Surveillance and falsification implications for open source intelligence investigations

BAYERL, Petra and AKHGAR, Babak <http://orcid.org/0000-0003-3684-6481>

Published version

BAYERL, Petra and AKHGAR, Babak (2015). Surveillance and falsification implications for open source intelligence investigations. Communications of the ACM, 58 (8), 62-69.

Pitfalls for OSINT investigations: Surveillance and online falsification tendencies

Petra Saskia BAYERL, Rotterdam School of Management, Erasmus University Rotterdam, the Netherlands (corresponding author)
Babak AKHGAR, Center of Excellence in Terrorism, Resilience, Intelligence, and Organized Crime Research at Sheffield Hallam University, U.K.

Open Source Intelligence or ‘OSINT’ has become a permanent fixture in the private sector to assess product perceptions, track public opinions or measure customer loyalty.[12] The public sector, and here particularly law enforcement agencies (LEAs) such as police, also increasingly acknowledge the value of OSINT techniques to enhance their investigative capabilities and to allow more effective responses against criminal threats.[5]

OSINT refers to the collection of intelligence from information sources that are freely available in the public. This includes offline sources such as newspapers, magazines, radio and television as well as information on the internet.[4,16,17] Especially the spread of social media have vastly increased the quantity and accessibility of OSINT sources.[3,11] OSINT thus compliments traditional methods of intelligence gathering at very low to no costs.[4,15]

OSINT increasingly supports the work of LEAs in the identification of criminals as well as their activities such as recruitment, transfer of information and money or the coordination of their illicit activities.[18] For instance, the capture of Mr. Palazzolo, a treasurer for the Italian mafia on the run for 30 years was accomplished partly by monitoring his Facebook profile.[8] OSINT also demonstrated its potential to help respond quickly to criminal behaviors outside the internet, for instance, during public order incidents such as the 2011 UK riots.[1] OSINT has therefore become an important tool in the arsenal of LEAs to combat crime and ultimately safeguard society.[14]

To fulfill these functions, OSINT depends heavily on the integrity and accuracy of open data sources. This integrity is jeopardized, if internet users choose not to disclose personal information or even to provide false information of themselves.[7,9] Such omissions and falsifications can have grave consequences, if decisions are being made from data that is assumed to be accurate, but is not.[19]

This issue has become especially poignant, since the revelations by former NSA-contractor Edward Snowden of large-scale monitoring of communications and online data by state agencies. The revelations have created considerable mistrust in citizens of internet-based surveillance by governments; bringing the tensions between 'the security of society' versus 'a fundamental right to privacy' into sharp profile. These discussions begin to show concrete effects. For instance, privacy-sensitive keywords in Google searches changed from the period before to after the Snowden revelations, as users proved less likely to use keywords "that might get them in trouble with the [US] government".[10] Despite the existence of mandatory national and international data protection and privacy regulations, internet users thus seem wary of online surveillance and in consequence modify their behaviors.

For organizations using OSINT in their decision-making, changes in users' behaviors and here specifically the willingness to provide accurate accounts of themselves are problematic; firstly, because they increase the incidence of false information; secondly, because they raise the complexity and costs for information validation (i.e., authentication of individuals' web footprint against additional and trusted sources).

It is our belief that better understanding the tendency of internet users of when and why to change their online behavior as reaction to online surveillance can help in pinpointing especially problematic areas for the validity of OSINT methods. Such an understanding can further effectively guide efforts for more targeted cross-validations. So far, we lack a clear picture in how far and in what ways concerns of online surveillance change information-bases relevant for LEAs' use of open source intelligence. We therefore started a research program to systematically investigate whether shifts in online behaviors are likely and if so, in what form. In this paper we report on a recent study, in which we focused on the falsification of personal information, investigating the link between falsification acceptance and propensity with attitudes towards online surveillance, privacy concerns and assumptions of online surveillance by different organizations.

STUDY DESIGN AND SAMPLE

To understand internet users' attitudes towards the falsification of personal information in connection with online surveillance, we conducted an online survey using the micro-working platform Amazon Mechanical Turk to recruit participants between January and March 2014. A total of 304 users reacted to our request, of which 298 provided usable answers. Our sample consisted largely of experienced internet users (72.2% with more than 11 years of experience) and intensive users, with 41.3% of participants using the internet for at least 7 hours per day. The majority of participants lived in the USA (83.9%), a smaller proportion in India (9.4%) and the remainder in Canada, Croatia, Kenya and Romania (0.4-1.1% per country). The gender distribution was nearly equal with 48.9% male versus 50.4% female participants (0.7% preferred not to answer the question). Participants were relatively young, with a majority of the people 40 years or younger (67.3%) of which most were between 21-30 years (35.6%). Older participants were slightly under-represented with 9.5% between 51-60 years and 3.9% over 60 years (0.7% preferred not to answer the question). The questionnaire was administered online. Participants received US$0.70 for completion of the survey, which took in average four minutes to fill out.

FINDINGS

Attitudes towards online surveillance by state agencies

The first question when investigating the impact of surveillance on online behaviors is certainly, how internet users perceive its value. To capture attitudes towards online surveillance by state agencies we asked our participants to indicate their agreement to eleven statements, five of them positive towards online surveillance (i.e., addressing benefits), three of them negative (i.e., addressing possible threats) and two capturing general acceptance. The average values across the whole sample are shown in Figure 1.

The general acceptance of online surveillance was at a medium level with m=3.35 when the focus was on the prevention of offline crimes, and m=3.33 when focusing on the prevention of online crimes (both on a scale from 1 to 5). Overall, negative attitudes were considerably stronger than positive ones. Participants were especially concerned about threats to the freedom of expression and speech and the undermining of trust in the own government. Interestingly, the claims state agencies frequently make that monitoring of online behavior ensures that the internet remains a safe place or increases the safety of society found little agreement.

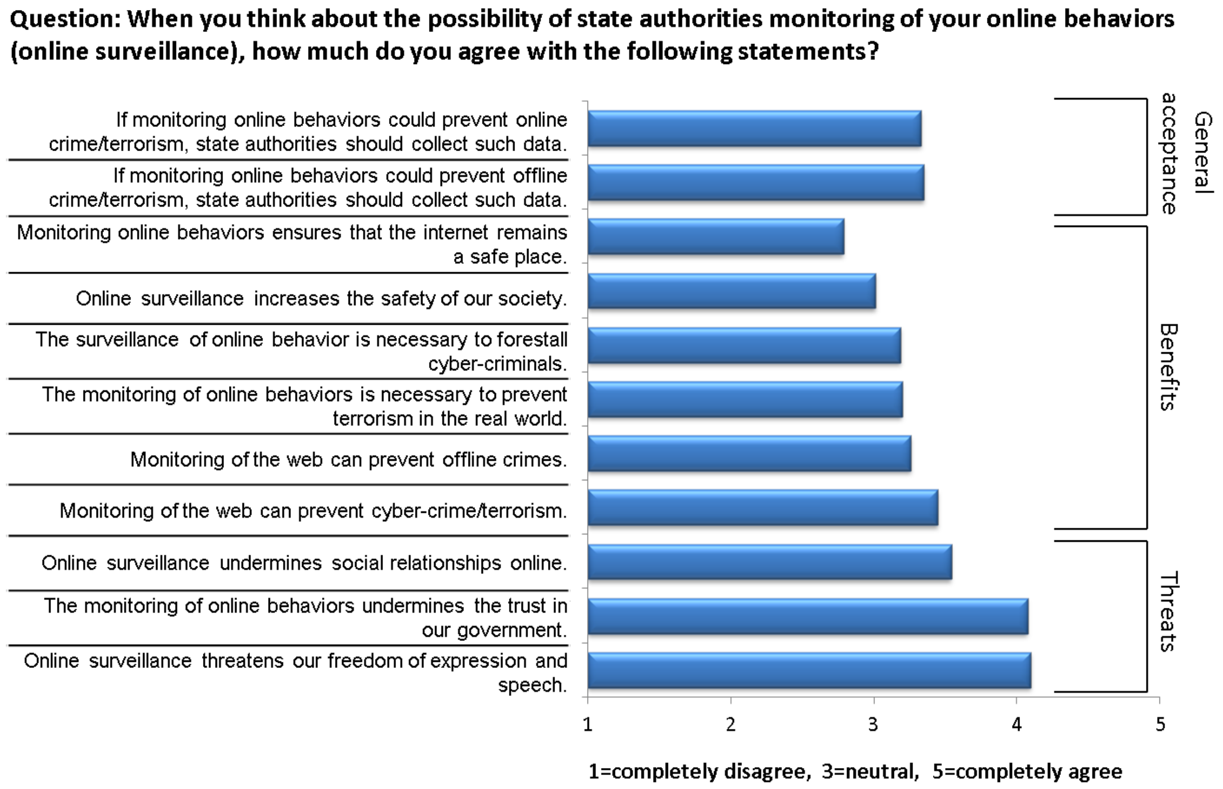

Figure 1. Attitudes towards the positive and negative sides of state online surveillance

Women were generally more accepting of online surveillance (t(280)=–3.02, p<.01) and saw significantly more benefits than men (t(279)=–2.60, p<.01). Men in contrast reported significantly higher concerns about its negative aspects (t(275)=3.69, p<.001; see Figure 2). Women were especially more willing to support online surveillance, if it could prevent crimes perpetrated outside the internet (offline crimes), whereas men were particularly concerned about the undermining of trust in the government. Further, users with more experience in the use of the internet (longer than 11 years) were significantly less positive towards online surveillance than users with shorter experience (7 years or less; F(2,274)=5.04, p<.01). Since age groups did not differ in their attitudes, this effect cannot be explained by generational differences. Instead it hints to an increasing sensitivity towards the issue with growing internet use.

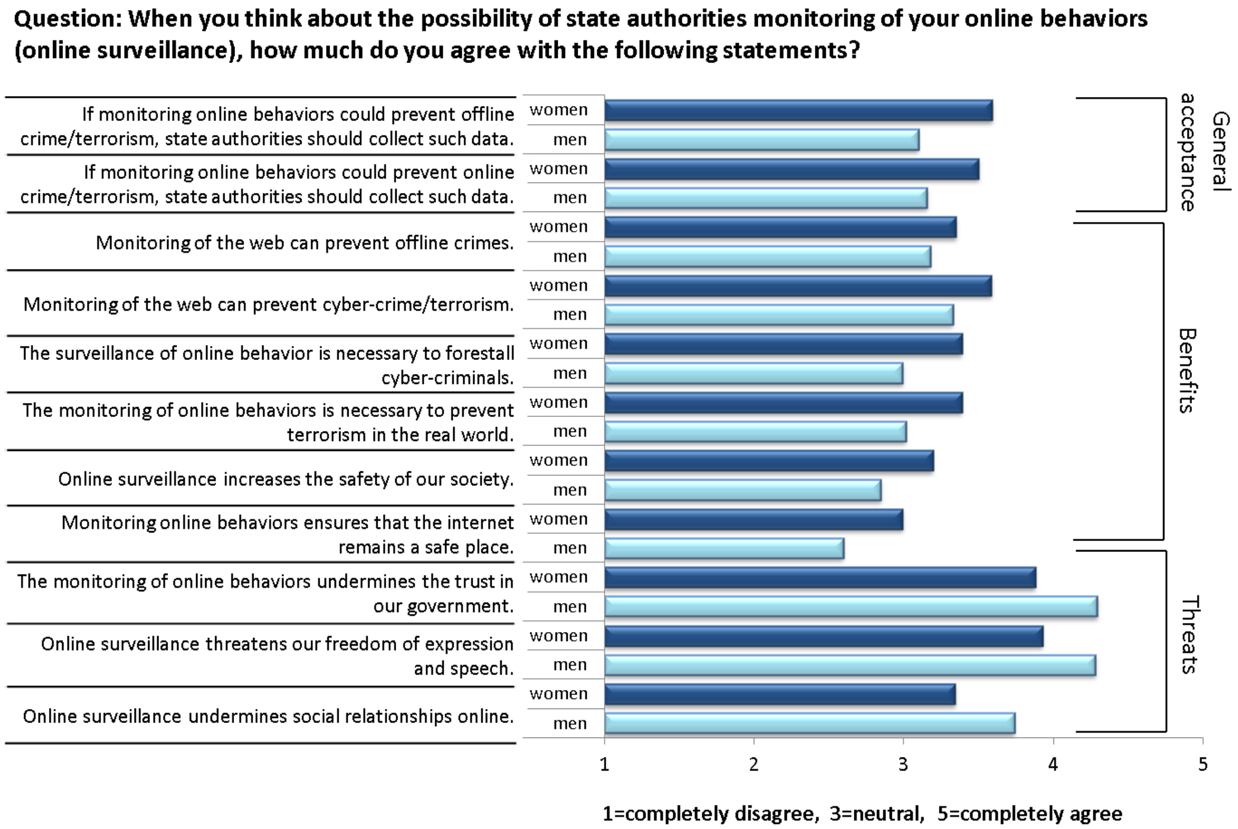

Figure 2. Gender differences in the perceived benefits and threats of state online surveillance

Surveillance by state agencies versus private companies

Compared to private companies, who are widely known to collect online data on a large scale, OSINT-use by state agencies has only recently come to the attention of the broader public. Yet, as the intense discussions in the aftermath of the Snowden revelations demonstrate, the sensitivity of the issue seems here even greater. Also, compared to OSINT-use by private companies, consequences of OSINT-use by LEAs can be considerably more severe for the individual under scrutiny. We therefore wanted to know whether online surveillance by state agencies may lead to different reactions than surveillance by private industry. For the second part of the survey we thus used three different framings for our questions: one mentioning that surveillance was conducted by state agencies, one mentioning surveillance by private companies and a third mentioning surveillance without naming a specific organization. 104 people filled out the survey on state authorities (34.9%), 103 answered the survey on public companies (34.6%) and 91 reacted to the generalized condition (30.5%).

First we were interested in the extent of online surveillance users assumed across the three sources of surveillance ranging from ‘none’ of their online behaviors to ‘all of them’. In all three conditions, the average indicates that users assumed at least some of their behaviors to be monitored, although the values were highest for private companies (m=3.52) and lowest for state agencies (m=3.13; see also Figure 3). This difference was also statistically significant (F(2,294)=5.37, p<0.01). This was a general tendency, as neither genders, age groups nor user groups with different degrees of internet experience differed in their assumptions of online surveillance. Despite current debates, private companies seem thus still perceived as more intrusive than state agencies. As we will describe below, this does not mean that surveillance by state agencies is seen as less severe than that of private companies, however.

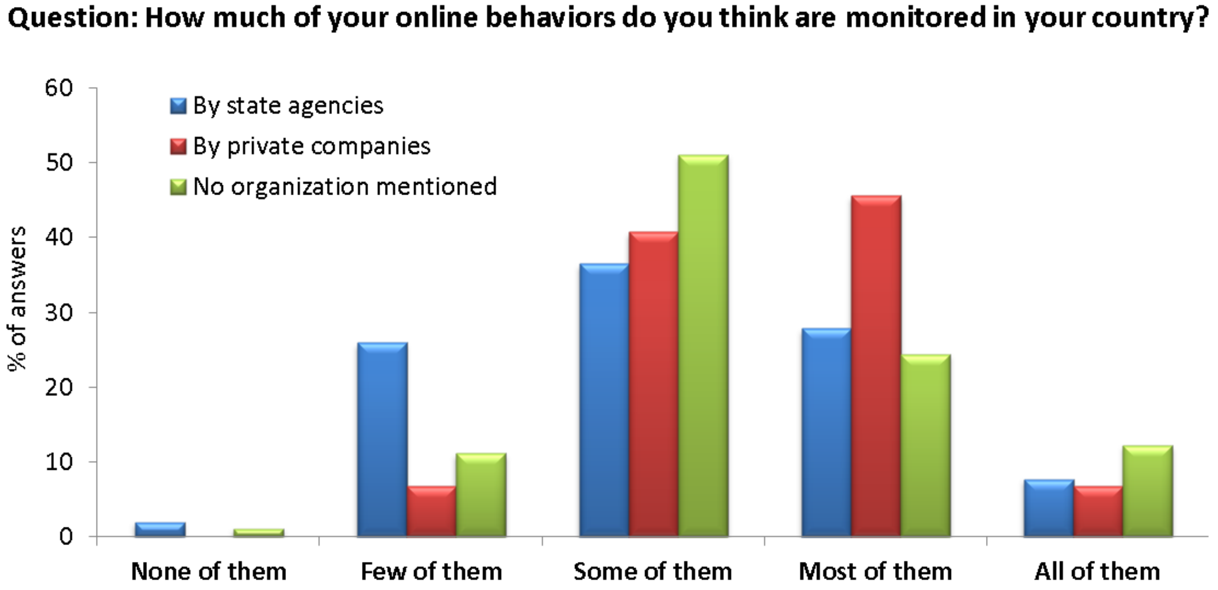

Figure 3. Assumptions of online surveillance by organization

Degree of acceptance and propensity to falsify personal information online

To understand, whether concerns of online surveillance impact the tendency to falsify personal information online we asked participants in all three conditions the same two questions:

- How acceptable they considered the falsification of personal information (*acceptance of falsification; from 1-not at all to 5-very much*).
- How likely they would falsify their own information (*propensity for falsification; from 1-would never do so to 5-have already done so*).

We asked for the falsification of five types of information, which are fixtures in most online profiles: (1) providing a false name, (2) providing a fake email address, (3) providing the wrong age, (4) using a fake photo, and (5) providing the wrong gender.

Taking all five aspects together, users showed a high level of acceptance for falsification (m=3.88, SD=0.99), while the propensity for falsification was somewhat lower (m=3.06, SD=1.05). Still, only a very small group of people (3.4%) indicated that they would never fake any of the information, whereas 7.4% indicated to have already done so for all five aspects.

Yet, interestingly falsification acceptance and propensity was not uniform across the five types of information. Using a false name and a false email address was seen as highly acceptable, whereas a false profile photo and wrong gender were considered considerably less acceptable (see Figure 4): Only 9.0% considered falsifying the own name as completely or highly unacceptable; for the falsification of the own gender this was 29.2%. The same trend emerged for the propensity of falsifying own information. 37.0% of participants indicated they had already used a fake name and email address, while 70.6% indicate they would never use the wrong gender or would be very unlikely to do so (see Figure 4). Users thus seem nearly five times more likely to indicate the wrong name and over six times more likely to provide a wrong email than indicate the wrong gender. This suggests that the falsification of personal information follows specific patterns; or phrased differently, that different pieces of information in a profile may have disparate likelihoods of being valid or invalid.

To compare the effect of the three surveillance sources, we summarized the five behaviors into one score for acceptance and one score for propensity, respectively. The three conditions did not differ in terms of falsification acceptance (F(2,285)=0.92, ns), but resulted in at least a marginal effect for falsification propensity (F(2,281)=2.77, p=.06). This was due to a slightly higher propensity for falsification when surveillance was conducted by private companies (m=3.26) compared to state agencies (m =2.91; t=–2.29, p<.05). Genders, age groups or length of internet use had no impact on either outcome.

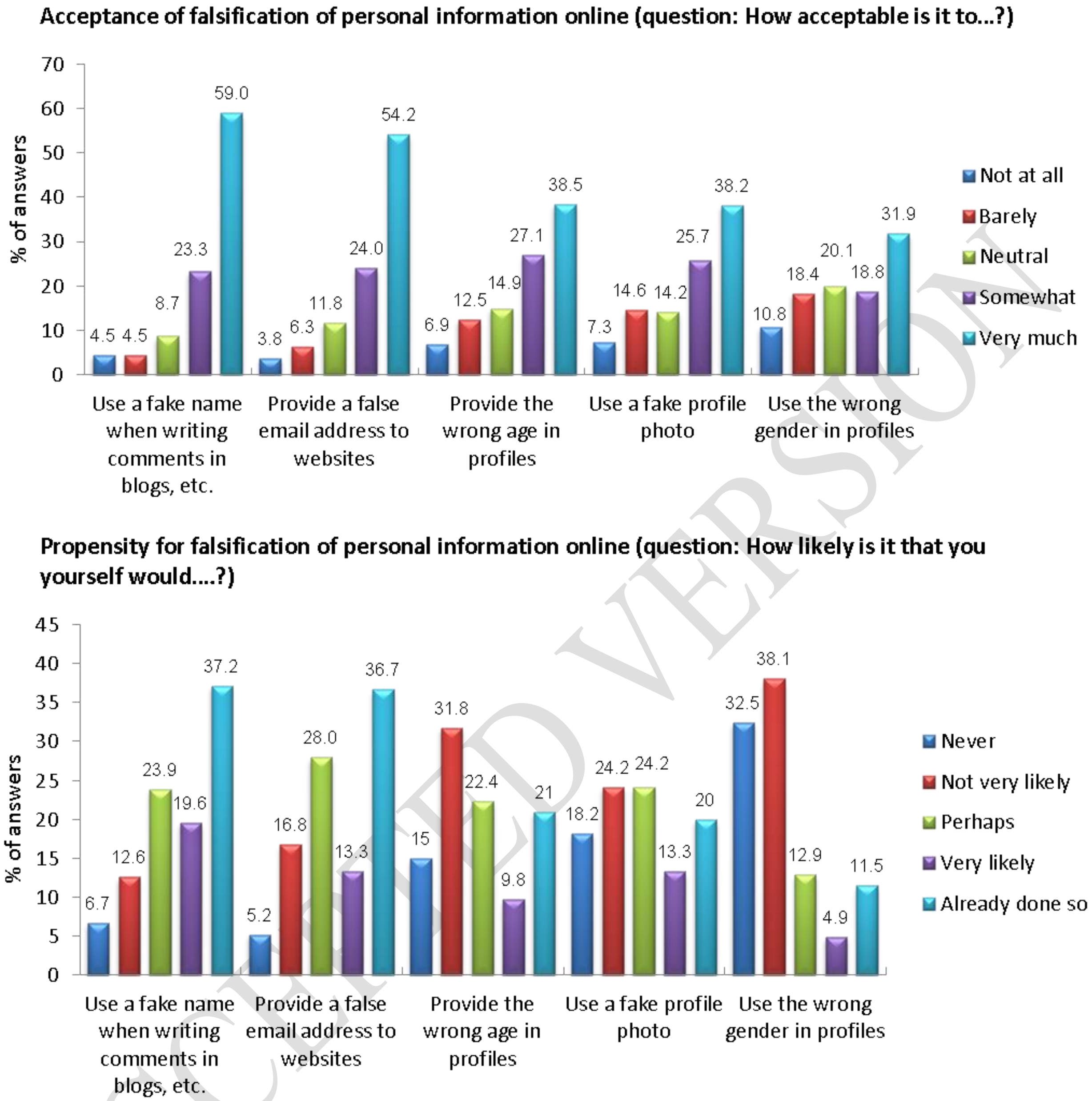

Figure 4. Acceptance and propensity for the falsification of personal information across all participants

Linking information falsification with surveillance assumptions and attitudes

Next we considered influences of surveillance awareness, attitudes towards surveillance and privacy concerns on information falsification. Because we used three separate versions of the survey to determine the influence of the organization conducting surveillance, the items on degree of surveillance awareness or their falsification acceptance and propensity referred to different entities (state agencies, private organizations or no organization in particular). We therefore calculated the correlations between surveillance awareness and information falsification for each of the three groups separately. This also gave us the opportunity to investigate, whether the context of surveillance had an impact on falsification behaviors. Table 1 reports the results for each of the three subgroups.

Table 1. Correlations between falsification behaviors, online surveillance assumptions and attitudes

GENERIC CONDITION (NO MENTION OF AN ORGANIZATION; n=91)								
		Mean	**Std. dev.**	**1.**	**2.**			
1.	Assumption of online surveillance	3.36	0.88					
2.	**Acceptance of information falsification**	3.80	1.06	**.22***				
3.	**Propensity for information falsification**	3.02	1.03	**.10**	**.66****			
CONDITION ‘SURVEILLANCE BY PRIVATE COMPANIES’ (n=103)								
		Mean	**Std. dev.**	**1.**	**2.**			
1.	Assumption of online surveillance	3.52	0.73					
2.	**Acceptance of information falsification**	3.99	0.96	**.13**				
3.	**Propensity for information falsification**	3.26	1.03	**.12**	**.63****			
CONDITION ‘SURVEILLANCE BY STATE AGENCIES’ (n=104)								
		Mean	**Std. dev.**	**1.**	**2.**	**3.**	**4.**	**5.**
1.	Assumption of online surveillance	3.13	0.96					
2.	General acceptance of online surveillance by state agencies	3.23	1.22	-.04				
3.	Benefits from surveillance	3.06	1.02	.01	.78**			
4.	Threats from surveillance	4.05	0.79	.11	-.38**	-.49**		
5.	**Acceptance of information falsification**	3.84	0.96	**.08**	**-.32****	**-.24****	**.21***	
6.	**Propensity for information falsification**	2.92	1.07	**.24***	**-.26****	**-.23***	**.13**	**.59****

* p < .05, ** p < .01; Pearson correlations, two-sided tests

Interestingly, assumptions of online surveillance had an impact only when framing online surveillance in the context of state agencies or as generalized activity. Here assumptions of online surveillance had a clear positive link with either the propensity to falsify personal information or the acceptance of this behavior (see Table 1). For surveillance conducted by private companies no significant link emerged. Again this suggests that the question of who conducts the surveillance may play a role in influencing concrete falsification behaviors. Surveillance by state agencies may trigger more concrete reactions than either generalized surveillance or monitoring by private companies.

As in the third condition all items referred uniformly to state agencies, this sub-sample gave us the opportunity to further investigate the link between attitudes towards online surveillance by those agencies and falsification. Here we found a very clear link between attitudes towards online surveillance, acceptance and propensity of falsification: The higher their general acceptance of surveillance and the higher the perceived benefits the less accepting users were of falsifying information and the less likely they were to do it themselves (see bottom of Table 1). Similarly, the more users perceived threats of online surveillance by state agencies, the more willing they were to accept falsifications.

In addition, acceptance of online surveillance moderated the relationship between falsification and assumed degree of surveillance. While higher assumptions of surveillance generally increased the propensity for falsification, this reaction was especially strong for people with a low acceptance of online surveillance by state agencies (see Figure 5). This suggests an important interaction between awareness and attitudes. While surveillance awareness alone may lead to information falsification, the main trigger seems the extent to which surveillance is seen as appropriate. This links tendencies for falsification of own information to how much a person considers state agencies as legitimate and trustworthy, thus emphasizing the potentially critical impact of negative press for the viability of OSINT-based decisions.

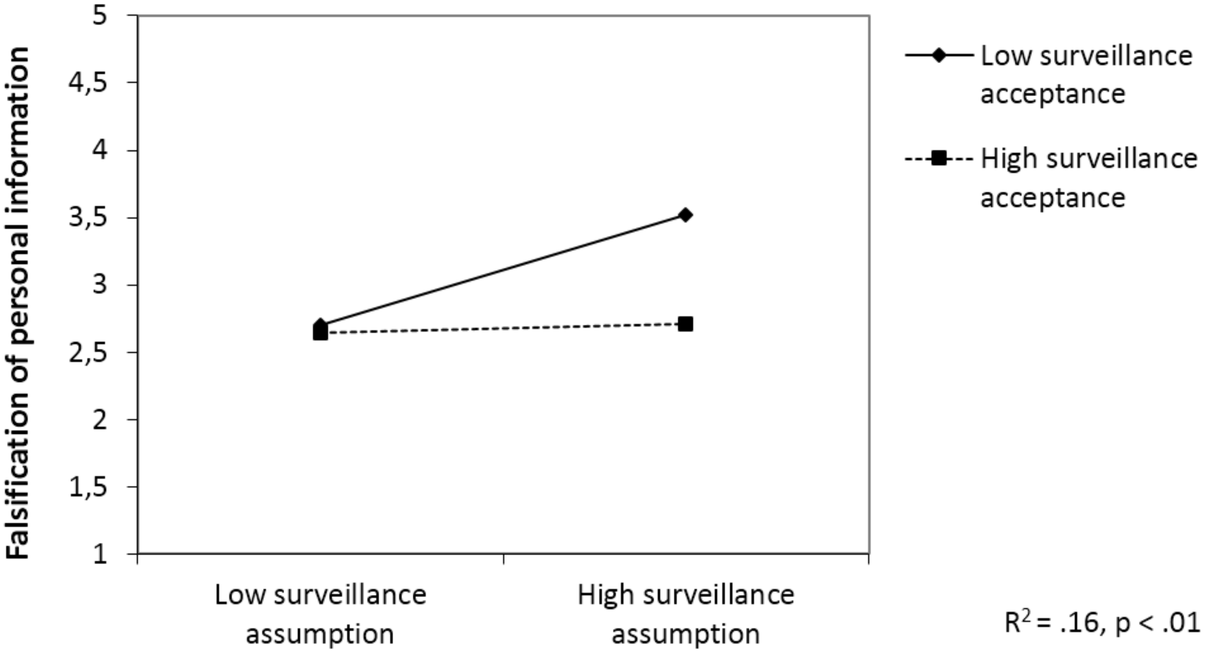

Figure 5. The role of surveillance assumptions and acceptance for information falsification

CONCLUSIONS

Our study demonstrates that discussions about ‘privacy’ versus the ‘rightfulness’ of online surveillance are more than a moral dilemma. Rather, the degree to which individuals are aware of online surveillance and the way they view the acceptability of this act, including the organizations implicated in it, can pose very concrete challenges for the validity of online data – and in consequence for the validity of decisions based on such data. While our study is certainly only a very small window into this complex issue, it demonstrates the potential for concrete, practical implications of surveillance for the usage of open source intelligence, specifically for law enforcement agencies. Surveillance is not neutral. To the contrary, our study attests that surveillance practices may threaten the integrity of the very data they are relying on.

Falsification tendencies as reactions to online surveillance create challenges for the usability of open-source data, increasing especially the efforts required for the validation of information. In the past, OSINT has been hailed as a cheap or even ‘no-cost’ source of operational information for LEAs.[4,16] Our findings suggest that increasing awareness of online surveillance, including painful revelations of problematic surveillance practices by states and LEAs, may severely reduce this benefit – at least for those internet users with a more critical outlook on state authorities and/or a higher need for privacy.

Technical solutions to counter the increased likelihood of falsifications are available. Dai and colleagues, for instance, proposed a number of 'trust score' computation models which try to determine data trustworthiness in anonymized social networks using a trusted standard.[5] Additional solutions are thinkable using validity pattern mining, reasoning-based semantic data mining and open-source analysis techniques. One important avenue for identification of false information is to identify possible links between profiles of a single user and then mine the data between profiles for validation. Often users explicitly link their profiles. For example, Twitter posts and Instagram photos can be organized so that they appear on the user’s Facebook timeline. This gives a direct and verified link to further information. Users may also post under the same pseudonym on a number of profiles. Collecting the data associated with each of these profiles provides further opportunity for corroboration. Similarly to Dai et al., another tactic could be to attempt to match the social graph of users across networks. By verifying where these networks overlap inconsistencies in personal data may be identified.

The most difficult part is determining the technological solutions that need to be employed in order to carry out the validation. Two such techniques are classification and association mining. Machine-learning based classification techniques can be used to establish a ground-truth dataset containing information that is known to be accurate. By training models on this data, outliers in new data indicate that the trustworthiness of the information may warrant further investigation. Association mining (or association rule learning) can be used to discover relationships between variables within data sets including social media and other open source intelligence.[12] These association rules can take data from the links discovered between multiple social networks and be used to validate the existing information.

Still, all these technical solutions rely on the cross-validation of open-source information with other (open or closed) sources. Growing falsification tendencies in the wake of increasing online surveillance awareness will make such cross-validations not only increasingly necessary, but also more complex and costly. Here, the notion of differential validity as evidenced in our data may provide a valuable perspective towards a more systematic and targeted approach to information validation by guiding validation efforts towards more or less problematic data. This approach uses the observation that personal information seems to possess systematic variations in its veracity (i.e., differential validity patterns). While our study focused only on a very small set of static information, we assume that similar patterns are observable also for other areas as well as more dynamic data.

An interesting question in this regard is how ‘volatile’ falsifications of personal information tend to be. Do users stick with one type of falsification (e.g., consistently modify name, relationship status or age across services) or do these pieces of information vary across services? Also, do users always use the same content (e.g., always the same false date of birth or photo)? Extending our knowledge of such falsification/validity patterns can considerably reduce the efforts involved in the validation of OSINT-based data. In our current study we did not investigate the reasons behind the differences in falsification acceptance and propensity for the various types of personal information. Getting a clearer understanding of these reasons could tell us much about the contexts in which falsification are more or less likely as well as the strategies internet users employ to remain private.

Clearly, we cannot return to the days of the ‘uninformed’ or ‘unaware’ internet user, and LEAs therefore need to find ways to deal with the consequences of online surveillance awareness and the possible ramifications it may have for the trustworthiness of online information. While we do not suggest that OSINT will lose its value for investigation processes, we certainly think that LEAs will have to become more sensitive to the reactions their own practices may create for the viability of their methods and in consequence the decisions based on these methods.

Employing ever more advanced technical solutions is certainly not the (sole) solution. Our findings made clear that even more than the pure fact of online surveillance, the perceived purpose and legitimacy of the act are the main drivers behind the extent to which users alter their behaviors online. This not only explains the role of (largely negatively tinted) public discussions for the behavioral changes in the wake of the Snowden revelations.[10] It also outlines the criticality of properly legitimizing online surveillance to reduce distrust in LEAs and thus pressures towards information falsifications and probably behavioral changes more generally.

References

1. Barlett, J., Miller, C., Crump, J. and Middleton, L. Policing in an Information Age, London: Demos (Mar. 2013).
2. Bell, P. and Congram, M. Intelligence-led policing (ILP) as a strategic planning resource in the fight against transnational organized crime (TOC). International Journal of Business and Commerce 2, 12 (2013), 15-*28.*
3. Best, C. Challenges in open source intelligence. In Proceedings of the Intelligence and Security Informatics Conference (Athens, Greece, 12-14 Sep. 2011), 58-62.
4. Best Jr, R.A. and Cumming, A. Open Source Intelligence (OSINT): Issues for Congress. Congressional Research Service (Dec. 2007).
5. Dai, C, Rao, F.Y, Truta, T.M and Bertino, E. Privacy-preserving assessment of social network data trustworthiness. In Proceedings of the 8th International Conference on Collaborative Computing (Pittsburgh, USA 14-17 Oct. 2012), 97-106.
6. Gibson, S. Open source intelligence: An intelligence lifeline. The RUSI Journal 149, 1 (2004), 16-22.
7. Joinson, A.N., Reips, U.D., Buchanan, T. and Schofield, C.B.P. Privacy, trust, and self-disclosure online. Human–Computer Interaction 25, 1 (2010), 1-24.
8. La Stampa. Mafia, fermato Vito Roberto Palazzolo scovato a Bangkok grazie a Facebook. (March 31, 2012); http://www.lastampa.it/2012/03/31/italia/cronache/mafia-fermato-vito-

roberto-palazzoloscovato-a-bangkok-grazie-a-facebook-vpnxhM5z5chH3iuIjttksJ/pagina.html

9. Lenhart, A., Madden, M., Cortesi, S., Duggan, M., Smith, A. and Beaton, M. Teens, Social Media and Privacy. Pew Internet and American Life Project Report, 2013; http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.
10. Marthew, A. and Tucker, C. Government Surveillance and Internet Search Behavior. Working paper, March 2014; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564
11. Mercado, S.C. Sailing the sea of OSINT in the information age. Studies in Intelligence 48, 3 (2009), 45-55.
12. Nancy, P., Ramani, R.G. and Gracia Jacob, S. Mining of association patterns in social network data (Facebook 100 Universities) through data mining techniques and methods. Advances in Computing and Information Technology. Berlin, Springer, 2013, 107-117.
13. Neri, F., Aliprandi, C., Capeci, F., Cuadros, M. and By, T. Sentiment analysis on social media. In Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (Istanbul, Turkey, 26-29 Aug. 2012), 919-926.
14. Omand, D., Bartlett, J. and Miller, C. Introducing social media intelligence (SOCMINT). Intelligence and National Security 27, 6 (2012), 801-823.
15. Ratzel, M.P. Europol in the combat of international terrorism. NATO Security through Science Series, Volume 19, Amsterdam: IOS Press, 2007, 11-16.
16. Steele, R.D. The importance of open source intelligence to the military. International Journal of Intelligence and Counter Intelligence 8, 4 (1995), 457-470.
17. Steele, R.D. Open source intelligence. Handbook of Intelligence Studies. New York, Routledge, 2007, 129-147.
18. Stohl, M. Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games? Crime, Law and Social Change 46, 4-5 (2006), 223-238.
19. The Telegraph. Connecticut school shooting: Police warn of social media 'misinformation', (Dec. 16, 2012); http://www.telegraph.co.uk/telegraphtv/9748745/Connecticut-school-shooting-police-warn-of-social-media-misinformation.html