In: Wohlgemuth, V., Fuchs-Kittowski, F., and Wittmann, J. (eds.)
Environmental Informatics – Stability, Continuity, Innovation. Current trends and future perspectives based on 30 years of history. Adjunct Proceedings of the EnviroInfo 2016 conference. pp. 151–156. Berlin (2016).

Reception of Terror in Germany – Security, Privacy and Social Media

Christian Reuter, Robin Gellert, Gordian Geilen[1]

1. Introduction

Privacy or security? Can those two maxims be harmonized? Or are they part of a zero-sum game, which does not allow any compromises? At least, this notion seems to be present in the civil population: Edward Snowden let the cry for more privacy in the internet become loud and his revelations have come across a great positive echo in several populations. But there was another political development. The Islamist terror has become almost omnipresent, and is still today. The so called "Islamic State" wages war against all those, who do not surrender to it and its believes. Its most devastating attack in Europe is represented by the Paris attacks in November 2015, with over 130 civilian casualties. New safety concepts were developed to prevent such attacks in the future. But one detail became very crucial: the terrorists had communicated and planed the attack via the internet. Both guiding ideas of security and privacy have gained additional benefit since 2013. Furthermore, both are welcomed by the population and are equally demanded by them. But is coexistence between those two seemingly contradictory concepts even possible if both concepts need to be equally executed? In this paper we examine a survey, in which we asked German citizens if they are, regarding the Paris attacks, willing to give up privacy for increased security. For this, we focused on privacy in social networks and the surveillance of terrorists in those domains. In addition, this paper will show clusters of opinions, wishes and tendencies of the German population regarding the zero-sum game "Security and Privacy".

2. Related Work: Privacy, Terrorism and Social Media

After the 9/11 attacks, Davis and Silver [1] investigated the willingness of the American population to trade civic rights for higher personal security. They found out that the willingness reinforces as the perception of threat increases, but this effect interacts with the trust in government. In contrast, another study in Europe could not find any significant correlations [2]. Denninger [3] discusses the relation of liberty and safety in the context of the anti-terrorism act but concludes that this rather derives from the dialectic of protection and anxiety. For the consideration of safety and liberty in the context of terrorism, Lepsius [4] argues that safety is not even an position because it is only connoted negatively in terms of defence of threat. Data preservation, a very controversial method to store all user-generated content of the digital world for a short time encounters in the German population to date considerable resistance due to the associated immense restriction of the privacy of Internet users [5].

Bartlett und Reynolds [6, p. 10] emphasize that since the NSA affair in 2013 and the revelations of Edward Snowden, the emerging demand in the population is the encryption of own data in the internet,

[1] Contact: Dr. Christian Reuter, Universität Siegen, christian.reuter@uni-siegen.de

especially in social media. However, even before Snowden existed the wish for more privacy in the population [7]. Bartlett und Reynolds [6, p. 10] talk about an increased public concern about personal data and privacy, whereby the private usage of encryption services such as "Tor" is raising, too. Even the operators of social networks themselves adapt higher security precautions for the safety of user privacy. Furthermore, after the revelations of Snowden, "Anti-Facebook" networks have become established (ibid.), which concentrate more on user privacy and special software for privacy protection.

Because of the reports above one can state that at least from mid-2013 privacy has gained of immense importance within the community of internet users and members of social networks. As the attacks in Paris demonstrate, domains "under the radar" were also established by terrorists as one can see in web presences of Al-Qaida, Taliban, FARC or IS.

The literature research shows two unambiguous facts: For one thing, the internet in general and the social network in special are used actively by all participating persons (users, governments and also terrorist groups), and for another it is clear that there are methods for the establishment of antiterrorist measures in the internet [8], but they all run in legal settings and seem to be limited due to the Edward Snowden spy affair. The most important aspect is the boundary between the desired privacy and the security needs of the people. There has been a terrorist attack in central Europe, planned over a network, which is the reason why one should consider if it was better, like Jeberson and Sharma [9] mentioned, to expand the current methods or to reduce the users' privacy in social networks for governmental activities.

Due to the available literature and the overall political context and world events, the following hypothesis can be constructed for the empirical study: Despite the wish for privacy, most of the users would be willing to waive it in favour of more security, at least temporarily and partially. This hypothesis is explicable with the fact that the Snowden revelations could have contributed to the wish for more privacy, but the advancing activities of the IS frighten the users so much that they would help the government by reducing their privacy. The given explanations lead to the research question of this paper: Which consequences do terrorist activities have on the security feelings and how far are they willing to waive their liberties in favour of more security? This question leads to another question, which will be important for this paper: How is the reception of fear of terrorism and warning, especially in social media?

3. Methodology: An Explorative Survey

In the following chapter, we present our empirical study. Our primary focus was to reduce the complexity of the topic by temporal consideration or in other words: our survey should contain questions, which are easy to comprehend and do not take long time to answer them to avoid rejection of participation due to a too long or complex survey. First of all, we describe the design of our questionnaire and the characteristics of the subjects. After that, we show the evaluation and clustering of the findings of the study.

To explore the question and focus of this work, we chose a questionnaire with a majority of quantitative questions, which shall capture the subjective sense of security and wishes of the German population. The primary focus of our survey is to answer the question, whether the subjects are willing to relinquish parts of their private sphere to gain more security. To get insides in this extensive and intimate topic, we asked an open question. All quantitative questions contain nominal and ordinal scale level. The first regards questions of wishes and experiences of the subjects, while the latter are used to value statements referring to the

given topic. With this, we could not only establish a cluster of individual experiences and opinions, but also form a cluster of utopic statements and therefore conclude in establishing mood- and priority-clusters.

Our survey was spread via social media, e-mail and personal contact and contains 61 answers of subject from Germany with a minimum age of 18. The majority of the subjects were between 18 and 30 years old (67%), followed by the subjects between 31 and 40 years (20%). The smallest group were the subjects older than 40 years (13%), while the survey has a balanced ratio regarding the sex of the subjects: 49% were female and 51% were male. With half of all participants (49%), students made up the majority of the participants, followed by employees (39%) and self-employed (7%). The smallest group were made up of persons currently unemployed (5%).

4. Empirical Results: No General Tendency

In the following section we will present selected results of our survey [10]. The absolute majority (89%) of the participants mention, that they had experienced misuse in social networks (through radical persons or groups). On this stage, due to a high response rate especially to this question, we can assume that such radical or extremist misuse in social media is not on the fringes. This is a first important finding referring to a possible, positive willingness to allow more and severe observation measures in social media, for personal experiences in general promote the willingness to change a given status quo.

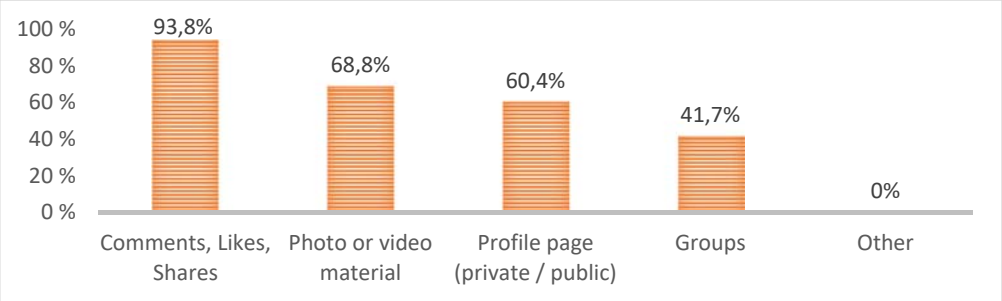

Figure 1: Participants´ answers to the question regarding experienced extremism or radicalism in social networks. Multiple appointment possible (n = 48).

This in reverse confirms the so called Sankt-Florian-principle, in English also known by the acronym *Nimby (Not in my backyard).* The principle implies that the willingness of citizens to participate in certain topics and events is mostly limited to their own living environment respectively participation only then occurs, when oneself is affected by an outer change (*in my backyard)* and a possibility of a dislocation of this change is not given. If these findings are correct and how the willingness to reduce privacy in social networks to gain more security is portrayed in our study, will be discussed later.

94% of those participants, who already experienced extremism or radicalism in social networks (fig. 1) mention that they have encountered it in form of commentaries, likes and shares of other users, followed by distinct graphical footage and digital videos (69%), private or public profiles (60.4%), as well as inside of groups of social networks (42%). Keep in mind, that multiple mentions were possible. The follow-up question, in what kind the user experienced extremist or radial content, should be considered as significant. Here too, multiple mentions were possible. The two most mentioned answers by the participants with 94%

and 90% are xenophobia and racism, followed by agitation against ethnic minorities (56%) and homosexuals (29%). Another important finding are experiences of appeals for radicalization via social media by groups such as the Salafists or even the IS, which a quarter of the participants (25%) have experienced. This can be valued as an indicator of an active presence of such radical groups in social media.

The responds to the question if the participants were willing to reduce their privacy in social networks and media to gain more security in exchange and if they would include the tracing of terroristic organizations and their supporters, were greatly ambivalent but also show a distinct tendency. 44% of the participants were willing to at least partially give up parts of their privacy, while 36% answered in the negative. Another 20% of the participants were unsure regarding this question. To this point it must be stated, that the opinions of the participants regarding a reduction of their privacy in favour of counter-terrorism measures differ. Only with the supplement of the follow-up question, an open question, a precise cluster about the opinions of the participants can be generated. Especially with the open answers of unsteady participants, who answered the previous question with a characterisation of "3", can be analysed more direct (fig. 2).

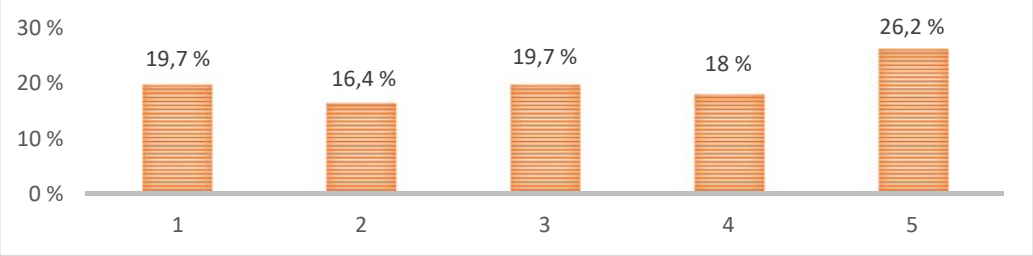

Figure 2: Participants´ answers to the question concerning their willingness to renounce privacy in favour of higher security (n = 61). Scale: 1 ("not agree at all") to 5 ("totally agree").

After the analysis of both questions, we could generate three clusters to summarize the opinions of our participants. They shall be explained in the following:

- **Strong Affection:** This group contains those participants, who answered the question of giving up privacy in exchange for more security with a characteristic of "4" or "5". They regard social networks as a public environment and argue, that every user must, under this premise, decide for him or her which information he or she wants to give to this public environment. Those participants are willing to give up their privacy to enable a better tracing of terrorists, for privacy is not given in social media ("*who is using social networks should be aware of what he posts there*", P41) or willing to partially reduce their privacy. Private messages or group memberships are those parts of privacy, which the participants are willing to give up the most.
- **Strong Antipathy:** A slightly smaller part of our participants think contrary and are strictly against a surveillance of social networks and are not willing to give up parts of their privacy in such domain. In this cluster one answer of a participant is very interesting, which complements the rest of the "opponents" of giving up privacy: "*Generally exchanging private sphere for safety does not seem to be fair to me: safety cannot be guaranteed a 100%. Therefore, I would not be willing to relinquish privacy*" (P14). This tonus can be found throughout the whole cluster and

shows, that these participants do not believe in an increasing security by surveillance of social networks and furthermore fear its misuse by public authorities, thus not trusting them und therefore are not willing to give up any part of their privacy.

- **Give-and-Take:** To those participants, who answered with a characteristic of "3", a trend indicator can be added by including the open answers into a cluster on its own. Those persons would not give up their privacy without cause, but are in return to prevent crimes willing to take a compromise and "offer help".

There are two aspects, which shall not be underestimated, when considering these clusters. First, the cluster "strong affection" is the major one. Just alike it is shown, giving up privacy in social domains is no novelty for this cluster. Second, we could show a synergy between the two clusters "strong affection" and "give-and-take". The latter is, just like the first, willing to give up at least partially and temporally their privacy. If we consider these two clusters as one unity, we can make out a tendency: For the majority, namely 63.9%, giving up their privacy is a realistic possibility.

5. Discussion and Conclusion: Privacy and Security

Privacy or security? Can those two maxims be harmonized? This was the question stated in the introduction. According to our finding, the "privacy-boom" of 2013, caused by the NSA-affair through Edward Snowden, still seems to be present today. Many of the participants of our study, which can be located in the second cluster "strong antipathy", argue that an increasing surveillance, since an absolute security is never given, only serves to spy on the fellow citizens for the purpose of market research or respectively "general control". On the other hand, the first cluster, "strong affection", wishes surveillance of the internet, because they consider it as a public environment.

Those two clusters, almost equal in their number of participants, show the two excesses regarding this controversial topic. Therefore, the third cluster "give-and-take" is of great value. Participants of this cluster care for their privacy, but are willing, in reasonable ground for suspecting, to give up privacy at least partially or temporally. By reflection of single clusters, an ultimate tendency regarding privacy or security cannot be constituted completely. There might be a readiness for compromises to give up privacy, but only in exchange for a promise to prevent and track down criminals or terrorists and their activities. With this perspective we need to make clear, that privacy is still an important aspect for our participants, but, as our study suggests, the overall conscious regarding social networks as public environments has changed and a general readiness to compromise to give up parts of privacy in social networks is at hand. But if we view the clusters "strong affection" and "give-and-take" as one unit, only then it is possible to make out the tendency as described above: To experience social networks as public environments with limited privacy, which in certain circumstances can be, much like in reality, intervened by executive forces.

The readiness respectively the strong affection to an increased observation of social networks can be based on the finding, that 88.9% of our participants have experienced radical or extremist presences, groups, postings or the like in social networks. If we further notice, that, due to the advance of the IS and the ongoing war in Syria and Iraq, the regain of strength of right winged parties and the refugee-crises, media and news are mostly concentrated on such topics, we can assume that participants of the clusters 1 and 3

have a certain and critical perspective on these parties, groups and extremist body of thought and possibly react more sensible, due to their extensive experiences with such topics in social media. To analyse such cross-references, a further study is needed, which should concentrate on experiences with extremist body of thoughts in social media. Furthermore, a study regarding socio-cultural and socio-economic aspects of the participants of the different clusters is needed.

As a conclusion for this study, we need to assume that at least the German citizens, that participated in our survey, are deeply divided, when dealing with the topic "security measures for the price of privacy" (see details in Reuter, Geilen & Gellert [10]). The revelations of Snowden still have influence on the sensibility regarding privacy in social networks, while the ongoing attacks of the IS show that there is indeed a readiness to compromise and give up parts of one's own privacy in such media. However, a requirement for this is an increased security or prevention of terrorist attacks similar to those happened in Paris. A tendency to give up privacy unconditionally for security could not be found.

Acknowledgements

The research project EmerGent' was funded by a grant of the European Union (FP7 No. 608352).

References

[1] D. W. Davis and B. D. Silver, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America," *Am. J. Pol. Sci.*, vol. 48, no. 1, pp. 28–46, Jan. 2004.

[2] M. Friedewald, M. van Lieshout, S. Rung, M. Ooms, and J. Ypma, "Privacy and Security Perceptions of European Citizens: A Test of the Trade-off Model," *IFIP Adv. Inf. Commun. Technol.*, vol. 457, pp. 54–70, 2015.

[3] E. Denninger, "Freiheit durch Sicherheit? Anmerkungen zum Terrorismusbekämpfungsgesetz," *Polit. Zeitgesch.*, vol. 10/11, pp. 22–30, 2002.

[4] O. Lepsius, "Freiheit, Sicherheit und Terror: Die Rechtslage in Deutschland," *Leviathan*, vol. 32, no. 1, 2004.

[5] M. Koshan, "Vorratsdatenspeicherung – verfassungsrechtliche Rahmenbedingungen und rechtspolitische Verortung," *Datenschutz und Datensicherheit - DuD*, vol. 40, no. 3, pp. 167–171, Mar. 2016.

[6] J. Bartlett and L. Reynolds, "State of the art 2015: a literature review of social media intelligence capabilities for counter-terrorism." Demos, Sep-2015.

[7] M. J. Metzger and S. Docter, "Public Opinion and Policy Initiatives for Online Privacy Protection," *J. Broadcast. Electron. Media*, vol. 47, no. 3, pp. 350–374, Sep. 2003.

[8] C. Reuter, K. Pätsch, and E. Runft, "Terrorismus und soziale Medien – Propaganda und Gegenpropaganda," in *Mensch & Computer: Tagungsband*, 2016.

[9] W. Jeberson and L. Sharma, "Survey on counter Web Terrorism," *COMPUSOFT, An Int. J. Adv. Comput. Technol.*, vol. 4, no. 5, pp. 1744–1747, 2015.

[10] C. Reuter, G. Geilen, and R. Gellert, "Sicherheit vs. Privatsphäre: Zur Akzeptanz von Überwachung in sozialen Medien im Kontext von Terrorkrisen," in *Informatik 2016: von Menschen für Menschen*, 2016.