The Ethics of Open Source Intelligence Applied by Maritime law Enforcement Authorities

Jyri Rajamäki, Sari Sarlio-Siintola and Jussi Simola
Laurea University of Applied Sciences, Espoo, Finland
jyri.rajamaki@laurea.fi
sari.sarlio@laurea.fi
simolajussi@gmail.com

Abstract: The MARISA Horizon 2020 project improves maritime security communities' information exchange, situational awareness, decision-making and reaction capabilities with a data fusion toolkit based on various heterogeneous and homogeneous data and information. Open source intelligence (OSINT) is intelligence collected from publicly available sources, including the internet, newspapers, radio, television, government reports and professional and academic literature. Social media intelligence (SOCMINT) can be defined as the analytical exploitation of information available on social media networks. It identifies social media content as an opportunity and challenge for open source investigations. This paper provides qualitative analysis of ethics in maritime surveillance. Ethical issues concerning OSINT, SOCMINT and big data are diverse and evolving. Their impact on MARISA concerns both technology, user processes and the business/governance model. Even though international regulatory guidelines are available, specific allowances, prohibitions and exceptions mainly stem from national legislation. European Data Protection Reform (EDPR) partly harmonizes the data protection regulation in EU countries (DPA), but still leaves the possibility for variation at the national level (DPD). One big challenge is coping with the mosaic effect. Data protection sets strong requirements for MARISA technology, utilizing various data sources and performing data fusions on various levels. Another big challenge concerns the reliance on automated analysis: How can data fusion algorithms which are reliable and transparent for the end user be developed? Combined with OSINT, big data is able to map behaviour and tendencies. However, data science is needed in OSINT because of the lack/low quality of big data, to find the correct answers, capture the correct data and to have the correct perception of how to proceed throughout the process. In the context of big data, it is also notable that current academic and public debates entertain the notion of shifting the emphasis from data collection to data analytics and data use. There are scholars who underline the need for "algorithmic accountability". It can therefore be expected that the legal requirements concerning personal data processing and big data may develop in this direction. Therefore, to separate the ethics of data collection from the ethics of processing and use is essential.

Keywords: ethics of OSINT, ethics of law enforcement, ethics of surveillance, open source intelligence, maritime surveillance, social media intelligence

1. Introduction

The ongoing MARISA Horizon 2020 project focuses on four major objectives: (1) to create improved situational awareness with a focus on delivering a complete and useful comprehension of the situation at sea; (2) to support practitioners throughout the complete lifecycle of situations at sea, from the observation of elements in the environment to the detection of anomalies and aids to planning; (3) to encourage fruitful collaboration between adjacent and cross-border agencies operating in the maritime surveillance sphere (navy, coast guard, customs, border police) in order to pull resources towards the same goal, leading to cost-efficient use of existing resources; and (4) to foster a dynamic eco-system of users and providers, allowing for new data fusion services, based on "distilled" knowledge, to be delivered to different actors at sea by the integration of a wide range of data and sensors (MARISA, 2018). Among maritime security communities, Marisa improves information exchange, situational awareness, decision-making and reaction capabilities with a data fusion toolkit based on various heterogeneous and homogeneous data and information. The toolkit fuses information and data from different sources into knowledge, capitalizing on the large amount of unexploited maritime data. It extends this information fusion to other data streams beyond maritime data, such as the open source intelligence (OSINT) coming from social networks and the Internet whilst leaving users fully in control of selecting whether or not to include such data streams (MARISA, 2018). The MARISA solution provides a mechanism to get insights from any big data source, perform analysis of a variety of data based on geographical and spatial presentation, use techniques to search for typical and new patterns that identify possible connections between events, and explore predictive analysis with models to represent the effect of the relationships of observed objects at sea. Enterprise and *ad hoc* reporting and services, within the CISE (European Commission, 2018) context, will be provided to support users and operational systems in their daily activities, as well as presentation tools for navigating and visualizing the results of data fusion processing.

Open source intelligence (OSINT) is based on publicly available information, both offline and online. Open source information (OSINF) has increased the range of security tools at the disposal of security. However, the side effects of this method of intelligence gathering should be balanced by a form of accountability. Most Western societies have strict legislation concerning phone tapping, but for social networking sites or apps this is less evident. Many security officials do not see a need for more accountability for OSINT because they see social media sites as a part of the public domain and so anyone is able to access it. The difference, however, between just anyone and a security official is that OSINT can indirectly or directly affect someone's private life or future opportunities and the use of OSINF for intelligence purposes has real life consequences. From a human rights perceptive, these side effects should be balanced (Eijkman & Weggemans, 2012).

The purpose of this paper is to assist MARISA developers, maritime surveillance decision-makers and end users, and also provide business models of MARISA to identify and to take into consideration legal, ethical and societal dimensions of the MARISA OSINT solution. The aim is to support the ethical sustainability of future MARISA solutions aimed at reducing harm from illegal activities and for the benefit of less human suffering and saved lives. This paper provides qualitative analysis of ethics and ethical issues concerning OSINT, SOCMINT and big data in maritime surveillance. The impact of these technologies on MARISA concern both technology, user processes and business/governance models. The rest of the paper is organized as follows. Tables 1–6 present summaries of the results of qualitative analysis. Section 2 addresses the matter at hand of the ethical challenges in law enforcement and maritime surveillance. Section 3 focuses on open source intelligence (OSINT), social media intelligence (SOCMINT) and big data applied by maritime law enforcement authorities from an ethical perspective. Section 4 offers discussion and concludes the paper.

2. The ethical challenges in maritime surveillance

The ethics of law enforcement in general have been discussed extensively in academia and in various reports and statements, both from the philosophical viewpoint as well as from a more practical point of view, especially concerning privacy and its trade off with security, freedom and other related human rights. Privacy and data protection are of special concern when, for example, using drones and surveillance cameras, with automated border control, and when collecting and analysing big data. In addition, the impact of new surveillance technologies on the fundamental rights of asylum seekers and refugees as well as the increased responsibility this more effective situational awareness brings (under international refugee law and the Search and Rescue regime: duty to render assistance) have all been debated by numerous scholars, see e.g. (Meijers Committee, 2012).

Many of the ethical/societal challenges and opportunities of MARISA are those of maritime surveillance in general and discussed above. However, MARISA's capacities for maritime surveillance, and especially border control, emphasizes the importance of taking these challenges and opportunities more seriously. The biggest ethical challenge concerns the use of MARISA in border control. This is related to the tensions between humanitarianism and security, and the human rights of both EU citizens and migrants. Furthermore, it is a challenge that may have various unwanted consequences, such as the balloon effect, or even tensions in international relationships.

At its meeting in June 2014, the European Council agreed on five priority areas to guide the EU's work over the next five years. This strategic agenda will be used to plan the work of the European Council and also acts as a basis for the work programs of other EU institutions. From the viewpoint of MARISA and maritime surveillance, two priority areas are of particular relevance, namely, "Freedom, Security and Justice" and "The EU as a strong global actor" (see Table 1). The first is relevant when talking about the ethics and societal sustainability of MARISA in a European context (e.g. border control and migration). The latter, especially pertinent since MARISA also aims for businesses outside the EU, and thus "The EU as strong global actor" asks for solid societal consideration of MARISA and its impacts on societies.

In order to resolve the question presented above, i.e. the tension between humanitarianism and security, and the human rights, and, in addition, the EU's Charter of Fundamental Rights can be used as tool in MARISA since it brings together, in a single document, the protection of fundamental rights protected in the EU. The Charter can also be used as an important tool in value creation since when MARISA solutions are aligned with ethical requirements, their value is on a solid foundation. The Charter was established in 2000 and became legally binding on EU Member States when it was ratified at the Treaty of Lisbon in December 2009. According to the

Societal Impact Expert Working Group Report (SIEWG, 2012), these fundamental rights should be a necessary requirement that could and should lead to drawing boundaries on what is and what is not acceptable in EC-funded security research initiatives. The EU Charter of Fundamental Rights is consistent with the European Convention on Human Rights adopted in the framework of the Council of Europe; when the Charter contains rights that stem from this convention, their meaning and scope are the same.

Table 1: EC priority areas and MARISA surveillance

Priority area	Contents	Maritime Surveillance Aspects
Freedom, security and justice *“The European Council emphasises the importance of good EU cooperation on security issues like terrorism and managing migration flows.”*	*better management of all aspects of migration, including irregular migration, asylum and border management* *preventing and combating organised crime, corruption and terrorism* *improving judicial cooperation between EU countries*	Privacy is strongly associated with freedom, and a society where every movement and action is recorded is considered contrary to this idea of freedom. In the context of maritime surveillance, it is important to protect the principle of “freedom of navigation”. Increased control and security measures are justified with the need to protect Europe against cross-border crime, such as illegal trafficking and smuggling. The European maritime border is, however, not only a security issue for the EU but also for those seeking to enter Europe by sea. Protecting Europe’s seas and borders should be aimed at both creating a secure maritime environment but also protecting the lives and physical and moral integrity of those who travel at sea.
EU as a strong global actor *“The European Council calls on the EU to ensure its strong engagement in world affairs.”*	*ensuring consistency between Member States' and the EU’s foreign policy goals* *promoting stability, prosperity and democracy in the countries closest to the EU* *engaging global partners on a wide range of issues such as trade, cyber security, human rights and crisis management”*	In the context of maritime surveillance, the lack of accountability and clear lines of responsibility between EU Member States and their different actors is a persistent problem. Furthermore, the diverging interpretations of rules of international law hinder the cooperation between Member States in maritime surveillance. Maritime surveillance is based on coordination and information sharing between Member States. Therefore, it has the potential to create a mutual control mechanism between the participating agents, with regard to both fundamental human rights and refugee law and rescue obligations.

3. Ethical framework for OSINT, SOCMINT and big data in maritime surveillance

In this section, we will investigate OSINT, SOCMINT and big data from the ethical and legal perspectives. Achievements in the earlier projects VIRTUOSO and MEDI@4SEC are discussed here. VIRTUOSO (Koops;Cuijpers;& Schellekens, 2011) and MEDI@4SEC (Hadjimatheou & Roosendaal, 2016) offer practical tools and frameworks to be adapted with minor updates in the MARISA context, namely privacy enhancing technologies (PET), a legal and ethical framework for OSINT, and ethical and legal challenges for SOCMINT.

3.1 OSINT

OSINT is intelligence collected from publicly available sources, including the internet, newspapers, radio, television, government reports and professional and academic literature (Glassman & Kang, 2012). OSINT binds through a systematic analysis process as a tight and informative thematic entity, the scattered information to be obtained from open sources. During the last few years, the internet and especially social media channels have revolutionized the ones that had significantly increased the amount of OSINT and information to be analysed.

OSINT has also been called ethical hacking, in other words, hacking that does not break the law and it is used for good from psychological or physical manipulation for getting information. OSINT requires knowledge of the network environment with a good performer, a comprehensive means selection and problem-solving skills. Ethical questions apply to the handling of the collected information. When collecting data from people, one must remember that the creation of person registers is strictly regulated.

On the market there are numerous efficient network analysis tools, some of which are also used by the LEAs. Wells and Gibson have studied OSINT from a UK perspective and considered the law enforcement and military domains. Their conclusion was that the UK police and military open source investigations have a great number of similarities. However, there are several observable differences: (1) the handling of a chain of evidence; police forces prioritise and integrate a chain of custody for any intelligence that may lead to prosecution in a court of law and therefore the police tend to have a more structured and detailed approach to evidence gathering; (2) the use of third party software and developers; the military prioritises the use of bespoke software tools and in-house training solutions, where the police have rationally used a variety of commercial and private sector solutions, some of which are specifically designed for police OSIN; and (3) the approach towards the dark web; the military has a far more cautious approach to operating on the dark web, whereas the police have faced both pressure and a necessity to operate in this domain due to policing-specific concerns, such as online child sexual exploitation (Wells & Gibson, 2017).

The International and EU regulation of OSINT includes the regulations and conventions named in Table 2 (right column). However, even though international regulatory guidelines are available, specific allowances, prohibitions and exceptions mainly stem from national legislation (Koops, 2013; Koops, Hoepman & Leenes, 2013). The European Data Protection Reform partly harmonizes the general data protection regulation in EU countries (General Data Protection Regulation), but in the case of law enforcement and crime prevention it still offers variation in the national level legislation (Data Protection Directive).

Hu (2016) identifies five key concerns relating to OSINT that are gathered in Table 2 (left column) together with corresponding regulation (right column). The first question in relation to open sources is the following: How trustworthy are they? Also, the line between espionage and OSINT can be very thin, therefore caution and double-checking are advised before conducting OSINT activities (Hribar, Podbregar & Ivanusa, 2014).

Table 2: Summary of legal and ethical framework for OSINT

Key concerns about OSINT	International and EU regulation of OSINT
Origin and intent of sources Unclassified but sensitive Mosaic effect Reliance on automated analysis Publicity and visibility	European Fundamental Rights European Convention on Human Rights Cybercrime Convention EU Data Protection Regulation IPR legislation Liability Regulation of investigative agencies

The main ethical challenges for OSINT in MARISA are similar to the challenges identified in the VIRTUOSO project, excluding data protection which is just changing. Therefore, we propose that MARISA applies the recommendations provided by the VIRTUOSO project concerning intellectual property rights and safeguards with end use (see Table 3).

3.2 SOCMINT

SOCMINT can be defined as the analytical exploitation of information available on social media networks. It identifies social media content as an opportunity and challenge for open source investigations (Trottier, 2015). According to some scholars, the surveillance of social media should be removed from the definition and discussion about OSINT and treated as an issue in its own right (Wood, 2016).

The concerns that Hu (2016) identifies relating to OSINT are also relevant to SOCMINT. However, the ability to monitor millions of social media accounts and hashtags in real time, and to then analyse and store this data, is a concern unique to social media. According to Wood (2016), we need to challenge the argument that SOCMINT is an inexpensive strategy with little impact on people's privacy because it relies only on so-called publicly available (i.e. non-private) information. Social media does not easily fit into either the category of public or private. We would argue that it is instead a pseudo-private space where there is an expectation of privacy from the state (Wood, 2016). The grey zone is a space of transition where legitimate and legal methods pass into illegitimate and illegal methods, but are neither specifically allowed nor specifically forbidden; and the ethics and morality of these methods are questionable (Podbregar, 2016).

The MEDI@4SEC (Hadjimatheou & Roosendaal, 2016) project identifies legal and ethical issues concerning SOCMINT both from the viewpoint of the police use of social media and from the viewpoint of the involvement of citizens in the provision of public security. These viewpoints are summarized in Table 4. When it comes to the use of SOCMINT, a framework for the analysis of social media use (Table 5) developed in the MEDI@4SEC project seems to be suitable for MARISA, at least in the early stage of the project.

Table 3: OSINT recommendations by VIRTUOSO

OSINT recommendations
1. Deploy complete transparency about VIRTUOSO on its publicly accessible website, including substantiation of the need, purpose, proportionality, and subsidiarity of the project, and about its efforts to apply privacy/security by design.
2. Make a clear division between the tasks and responsibilities of the platform developer and provider with respect to content, and those of application providers and end users.
3. Specify the purpose(s) of the prototype.
4. Determine who is the data controller within the project and notify the relevant Data Protection Authority.
5. Substantiate why prototype testing requires real-life data. If using real-life data is necessary, personal data should be anonymised or irreversibly pseudonymised as soon as they are recognised as personal data. Personal data that cannot be anonymised (e.g. photographs and indirectly identifying personal characteristics) should be stored only for as long as is strictly necessary for testing the prototype.
6. Limit the processing of photos and video in view of the prohibition to process sensitive data.
7. Respect stipulations of access restrictions in robots.txt files or in meta-information of websites.
8. Be aware of national differences in copyright exemptions and the application of implicit licenses; activities can best take place in countries with a copyright and database-right regime that is most favourable for the project in these respects.
9. Conduct a risk analysis to determine which level of liability is acceptable for data protection infringements (e.g. for processing sensitive data) and for IPR infringements in light of uncertainties about, for example, the existence of implicit licenses and the applicable law with respect to statutory exceptions.
10. Apply privacy/security by design by restricting the functionalities of the end product(s) as much as possible (i.e. make them minimally invasive of human rights and intellectual property rights) while ensuring they can serve their intended purpose of open source intelligence by public authorities for public security.

Table 4: Ethical and legal challenges of SOCMINT

Police uses of social media	**Citizens as providers of public security (DIY policing)**
Legal issues 1)The double role of public security agents enforces of the law, data controllers) 2)Fundamental rights of citizens 3)Involvement of citizens in the provision of public security	Difficulty in ensuring transparency, accountability and non-discrimination. Citizens are driven by their own interpretations of the law and morality without democratically legitimized authority.
Ethical issues 1)Disproportionate interference with the privacy of innocent individuals or groups 2)Risk of outright discrimination 3)Unfair access of some vulnerable or disadvantaged groups to criminal justice of public security 4)Police officers rights to a private life and to freedom of expression	Key challenges (concerning especially the dark web): -How to distinguish between illegal and merely offensive or otherwise unethical behaviour -How to determine the line between justified covert interactions with criminals and unjustified entrapment

Table 5: Ethical criteria for SOCMINT

Ethical criteria for SOCMINT
1. Risks of disproportionate interference with the privacy of innocent individuals. 2. Risks of outright discrimination or unwarranted stigmatization of individuals or groups as criminally suspicious as well as risks of discrimination. 3. Unfair (because less easy or reliable) access of some vulnerable or disadvantaged groups to criminal justice or public security resulting from their relative lack of technology and/or technological skills. 4. The rights of police officers to a private life and to freedom of expression on social media.

3.3 Big data

Considering the potentially huge amount of data to store in the MARISA concept, it is proposed to adopt an original "big data" approach. Wikipedia defines "big data" as a "collection of datasets so large and complex that it becomes difficult to process using on-hand database management tools". In practice, "big data" regroups a set of techniques/tools suitable for this storing and processing such datasets with, usually, a "NoSQL" approach.

Capabilities to gather, analyse, disseminate, and preserve vast quantities of data raise concerns about the nature of privacy and the means by which individual privacy might be compromised or protected. Anonymity overlaps with privacy, but the two are not identical. Likewise, the ability to make intimate personal decisions without government interference is considered to be a privacy right, as is protection from discrimination on the basis of certain personal characteristics (such as race, gender or genome). Privacy is not just about secrets.

Data collection: Individuals constantly release into the MARISA environment information whose use or misuse may be a source of privacy concerns. Physically, these information emanations are of two types and can be called "born-digital" and "born-analog." Born-digital information is created by the individuals themselves or by a computer surrogate, specifically for use by a computer or data processing system. When data are born digital, privacy concerns can arise from over-collection. Over-collection occurs when a program's design intentionally, and sometimes clandestinely, collects information unrelated to its stated purpose. Over-collection can, in principle, be recognized at the time of collection. Born-analog information arises from the characteristics of the physical world. Such information becomes accessible electronically when it impinges on a sensor such as a camera, microphone or other engineered device. When data are born-analog, they are likely to contain more information than the minimum necessary for their immediate purpose, and for valid reasons. One reason is for robustness of the desired "signal" in the presence of variable "noise" (Executive Office of the President 2014a). In addition, the MARISA concept itself creates metadata, e.g. interconnection between the developed services develops meta-data from all data to be transmitted. Metadata are ancillary data that describe properties of the data such as the time the data were created, the device on which they were created or the destination of a message. Included in the data or metadata may be identifying information of many kinds. It cannot today generally be asserted that metadata raise fewer privacy concerns than data (Executive Office of the President 2014a).

Data analytics: After data are collected, data analysis techniques (termed "analytics") come into play and may generate an increasing fraction of ethical and privacy issues. By analytics, nonobvious and sometimes private information can be derived from data that, at the time of their collection, seemed to raise no, or only manageable, privacy issues. Data fusion occurs when data from different sources are brought into contact and new facts emerge. Individually, each data source may have a specific and limited purpose, but their combination may uncover new meanings. Such new information, used appropriately, may often bring benefits to individuals and society. However, the wide variety of potential uses for big data analytics raises crucial questions about whether our legal, ethical, and social norms are sufficient to protect privacy and other values in a big data world (US Executive Office of the President, 2014a). The "brain" of MARISA is enhanced data fusion and analysis to improve maritime surveillance as well as search and rescue with respect to response time and situational awareness. Due to data fusion in MARISA, privacy concerns may not necessarily be recognizable in born-digital data when they are collected. Due to signal processing robustness and standardization, the same is true of born-analog data—even data from a single source (e.g. a single camera). When born-digital and born-analog data are combined with data fusion, new kinds of data are generated from data analytics.

Use of data: Data analysis does not directly touch the individual (it is neither collection nor, without additional action, use) and may have no external visibility. By contrast, it is the use of data (including born-digital or born-analog data and the products of data fusion and analysis) that can cause adverse consequences for individuals. Violations of privacy are possible even when there is no failure in computer security. If an authorized individual chooses to misuse data, what is violated is privacy policy, not security policy. Or, as we have discussed, privacy may be violated by the fusion of data—even if performed by authorized individuals on secure computer systems (US Executive Office of the President, 2014b)

Infrastructure behind data: Data analytics requires not just algorithms and data but also physical platforms where the data are stored and analysed. The related security services used for personal data are also an essential component of the infrastructure. Good cybersecurity enforces policies that are precise and unambiguous. On the other hand, compromised cybersecurity is clearly a threat to privacy. Privacy can be breached by failure to enforce confidentiality of data, by failure of identity and authentication processes or by more complex scenarios such as those compromising availability (US Executive Office of the President, 2014a).

An ethical issue in the big data context is data protection and privacy. Regulation of data protection and privacy is founded on fundamental rights that are enshrined in treaties such as the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights in EU.

Another ethical issue comes with automated policing. Automated discrimination is possible when augmented surveillance becomes more common. It intersects with the technical issues of unintended biases in algorithms and big data that could skew analyses generated by artificial intelligence (AI) systems (Rahman, 2017). Algorithms tell computers step by step how to solve a certain problem. According to Rahman (2017), the first problem comes from algorithmic bias—AI algorithms being a reflection of the programmers' biases—may possibly give rise to the risk of false alerts by AI surveillance systems thus resulting in wrongful profiling and arrest; and the second problem is that AI profiling systems utilise historical data to generate lists of suspects for the purposes of predicting or solving crimes. AI systems are only as good as the data sets that the systems trained and worked with (Rahman, 2017).

A framework for the big data proposed by Broeders, et al. (2017) seems to be suitable in turn for the purposes of MARISA both on the level of technology, user processes and business model (see Table 6). It emphasises the phases of analysis (and use) of big data. The important choices are made in the phase of the analysis: selecting the algorithms, data sources and categorisation, assigning weight to various data, etc. In the current legal framework, the analysis phase has remained relatively unregulated and algorithmic accountability is largely lacking. Therefore, quality criteria should be made more explicit to increase organisational awareness and to create more accountability; a legal and explicit duty of care should be introduced for government organisations using big data analysis in the domain of security. Furthermore, when it comes to the use of big data, the real life consequences merits very thorough scrutiny of how big data analyses contribute to decision-making processes and their practical use. (Broeders et al, 2017).

Table 6: Framework for big data (Broeders et al, 2017)

Regulation in the analysis phase A legal and explicit duty of care External reviews and audits Sunset clauses and Surveillance Impact Assessment (SIA) (>PIA)
Regulation for the use of the data Bounding profiles No (semi)-automatic decision making Own the data, own the consequences
Reinforcing oversight Increasing layered transparency Increasing possibilities for judicial review

4. Discussion

Ethical issues concerning OSINT, SOCMINT and big data are diverse and evolving. Their impact on MARISA concern both technology, user processes and the business/governance model. Even though international regulatory guidelines are available, specific allowances, prohibitions and exceptions mainly stem from national legislation. European Data Protection Reform (EDPR) partly harmonizes data protection regulation in EU countries (DPA), but still leaves the possibility for variation on the national level (DPD).

One big challenge is coping with the mosaic effect. Data protection sets strong requirements on MARISA technology utilizing various data sources and performing data fusions on various levels. Another big challenge concerns the reliance of automated analysis: How can data fusion algorithms that are reliable and transparent for the end-user be developed? As dos Passos (2016) argues, associated with OSINT, big data is about being able to map behaviour and tendencies. However, data science is needed in OSINT because of the lack/low quality of big data, to find the correct answers, capture the correct data and to have the correct perception of how to proceed throughout the process.

In the context of big data, it is also notable that current academic and public debates entertain the notion of shifting the emphasis from data collection to data analytics and data use. There are scholars who underline the need for "algorithmic accountability" (Broeders et al, 2017). It can therefore be expected that the legal requirements concerning personal data processing and big data may develop in this direction. Therefore, to separate the ethics of data collection from the ethics of the processing and use of data is essential.

References

Broeders, D., Schrijvers, E., van der Sloot, B., van Brakel, R., Hoog, J. and Ballin, E. (2017) ”Big data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data”, *Computer Law & Security Review*, 33, pp 309-323.

dos Passos, D. (2016) “Big Data, Data Science and their contributions to the development of the use of open source intelligence”, *Systems & Management*, 11, pp 392-396.

Eijkman, Q. and Weggemans, D. (2012) “Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?” *Security and Human Rights*, pp 285-296.

European Commission (2018) Maritime CISE, A Common Information Sharing Environment for Maritime Surveillance in Europe, [online], https://webgate.ec.europa.eu/maritimeforum/en/frontpage/1046.

Glassman, M. and Kang, M. J. (2012) ”Intelligence in the internet age: the emergence and evolution of OSINT”, *Computers in Human Behavior*, 28, pp 673-682.

Hadjimatheou, K. and Roosendaal, A. (2016) MEDIA4SEC: Report on State of the Art Review, [online], http://media4sec.eu/downloads/d4-2.pdf.

Hribar, G., Podbregar, I. and Ivanusa, T. (2014) ”OSINT: A ‘Grey Zone?” *International Journal of Intelligence and CounterIntelligence*, 27, pp 529–549.

Hu, E. (2016) Responsible Data Concerns with Open Source Intelligence, [online], https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/.

Koops, B. (2013) “Police investigations in Internet open sources: procedural law issues”, *Computer Law & Security Review*, 29, pp 676-688.

Koops, B., Hoepman, J. and Leenes, R. (2013) “Open-source intelligence and privacy by design”, *Computer Law & Security Review*, 29, pp 676-688.

Koops, B.-J., Cuijpers, C. and Schellekens, M. (2011) “VIRTUOSO: D 3.2 Analysis of the legal and ethical framework in open source intelligence”, [online], http://www.virtuoso.eu/VIRTUOSO/servlet/document.fileView/Virtuoso-D3%202-Legal%20and%20ethical%20constraints-final-2011-12-21.pdf.

MARISA. (2018) “MARISA - Maritime Integrated Surveillance Awareness” [online], Marisa Project, https://www.marisaproject.eu/.

Meijers Committee. (2012) Note of the Meijers committee on the proposal for a regulation establishing the European border surveillance system.

Podbregar, I. (2016) “Some Counterintelligence Dilemmas”, in I. Podbregar, & T. Ivanuša, *The Anatomy of Counterintelligence: European Perspective,* Sharjah: Bentham Science Publishers, pp 133-141.

Rahman, F. (2017) “Smart Security: Balancing Effectiveness and Ethics”, RSIS Commentary, 235 [online], https://dr.ntu.edu.sg/bitstream/handle/10220/44235/CO17235.pdf?sequence=1&isAllowed=y.

SIEWG (2012) Societal Impact Expert Working Group EC DG ENTR Report, CIES.

Trottier. (2015) “Open source intelligence, social media and law enforcement: Visions, constraints and critics”, *European Journal of Cultural Studies,* 18, pp 530-547.

US Executive Office of the President (2014a) “Big Data and Privacy: A Technological Perspective”, White House.

US Executive Office of the President. (2014b) “Big Data: Seizing Opportunities, Preserving Values”, White House.

Wells, D. and Gibson, H. (2017) “OSINT from a UK perspective: Considerations from the law enforcement and military domains”, in H. Maasing, *From research to security union*, Tallinn: Sisekaitseakadeemia, pp 83-114.

Wood, M. G. (2016) “Social media intelligence, the wayward child of open source intelligence”, [online], https://medium.com/privacy-international/social-media-intelligence-the-wayward-child-of-open-source-intelligence-201f31dfb81d.