3. Privacy and data protection in open source intelligence and big data analytics: Case 'MARISA'

Jyri Rajamäki, Sari Sarlio-Siintola, Nina Alapuranen & Minna Nevanperä

Open Source INTelligence (OSINT) is intelligence collected from publicly available sources, including the internet, newspapers, radio, television, government reports and professional and academic literature (Glassman & Kang, 2012). Local and national law enforcement authorities, intelligence agencies and the military commonly take advantage of OSINT. An important aspect of law enforcement authorities' use of OSINT is social media, which aggregate huge amounts of data generated by users who are in many cases identified or identifiable. Combining social media with other datasets creates a technological landscape in which big data analytics can be used to implement predictive social surveillance systems (Staniforth, 2016). The line between espionage and OSINT is thin (Hribar;Podbregar;& Ivanusa, 2014), and caution and double-checking are advised before combining OSINT with big data analytics. Law enforcement authorities must always ensure that their use of OSINT and big data analytics falls within national and international legal frameworks, including General Data Protection Regulation (GDPR) and the Law Enforcement Directive, which focus on privacy and data protection.

From a privacy point of view, the use of social media in surveillance is a notable topic. Police and other law enforcement bodies are able to access private information without interacting with users on site. Trottier points out that on social media we're moving towards asymmetric relations of visibility between police and the public. Individuals are not aware that they are under watch (Trottier 2016). What is interesting about law enforcement using social media is that the awareness of such surveillance varies, based on the type of platform. In many countries, police are already visible, for example, on Facebook, and for that reason, it should not be a surprise that the information available will be used for surveillance purposes. The challenge is that law enforcement bodies are also using other social media platforms such as Twitter, and this might be surprising to some individuals. This is what brings challenges from a privacy point of view. Should individuals nowadays assume that if they post something on social media, that information could be used for purposes

other than what the platform is intended for? Or should individuals still be able to trust that their information is not used for a purpose that might be surprising? This is how the GDPR expects personal data processing to work, and this is a question discussed in the MARISA project from an ethical point of view: Is it surprising to citizens that law enforcement bodies are using social media for their own purposes, or is it something that individuals should already expect, taking into account the public nature of many social media platforms? Social media provides valuable information to law enforcement bodies, but the question remains of how it should be used so that it can build trust between citizens and authorities. Should there be common rules for this usage, and where should this kind of information be provided – on the law enforcement side, on the social media site, or somewhere else?

In 2019 the European Commission introduced their Ethics Guidelines for Trustworthy AI. The Privacy by Design approach is recommended when solving privacy issues in the development of AI systems. According to the Commission, privacy protection should be a fundamental assumption for all AI systems, and it must be ensured throughout the lifecycle of the AI system. This must cover all data the users provide the system and the data created over the course of their interaction. The information gathered on the users must be handled in such way that it does not cause any harm to the user, and the data cannot be used to discriminate or to be used unlawfully in any way (European Commission, 2019).

This article analyses privacy and data protection issues in open source intelligence and big data analytics carried out by law enforcement authorities. The empirical case explores these challenges in the MARISA project. The overall aim is to accelerate the discussion on the problem of privacy and data protection with regard to law enforcement technical tools, which may lead to restrictions of individual liberty and erosion of society's foundations of trust.

MARISA SERVICES AND PERSONAL DATA

The MARISA Toolkit is built atop a big data infrastructure that provides the means to collect external data sources and operational systems products and to organize and exploit all incoming data as well as all the data produced by the various services. The MARISA toolkit provides a suite of services to correlate and fuse various heterogeneous and homogeneous data and information from different sources, including internet and social networks. MARISA also aims to build on the huge opportunity that comes from open access to big data for maritime surveillance: the availability of large to very large amounts of data—acquired from various sources ranging from sensors, satellites, internal sources and open source,—improves knowledge. The MARISA toolkit provides new means for the exploitation of the bulky data silos, leveraging on the fusion of heterogeneous sector data and taking advantage of a seamless interoperability with existing legacy solutions available across Europe.

The MARISA toolkit has two relevant data sources: 1) data coming from the sensors and 2) data coming from OSINT/social media. Data from sensors: These sensors are embodied in the operational environment of the legacy systems. In these environments, owned by participating Member State governmental entities, we can presume that the data are used on the basis of need-to-know and need-to-share. Thus, the privacy of the data can be taken for granted. Data from open sources: This case is more problematic, since the origin of the data is not controlled by any public entity. Nevertheless, there are two possibilities: 1) A system performing in a classified environment (as could be the case in managing EU-restricted data). Here the data coming from open sources enters, by means of a cross-domain exchange devices, in a highly regulated environment, where again the privacy of the data managed can be taken for granted on the basis of need-to-know and need-to-

share. 2) A system performing in an unclassified environment (this will be the most common case) (MARISA, 2018).

When Automatic Identification System (AIS) data is linked to crew lists, locations of persons will be exposed, and this is personal data covered by the GDPR. As well, the end users' operational systems connected to the MARISA toolkit can include personal data or anonymized personal data. The first-phase MARISA service description document (MARISA, 2018) defines the following open-source- or AIS-data-related services: AIS verification, Twitter, OSINT and GDELT. Table 1 presents those services.

Table 1. *Personal Data and Open Source Related MARISA Services (adopted from MARISA, 2018)*

NAME OF THE SERVICE	DESCRIPTION
AISVerificationService: ProcessLocations	Verifies the claimed position in an AIS message against measurements from a radio locating system; accesses a file system that contains results from the radio locating system.
TwitterService: GetRelevantTweetsInArea	Retrieves a list of relevant tweets in a given area and time period and computes an appropriate risk.
GDELT: GetRelevantEventsInArea	Takes OSINT sources such as GDELT project data/news and filters the results using natural language processing in order to identify possible events related to the maritime domain such as naval incidents, piracy, pollution, etc.
OSINT: GetTweetsByParams	Retrieves a list of relevant tweets in terms of keywords, given area and publication date.

PRIVACY CHALLENGES OF MARISA SERVICES

Data generation and collection

Table 1 presents personal data and open-source-related MARISA services. AIS without crew lists does not contain information that can be used to identify a private person. OSINT service mainly collects its information via Twitter and DGELT. From a data collection point of view, the MARISA GDELT service may not have privacy concerns, because professional journalists should have considered that issue when producing a report. On Twitter, several technical features and tweet-based social behaviours may compromise privacy. Tweets are complex objects that, in addition to the message content, have many pieces of associated metadata, such as the username of the sender, the date and time of the tweet, the geographic coordinates the tweet was sent from, if available, and much more (Glasgow, 2015). "Most metadata are readily interpretable by automated systems, whereas tweet message content may require text processing methods for any automated interpretation of meaning" (Glasgow, 2015). "Direct Messages" are the private side of Twitter and "retweeting" is directly quoting and rebroadcasting another user's tweet. Someone might unintentionally or intentionally retweet a private tweet to a public forum. Other behaviours include mentioning another user in one's tweet talking about that user. According to Rumbold and Wilson (2018), when one puts any information in the public domain—whether intentionally or not—one does not waive one's right to privacy, but one can only waive one's right to privacy by actually waiving it. The GDPR requires that a person knows for what purposes their

personal data is being used. Considering that personal data should not be used for unexpected purposes, one could ask if this requirement is fulfilled when Twitter data is used for surveillance. Although there may be legally acceptable reasons why data could be used for such purposes, the ethical question remains: Will such data usage build trust between citizens and authorities, and what kind of actions should be taken to avoid potential mistrust?

Data analytics

Big data may be analysed by artificial intelligence (AI), which can provide detailed, personalized characteristics of an individual and a prediction of his or her future behaviour (Moallem, 2019). The MARISA toolkit includes big data infrastructure, and AI-anonymized data can be de-anonymized quite quickly in certain conditions (Campbell-Dollaghan, 2018). Algorithms tell computers how to solve a certain problem step by step. However, predictive algorithms are often unpredictable (Wójtowicz & Cellary, 2019). According to Rahman (2017), the first problem comes from algorithmic bias—AI algorithms being a reflection of the programmers' biases—and may possibly give rise to the risk of false alerts by AI surveillance systems, thus resulting in wrongful profiling and arrest; the second problem is that AI profiling systems utilise historical data to generate lists of suspects for the purposes of predicting or solving crimes. Machine learning (ML) techniques including neural networks run in two phases (the training phase and the prediction phase), and the quality of predictions is absolutely dependent on examples used for the training phase. ML systems are only as good as the data sets that the systems trained and worked with (Rahman, 2017). Here comes the challenge when social media is used as a source: How can one ensure that the data does not provide misleading results?

Use of data

Data analysis does not directly affect the individual and may have no external visibility. According to Dignum et al. (2018), three ethical issues are particularly concerning to AI systems: accountability, responsibility and transparency. They state that these three values are important to discuss when trying to ensure societal good. How the AI system follows these ethical principles depends upon what kind of reasoning is possible. If we believe the AI system is incapable of ethical reasoning, it means we should always have human supervision. That also means that the supervisor should have sufficient knowledge and the means to do the job. This approach is called human-in-the-loop. Another approach to the ethical reasoning of the system is in designing the environment itself in such a way that deviation is impossible and the moral decision-making of the system is unnecessary. Ethics by Design considers the AI system to be an ethical agent itself; these agents are known as artificial moral agents. That means the AI system is able to include moral reasoning into its deliberation and decision-making and explain its behaviour in terms of moral concepts. This approach requires complex decision-making algorithms based on deontic logics. The system design requires explicit and complex design based on reinforcement learning to be able to act as a moral decision-maker (Dignum et al., 2018, 1-3).

PRIVACY DESIGN FRAMEWORK IN THE MARISA PROJECT

The implementation of privacy-by-design in the MARISA toolkit is an overall requirement or constraint for the development of the MARISA project (MARISA, 2018). Ethics by Design and Values in Design became key values when considering designing ethical and trustworthy MARISA services utilising big data analytics. Their

goal to ensure that ethical matters—including privacy and data protection—are considered from the earliest stages of the project and throughout the full development and design process. Technical infrastructures and technology often reveal human values mostly because of the tensions, failures and counter productivity. The Values in Design approach tries to create discipline that includes values in the socio-technical designing process (Knobel & Bowker, 2011). Ethics by Design in artificial intelligence is concerned with methods, algorithms and tools needed to ensure that autonomous agents with capability to reason take the path of ethical decisions and that their behaviour stays within the moral boundaries provided to the system (Dignum et al., 2018).

Privacy by Design is a part of the same continuum of Values by Design and Ethics by Design that emphasizes taking ethics—in this case privacy—into the design process from the beginning. This means a proactive method for preventing privacy issues from happening by defining privacy as the system's default setting (Cavoukian, 2012).

Applying the Privacy by Design approach was part of our systematic framework for identifying ethical aspects of the MARISA solution (see the article "An Ethical Framework for Maritime Surveillance Technology Projects" in this publication). Based on that holistic approach, privacy and data protection requirements for the technology and for the organizational arrangements were defined. The validation of technical features was a part of the MARISA validation process. In addition, a Privacy and Data Protection Impact assessment was performed in order to identify potential technical and non-technical risks related to privacy and data protection. The need to conduct this kind of impact assessment as part of each new MARISA implementation was also codified in the MARISA Code of Conduct and MARISA implementation documents.

ACKNOWLEDGEMENTS

Acknowledgement is paid to the MARISA Maritime Integrated Surveillance Awareness project. This project is funded by the European Commission through the Horizon 2020 framework under grant agreement number 740698. The sole responsibility for the content of this paper lies with the authors. It does not necessarily reflect the opinion of the European Commission or of the full project. The European Commission is not responsible for any use that may be made of the information contained therein.

References

Agre, P. 1997. Toward a Critical Technical Practice: Lessons Learned in Trying to Reform AI. In G. Bowker, L. Gasser, S. L. Star, & B. Turner, Social Science, Technical Systems and Cooperative Work: The Great Divide (pp. 131–158). Hillsdale: Lawrence Erlbaum.

Campbell-Dollaghan, K. 2018. Sorry, your data can still be identified even if it's anonymized. Retrieved Aug 14, 2019, from https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized

Dignum, V., Baldoni, M., Baroglio, C., Caon, M., Chatila, R., Dennis, L., . . . Ted. 2018. Ethics by Design: necessity or curse? Retrieved from https://www.aies-conference.com/2018/contents/papers/main/AIES_2018_paper_68.pdf

Friedman, B., & Nissenbaum, H. 1997. Bias in Computer Systems. In B. Friedman, Human Values and the Design of Computer Technology (pp. 21–40). Cambridge and New York: Cambridge University Press.

Glasgow, K. 2015. Big data and law enforcement: Advances, implications, and lessons from an active shooter case study. In B. Akhgar, G. Saathiff, H. Arabnia, R. Hill, A. Staniforth, & P. Bayerl, Application of Big Data for National Security (pp. 39-54). Waltham: Butterworth-Heinemann.

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

High-Level Expert Group on Artificial Intelligence. 2019. Ethics guidelines for trustworthy AI. Brussels: European Commission.

Hribar, G., Podbregar, I., & Ivanusa, T. 2014. OSINT: A "Grey Zone"? International Journal of Intelligence and CounterIntelligence, 27, 529–549. doi:10.1080/08850607.2014.900295

Knobel, C., & Bowker, G. 2011. Computing ethics: Values in Design. Assosiation for Computing Machinery. Communications of the ACM, 57(7), p.26.

MARISA. 2018. D3.2 MARISA services description document.

Moallem, A. 2019. Perspectives on the future of human factors in cybersecurity. In A. Moallem, Human-computer interaction and cybersecurity handbook (pp. 353-366). Boca Ratom: CRC Press.

Rahman, F. 2017, Dec 14. Smart Security: Balancing Effectiveness and Ethics. RSIS Commentary, 235. Retrieved from https://dr.ntu.edu.sg/bitstream/handle/10220/44235/CO17235.pdf?sequence=1&isAllowed=y

Rumbold, B., & Wilson, J. 2018. Privacy Rights and Public Information. The Journal of Political Philosophy.
Sengers, P., Boehner, K., David, S., & Kaye, J. 2011. Reflective Design. Proceedings of the 4th Decennial Conference on Critical Computing: Between Sense and Sensibility (pp. 49–58). New York: ACM https://dl.acm.org/doi/pdf/10.1145/1094562.1094569