect intertwined with notionsof justice, responsibility, integrity, fairness and democracy.[43] Simultaneously accountability is concrete and 'value free' and focuses on the 'obligations to evidence management or performance imposed by law, agreement or regulation'.[444]Blind distinguishes between 'accountability as the philosophy of government' andaccountability as the 'means' of government.[45] In this article we recognize this difference and differentiate between the process through which politicians or heads of security – and intelligence agencies or the police inform society about their plans and actions in terms of open source collection and justify the need to doso, while the actual behaviour of officials and the outcome analyses by security –and intelligence agencies or the police are subject to review or sanctions.[46] This aforementioned form of accountability is characterised by its focus on the ruleof law and good governance, as well as the inclusion of civil society or ordinary people.[47] It could imply that the head of a security – and intelligence agency, or those politically responsible, not only publically announce the purpose of collection,

41 Hildebrandt *et al.*, p.8 (see note 23 above)

42 P.E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape,*

Cambridge, Massachusetts, 2001, p.7.

43 P.K. Blind, 'Accountability in Public Service Delivery: A multidisciplinary review of the concept', *Expert Group Meeting Engaging Citizens to Enhance Public Sector Accountability and Prevent Corruption in the Delivery of Public Services*, Vienna, 2011. Retrieved 21 August 2012, http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan046363.pdf.

44 E.L. Kohler, *A Dictionary for Accountants,* New Jersey, 1975.

45 Blind, p.4 (see note 45 above)

46 J.M. Ackerman, 'Social Accountability in the Public Sector: A conceptual discussion', in *Social Development Papers: Participation and Civic Engagement*, 2005, no. 82, p.6. Retrieved 26 August 2012, http://siteresources.worldbank.org/INTPCENG/214574-1116506074750/20542263/FINALAckerman.pdf.

47 Blind (see note 45 above); Ackerman (see note 46 above)

processing, mining or sharing of OSINF, but also limit its use to predefined threats such as national security (e.g. for cyber espionage, internationalterrorism). Furthermore, international — and/or national law makers should determine what the boundaries are (the rule of law) and how data subjects can seekreaddress (internal — or external accountability mechanisms). Finally, the design ofsoftware that enables OSINT and simultaneously emphasizes accountability (data protection by design) should be modified accordingly. This includes privacy-enhancing-technologies (PET's) or transparency-enhancing-technologies (TET's).[48] These measures may be considered as a form of good governance in relation to balancing the security officials' use of OSINT.

Apart from the necessity to protect national security interests, which may interfere with transparency efforts, there are other accountability dilemmas in relation to OSINF. Ensuring accountability is more complex if the information is notcollected by the security agency itself, but by other public — or private entities. It isnot uncommon for intelligences and security agencies to share information on an(inter-)national level and since 9/11 it has become more common for law enforcement agencies to do so as well. This is a recent development because 'traditionally a distinction exists between collecting intelligence for national security purposes and gathering evidence for criminal investigations, as they servedifferent purposes'.[49] Security — and intelligence agencies prefer to keep their sources confidential, whereas law enforcement agencies ultimately have to share the case file with the defence council. Nonetheless, OSINT used by intelligence —and security agencies is also collected and processed by other state agencies and sometimes shared with international partners and this has affected accountability inpractise. Consider for instance whether security analysts know what the original source of a piece of information containing personal data was, let alone if those affected may ever have the opportunity to access or correct it. What if the personal data is used by the security analyst's agency for a security clearance investigation of refugees?

Likewise OSINF and OSINT are also collected by private companies. As is discussed above, there has been a major growth in private companies involved inthe collection of OSINF and the acquiring of OSINT. The Wikileaks Global Intelligence Files, for example, reflect how the company Stratfor provides intelligence to public and private entities including the US Defense Intelligence Agency.[50] One of the released 5.5 million hacked Stratfor emails reveals the existence, a predictive software system TrapWire of TrapWire Inc. that combinesCCTV images and number plate recognition (ANPR) collected in the public domainof two America cities.[51] Another multinational security company Raytheon has developed a riot program that mines social networking sites and on the basis of theoutcome is able to track people at their location.[52] Evidently, private entities are able to sell or share the software or the open source information with security — and intelligence agencies or the police, who probably

48 M. Hildebrandt, 'Privacy Enhancing Technologies', *Hide Project, Pets 2nd Focus Group,* 2011. Retrieved 26 August 2012, http://ebookbrowse.com/hide-fg-privacy-enhancing- technologies-minutes-20091016-pdf-d113363089; J.J.F.M. Borking, *'Privacyrecht is een Code: Over het gebruik van Privacy Enhancing Technologies'* (Privacy is a Code: About the use of Privacy Enhancing Technologies), Deventer, 2010.

49 Q.A.M. Eijkman and B. van Ginkel, 'Compatible or Incompatible: Intelligence and human rights in terrorist trials', in *Amsterdam Law Forum,* 2011, no. 4, p.4.

50 Wikileaks, 'Stratfor Emails: Wikileaks impact is Stratfor's bottom line', *The Global Intelligence Files,* 2012a. Retrieved 1 March 2012, http://wikileaks.org/WikiLeaks-Impact-is-Stratfor-s.html.

51 Parent company Cubic Cooperation. Previously owned by Abraxas Applications, who had created it under Abraxas Applications Inc.. It is a private company that employs several former public officials of the Central Intelligence Agency (CIA) and other agencies. See: RT, 'TrapWire Tied to Anti-Occupy Internet-spy-program', 2012. Retrieved 28 August 2012, http://rt.com/usa/news/trapwire-abraxas-cubic-surveillance-251/; C. Arthur, 'Trapwire surveillance system exposed in document leak', in *The Guardian Online*, 2012. Retrieved 13 August 2012, http://www.guardian.co.uk/world/2012/aug/13/trapwire-surveillance-system-exposed-leak.

52 R. Gallagher, 'Software that tracks people on social media created by defense firm', in *The Guardian Online*, 2012. Retrieved 10 February 2013, http://m.guardian.co.uk/world/2013/feb/10/software-tracks-social-media-defence.

use it for investigation purposes.[53] These developments take place, while questions of accountability forthe use of the personal data stored on social networking sites remain unaddressed.As Ben Hayes concludes 'we must (then) develop the tools and communities needed to bring them under democratic control'.[54]

In response to these developments, civil society is in the best position to hold the state accountable. Regarding the use of open social networking one of thechallenges in terms of holding security officials or their agencies accountable is thatin most cases the data subject has no idea that their online behaviour has been monitored. When this monitoring leads to differential treatment accountability issues become more realistic. But who will issue a complaint? Consider if you arenot aware that your 'denial of an opportunity' is the result of a private company oran intelligence agency keeping track of your digital pursuits? To some extent civilsociety can hold security agencies accountable by blogging, writing reports, informing the public or petitioning to public authorities. Nonetheless, OSINT is a growing business and challenging to monitor for outsiders. Subsequently, some take more drastic steps such as hacking (governmental) websites or developing encryption software programs to communicate 'without anyone watching'.

Reflections

In this article we argue that the increased use of Open Source Information (OSINF)and Open Source Intelligence (OSINT) for safety and security purpose needs to bebalanced by assessing what state accountability in a digital world should entail. Even though security – and intelligence agencies and the police are tempted to increase their use of social networking sites, tweets, blogs or apps, state accountability mechanisms have struggled to adapt to the online open source culture. Consider for instance the dilemma that intelligence is frequently collected,processed, minded and stored by external entities including foreign security – andintelligence agencies or private companies. Subsequently, it is reasonable to assume that the security officials or analysts, who are the end-users, are oblivious to the original source or its specific context. The use of OSINT requires, despite the fact that ordinary people are usually unaware of being profiled or where or how their digital personal data is stored in data bases or 'the cloud', that the public at large begins to ask more questions. The most important reason being thatdespite the safety and security benefits, this information may have real-life consequences.

State accountability for OSINT should at least require that it is used on the basis of a law. Furthermore politicians, heads of security agencies or security officials should proactively inform society about their plans and actions in relationto OSINF and justify the need to acquire OSINT. This should preferably happen online and also, if possible, at the – public – entity where the data subjects are confronted with the outcome. Even though the security official, who collects information about a person who potentially poses a threat, may be aware that thisparticular information needs to be verified, it is reasonable to assume that in real life no risks are taken.

Furthermore, state accountability should entail that the actual process and outcome of data collection, – processing, – mining and – sharing is subjected toreview or sanctions. In practice, however, this is challenging: Which entity or whocarries the responsibility? And, what about accountability? On an individual level:Is it the analyst, the risk profiler, the executive security official etc.? Is individualaccountability in this context realistic

53 Public Intelligence, 'Unraveling TrapWire: The CIA-connected global suspicious activity surveillance system', 2012. Retrieved 29 August 2012, http://publicintelligence.net/unravelling-trapwire ; Wikileaks, 'Stratfor Emails', *Wikileaks: The Global Intelligence Files,* 2012b. Retrieved 9 August 2012, http://www.wikileaks.org/gifiles/releasedate/2012-08- 09.html.

54 Hayes, p.8 (see note 5 above)

or is it simply a matter that when everybody,the whole chain of security officials who collect, mind, process and store data, isresponsible, nobody is accountable? Formally those entities who collect and storeOSINT are accountable, but in practice it is unlikely that a data subject will ever haveaccess or correct information (probably for security reasons). Therefore before anyform of new state accountability mechanism is considered, an informed public –and political debate about the desirability of OSINF accountability by the state should take place. The use of OSINT for safety and security purposes is a reality, but(re)assessing state accountability is necessary for its legitimate use by security –and intelligence agencies and the police.

This article was first published with Brill | Nijhoff publishers, and was featured on the Security and Human Rights Monitor (SHRM) website.

Security and Human Rights (formerly Helsinki Monitor) is a journal devoted to issues inspired by the work and principles of the Organization for Security and Cooperation in Europe (OSCE). It looks at the challenge of building security through cooperation across the northern hemisphere, from Vancouver to Vladivostok, as well as how this experience can be applied to other parts of the world. It aims to stimulate thinking on the question of protecting and promoting human rights in a world faced with serious threats to security.

Netherlands Helsinki Committee
Het Nutshuis
Riviervismarkt 4
2513 AM The Hague
The Netherlands

www.nhc.nl