


Online Surveillance Awareness as Impact on Data Validity for Open-Source Intelligence?

Petra Saskia Bayerl¹  and Babak Akhgar²

¹ Rotterdam School of Management, Erasmus University,
Rotterdam, Netherlands
pbayerl@rsm.nl

² CENTRIC, Sheffield Hallam University, Sheffield, UK
B.Akhgar@shu.ac.uk

Abstract. Online surveillance, especially of open sources such as social media (OSINT/SOCMINT), has become a vital source of information for decisions made by public institutions such as law enforcement agencies. This keynote discusses the concept of online surveillance awareness (OSA) as a possible long-term threat to the quality of OSINT-relevant online sources. An interdisciplinary research agenda to systematically investigate the links of OSA to the reliability and validity of OSINT sources and thus the quality of OSINT more generally is outlined.

Keywords: Online surveillance awareness · Online surveillance · OSINT · Data reliability · Data validity · Law enforcement agencies · Research agenda

1 Introduction

Open source Intelligence (OSINT) is increasingly being utilized by Law Enforcement Agencies (LEAs) and public authorities in order to enhance a wide range of their functions. These include investigative capabilities, situation awareness, the management of public disorder, responses against criminal threats, responses to crises, as well as understanding public perceptions of security and safety [1–3].

Examples of OSINT applications by LEAs can be found in their public announcements, news broadcasts and in the professional literature. Most prominent amongst them are cases such as the ‘Arab spring’ in 2010–2011, the riots in London and other English cities in summer 2011, the 2012 London Olympics, FBI-hostage negotiations in Pittsburgh in 2012, the murder of British soldiers in the streets of London in 2013 or the abduction of Nigerian girls from their school by Boko Haram in early 2014. These events have seen a considerable reliance on the processing of OSINT, and more specifically social media intelligence (SOCMINT) by LEAs, security agencies and public authorities in particular. OSINT can support tasks such as the creation of situational awareness, intelligence gathering, sentiment analysis and communication with and from the public.

LEAs gathering information from open sources depend on the monitoring, collection and analysis of often very large amounts of data. These are activities, which happen

generally unbeknownst to the producers of the data, i.e., the citizens using the internet. However, since the Snowden revelations knowledge about online surveillance has become ubiquitous. Our question is what happens, when internet users are aware of the presence, type and degree of online surveillance? In what way does this influence their behaviors and in which ways and to what degree does this impact the quality of OSINT sources, if at all?

Issues in the quality, i.e., reliability and validity of open data sources, threaten the dependability, effectiveness and efficiency of decisions made using it. These may result in critical mistakes for deployment of resources and actions by LEAs and other authorities, for instance, during a criminal investigation or the management of crises. We argue that online surveillance awareness (OSA), i.e., the knowledge or at least assumption of users that their behavior and information online is monitored, collected and analyzed, threatens the quality of OSINT and OSINT-based decisions. This issue has so far received little attention in discussions of OSINT, and even less empirical efforts have been undertaken to systematically investigate the concrete effects of OSA on OSINT quality for LEAs. In this keynote we will reduce introduce the concept of online surveillance awareness presenting a research framework and agenda to investigate the links of OSA to the reliability and validity of OSINT sources and thus the overall quality of OSINT.

2 Online Surveillance and OSINT Effectiveness

Surveillance of online behavior is a vital aspect of efforts to fight crime as well as in the response to and management of crises. We argue that two elements affect the quality of OSINT: (1) awareness of online surveillance and (2) public attitudes towards surveillance.

A first indication for this link can be found in a recent study by Marthew and Tucker, which investigated the shift in Google search patterns prior compared to after the Snowden revelations in ten different countries [4]. As they demonstrated, in most countries keywords became less ‘contentious’, i.e., users avoided searches “they believe might get them in trouble with the [U.S.] government” [4]. Although the study does not allow a direct causal link, it provides strong indications of OSA and subsequent modifications of online user behavior. In our own research, we have investigated assumptions of online surveillance and the tendency for falsification of personal information [5]. We found that OSA in the form of online surveillance assumptions increased the acceptance of falsification in others as well as the propensity to falsify our own personal information.

Our study on information falsification introduces two possible contingencies to the effect of OSA on OSINT: perceived usefulness and acceptance of online surveillance and type of organization conducting the surveillance (in our case state agencies versus private companies). On a conceptual level this leads a possible Effects Model of OSA for falsification of personal information, which links online surveillance with falsification moderated by usefulness perceptions and user trust in the organizations conducting online surveillance (see Fig. 1).

Together these studies provide first empirical indications that OSA can change user behavior on a large scale. This link between OSA and changes in online user behavior creates not only social, legal and political implications but also critical practical

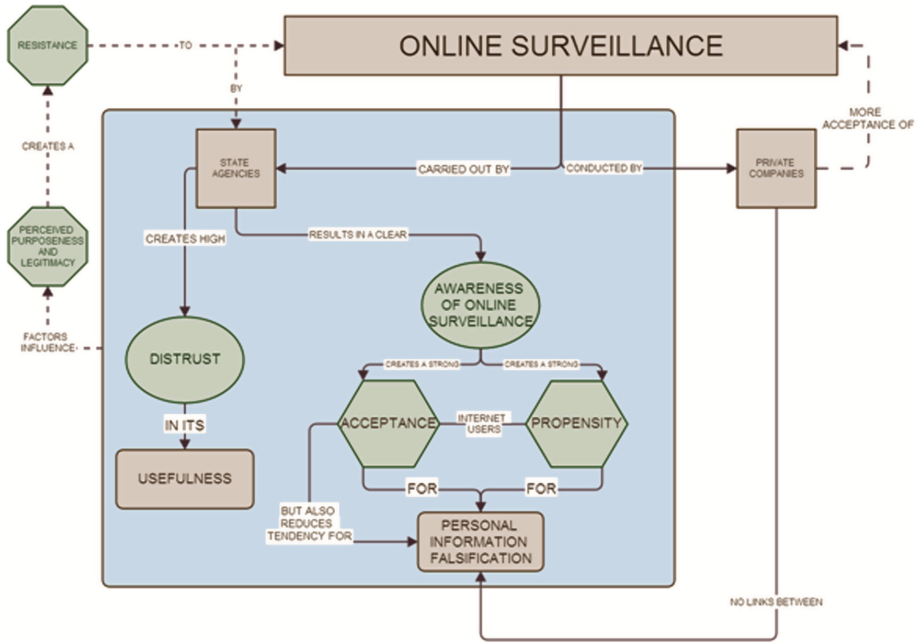


Fig. 1. Suggested effects model for the link between online surveillance and falsification of personal information based on [2]

implications for LEAs and other organizations basing operational decisions on OSINT, starting with the design and development of relevant tools and platforms. Similarly, OSA is also likely to affect citizens' acceptance of the tools and applications put forward by LEAs for use during situations such as natural disasters or help and advice services (e.g., "ask the police" applications).

As the debates and reactions in the aftermath of the Snowden revelations demonstrate, online surveillance awareness threatens citizens' trusts in state authorities and LEAs. Critically, trust is one of the main factors that determine whether citizens use online services provided by LEAs [6]. In our opinion, it is thus crucial to systematically investigate the impact of online surveillance awareness on the multitude of sources and information types LEAs use in OSINT-based analyses and operations. In the following, we put forward a road map and agenda for future research efforts into this area.

3 A Research Road Map and Agenda

In order to further explore the relationship between OSINT quality and online surveillance awareness and to create a 'reference architecture' for the development of future OSINT applications, we sketch a research road map outlining possible topics and methodologies. Our agenda is based on the generic framework presented in Fig. 2.

As demonstrated in Fig. 2, several areas require investigation to understand the link between OSA and possible implications for OSINT quality. Firstly, the features of online

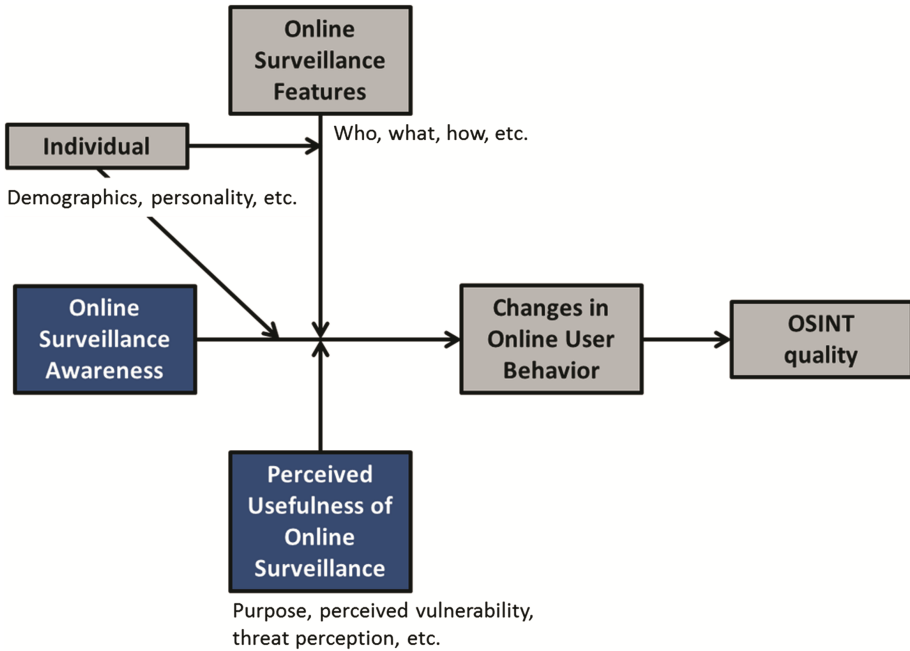


Fig. 2. Generic research framework for the link between online surveillance, online user behaviours and OSINT quality

surveillance (e.g., type of information collected, implicated organizations, and collection process) may influence how intrusive or problematic online surveillance is perceived. We hypothesize that the more problematic the surveillance is considered, the stronger the relationship between OSA and behavioral changes will be. Connected to this is the perceived usefulness of the surveillance [5], which will also depend on personal variables such as perceived vulnerability to the threats address in the surveillance (cyber-grooming, financial fraud, terrorism, crises, etc.). Moreover, features of the individual may play a role in shaping the relationship between OSA and behavioral changes, for instance, in terms of gender, online experiences, political orientations, etc. For example, men seem more critical about online surveillance than women, while less experienced internet users seem less critical than users with longer online experience [5]. Individual features may also play a role in determining the impact of surveillance features on the OSA-behavioral link, in that demographics, personalities, national contexts, etc. may influence judgments about the what, who and how of the surveillance process. Of course the behavioral changes are only relevant in as far as they impact OSINT-relevant information. It is therefore also vital to determine which relevant behaviors may be more or less influenced by OSA.

Our research agenda combines elements of big data analytics with psychological, organizational and criminological perspectives. We thus envision research on OSA-impacts as an interdisciplinary endeavor. Accordingly, methodologies will span the range from observations and experimentation to sentiment analysis and behavioral modelling. These methodologies will be adapted depending on the specific parts of the model under

investigation (e.g., investigation inter-individual differences versus investigating impacts of behavioral changes on different quality parameters).

We propose this research framework as a possible road map to inform newly established, but also existing research projects. Below we use an example from the context of crises management to illustrate how it may be integrated into more traditional research efforts on OSINT applications.

4 Application Scenario: OSINT Quality in Crises Management

One of the key elements for the management of crises is a clear understanding of the situation to enable decision makers to take appropriate actions in often volatile conditions. OSINT is one of the channels which can act as information source for decision makers. To avoid wrong decisions during fast developing critical situations, the reliability and validity of information is of special concern.

The use of OSINT in crisis response and management is addressed in several research projects, among them the EU-security project ATHENA. ATHENA explores how the huge popularity of new communication media, particularly web-based social media such as Twitter and Facebook, and the use of OSINT can be harnessed to provide efficient and effective communication and enhance situational awareness during crises. Its aim is to enable and encourage users of social media to contribute to the security of citizens in crisis situations by developing a suite of software tools to enhance the decision-making capabilities of LEAs, crisis management command and control centers, first responders, and citizens during and in the aftermath of crises ('ATHENA platform') [7]. Athena outputs will then feed into a Command and Control Centre for decision making authorities (e.g., LEAs and emergency planners). The effectiveness of the ATHENA platform relies heavily on the quality of its source information, which is obtained from open sources in the public space [8]. Its success further depends on the trust between citizens, LEAs and other organizations involved in crisis management efforts.

As part of our research agenda we will investigate the proposed framework (see Fig. 2) during the live exercise of Athena in collaboration with UK and European LEAs and other crisis management authorities. Amongst others, these exercises can focus on investigating in more detail the role of OSA for the willingness of citizens to provide information on social media during crises, the quality of this information (e.g., level of detail) and the role of trust in these situations.

5 Challenges to be Addressed in Current and Future Research on OSA-OSINT Links

While we firmly believe that systematic research into the costs and benefits of online surveillance awareness is a vital addition to current discussions of OSINT-use and application design. In addition there are also challenges to develop a unified research agenda as suggested in this paper. We have identified the following closely interlinked challenges for the development and deployment of the research agenda:

- (1) The speed of technological change
- (2) The evolution of internet regulatory, societal and technological frameworks, which are and may remain scattered across EU and international regions and institutions
- (3) The lack of a clear strategy to address the multi-disciplinary dimension of online surveillance by member states and authorities. The OSINT domain is addressed by many different organizations, research disciplines and approaches. The dialogue among these stakeholders remains too localized and needs to be coordinated in order to identify consensus on what is considered to be OSINT from ethical and legal standpoints.
- (4) A lack of a common terminology across disciplines, which hampers the development of a multidisciplinary approach.

All these challenges explain the need for a comprehensive, multidisciplinary research agenda elaborated through a citizen centered multidisciplinary and multifaceted methodological approach. Research on OSINT needs to evolve towards concrete solutions governed by citizens' rights to freedom of speech and the full spectrum of ethical concerns while maintaining national security of each country. In this context we believe that the consequences of online surveillance and the awareness of online surveillance for citizens' online behaviors and the relationships with each other as well as state authorities are of vital concern. In our research agenda we aim for a systematic investigation of these effects to create actionable knowledge for LEAs, designers of OSINT-tools and platforms, and decision makers relying on the quality of their data.

References

1. Akhgar, B., Yates, S.J.: Strategic intelligence management for combating crime and terrorism. In: Akhgar, B., Yates, S.J. (eds.) *Intelligence Management*, pp. 145–157. Springer, London (2011)
2. Bell, P., Congram, M.: Intelligence-Led Policing (ILP) as A Strategic Planning Resource in the Fight against Transnational Organized Crime (TOC). *Int. J. Bus. Commer.* **2**(12), 15–28 (2013)
3. Steele, R.D.: Open source intelligence. In: Johnson, L. (ed.) *Handbook of Intelligence Studies*, pp. 129–147. Routledge, New York (2007)
4. Marthews, A., Tucker, C.: Government surveillance and internet search behavior. In: SSRN (2014)
5. Bayerl, P.S., Akhgar, B.: Pitfalls for OSINT investigations: Surveillance and online falsification tendencies. *Communications of the ACM*, August 2015
6. Bayerl, P.S., Horton, K., Jacobs, G., Akhgar, B.: Who wants police on social media? In: *Proceedings of the 1st European Conference on Social Media*, pp. 42–49 (2014)
7. Andrews, S., Yates, S., Akhgar, B., Fortune, D.: The ATHENA project: using formal concept analysis to facilitate the actions of responders in a crisis situation. In: Akhgar, B., Yates, S. (eds.) *Strategic Intelligence Management: National Security Imperatives and Information and Communication Technologies*, pp. 167–180. Elsevier, Amsterdam (2013)
8. West Yorkshire Police: Athena Project: Latest News, 29 April 2014

Global Security, Safety and Sustainability: Tomorrow's
Challenges of Cyber Security

10th International Conference, ICGS3 2015, London,
UK, September 15-17, 2015. Proceedings

Jahankhani, H.; Carlile, A.; Akhgar, B.; Taal, A.; Hessami,
A.G.; Hosseinian-Far, A. (Eds.)

2015, XIII, 361 p. 95 illus., Softcover

ISBN: 978-3-319-23275-1