Renouncing Privacy in Crisis Management? People's View on Social Media Monitoring and Surveillance

Larissa Aldehoff, Meri Dankenbring, Christian Reuter
Science and Technology for Peace and Security (PEASEC), TU Darmstadt
aldehoff@peasec.tu-darmstadt.de; reuter@peasec.tu-darmstadt.de; www.peasec.de

ABSTRACT
Social media is used during crises and disasters by state authorities and citizens to communicate and provide, gain and analyze information. Monitoring of platforms in such cases is both a well-established practice and a research area. The question, whether people are willing to renounce privacy in social media during critical incidents, or even allow surveillance in order to contribute to public security, remains unanswered. Our survey of 1,024 German inhabitants is the first empirical study on people's views on social media monitoring and surveillance in crisis management. We find the willingness to share data during an imminent threat depends mostly on the type of data: a majority (63% and 67%, respectively) would give access to addresses and telephone numbers, whereas the willingness to share content of chats or telephone calls is significantly lower (27%). Our analysis reveals diverging opinions among participants and some effects of sociodemographic variables on the acceptance of invasions into privacy.

Keywords
Social Media, Privacy, Security, Crisis Management, Surveillance.

1 INTRODUCTION

Data in social media shared by inhabitants can be very useful for state authorities such as police, fire and rescue organizations in cases of crises and disasters, which is also shown by the fact that social media are a crucial part of ISCRAM research. Analyzing all ISCRAM papers related to social media from 2004-2018 Reuter et al. (2018), found that the papers predominantly examine social media posts in English, mostly posted on Twitter. Geographically, the analysis focused on crises in Europe and North America. Another conclusion is that in order to realize broader analyses of social media content, it will be necessary to overcome the obstacle of "even more complicated data-extraction scenarios" (Reuter et al. 2018). This obstacle is a consequence of the current increase in awareness for privacy issues and resulting changes in online behavior, as well as terms of use. Examples in point are the growing popularity of discarding Facebook's public post search feature and of the sandbox mode on Instagram. The European General Data Protection Regulation (GDPR) efficiently curbed the amount of user data that is publicly accessible for processing. Moreover, the above-mentioned debate on privacy may lead to a decrease in people's willingness to having their online behavior analyzed (Reuter et al. 2018). Notwithstanding the usefulness of data collected from social media and by surveillance measures in cases of crisis and disaster, privacy concerns have to be considered when using this data for crisis management. One part of this complex issue is the people's perception of privacy.

Therefore, this paper addresses the research question: *How far are people willing to provide their data in social media and accept surveillance to support authorities in cases of crisis and disaster?* We provide answers to the question which types of data people are more concerned to share and under what conditions they are willing to make their data available. Additionally, we ask about people's opinions on several surveillance measures aimed at increasing public security in cases of imminent threats. Some of those measures are already practiced in Germany or elsewhere, others are still broadly and controversially discussed.

Through a representative survey of 1,024 respondents, we found that German inhabitants were only partially willing to give up their privacy on social networks and, depending on the crisis context, would give specific authorities access to non-intimate but private data. Nevertheless, this disposition to (partially) waive privacy to support state authorities' crisis management goes hand in hand with the demand of holding the state accountable:

inhabitants want increased transparency of data collection as well as rights regarding the use of collected data by state authorities. We analyzed sociodemographic factors of our subjects such as gender, age and educational background and their influence on the answers given. By means of simple regression analyses we partly found correlations, partly no correlations between these criteria. Overall, there is a tendency for subjects to cooperate on certain conditions such as transparency of monitoring and selection of data transmission.

In the beginning of the paper we outline the state of research concerning social media in crisis management and users' perception of privacy in social media and surveillance (section 2). We will continue with the methodology (section 3) and the results of our analysis (section 4), followed by a conclusion and implications for further research (section 5).

2 STATE OF RESEARCH

The following section reflects the current state of research concerning social media as a tool in crisis management as well as on public perceptions of privacy concerning social media monitoring and surveillance. Moreover, it presents the research gap we aim to address.

2.1 Social Media in Crisis Management

Social media are becoming more sophisticated by the day. This is not only true for social media in day-to-day use, but also their employment in cases of emergencies (Reuter, Hughes, et al., 2018; Reuter & Kaufhold, 2018). Information technology plays a major role in context of peace and security (Reuter, 2019). The first use of social media for purposes of disaster support documented and detected by the authors took place in 2001. Since then, the use of social media has increasingly intensified, provoking a growing amount of research on the topic. It has analyzed different cases and users, practices and tools with diverging methodologies. A main goal being the support of actors involved in crises, emergencies or disasters, depending on their nature and size. The research and advancements made so far are summarized under the term of crisis informatics (Hagar, 2007; Palen et al., 2009).

Reuter & Kaufhold (2018) found studies emphasizing the role social media played in the handling of a significant majority of large emergencies in the last decade, and even in most emergencies since 2001. Although many studies initially focused on the US, research studying other continents is making up ground, thus enabling systematic comparisons across countries, regions and kinds of emergencies. Nonetheless, most studies still focus on Twitter, which is possibly due to the ease of data selection on the platform. Reuter & Kaufhold's (2018) analysis was centered on the analysis of different usage patterns, such as communication between citizens (i.e. C2C), communication from authorities to citizens (i.e. A2C), communication from citizens to authorities (i.e. C2A) and between authorities (A2A). It is important to note that the perception of social media varies across users, i.e. diverges between authorities and citizens. Although both tend to pose similar challenges, such as a lack of trust and knowledge, citizens still expect that authorities monitor social media. Thus, expectations have to be aligned in order to overcome existing problems. Due to the almost omnipresent nature of social media and its low entry and usage barriers ,"the role held by members of the public in disaster (…) is becoming more visible, active, and in possession of greater reach than ever seen before" (Palen & Liu, 2007). Each citizen can post information about an event, thereby helping the authorities and other citizens. The willingness to use voluntarily communicated information is ambiguous. Reuter & Spielhofer (2017) investigated the reasons why citizens do not use social media for crisis communication and identified them as "mistrust as well as the perceived lack of a clear purpose for using social media in emergencies" (Reuter & Spielhofer, 2017).

In addition to the positive aspects of social media collaboration between citizens and public authorities, there are also negative aspects, as illustrated by the case of the Munich rampage in the summer of 2016. While the gunman was hunting for people in the shopping center, eyewitnesses posted a number of videos on Twitter and Facebook virtually live. The police later criticized these actions on social channels, considering them to have unsettled and panicked the population. In addition, the perpetrator could have been informed about the ongoing police operation as well as countermeasures of the emergency services. A helpful communication tool such as social media can only be used effectively if actors are aware of consequences of certain courses of action (see Dobel, 2016; Schillat, 2016). In emergencies people are usually willing to help, but still do not want to be monitored.

2.2 Perception of Privacy in Social Media and Surveillance

Social media do not only pose chances, rather, looking at crisis management, there are several problems, risks and challenges (Kaufhold & Reuter, 2019). The revelations of Edward Snowden or the Cambridge Analytica affair are just two broadly discussed examples for the potential misuse of data and show the pressing relevance of privacy. One important aspect of privacy is its perception by users. The existing research on the privacy paradox suggests that people are willing to limit or even renounce their privacy for relatively small benefits, or even none

at all (Norberg et al., 2018). But further research showed that this approach is too narrow. First of all, it has to be noted that users do not necessarily understand that they are sharing personal data to be able to use "free" social networks, services and apps (Turow et al., 2015). Additionally, they lack knowledge on the consequences of sharing their data, and if so, are unable to regain control over data already shared (Acquisti & Grossklags, 2006). Therefore, users do not make an informed and deliberate choice. Even users who are aware of this, often do not see an alternative and share their data because the effort to search for and use other services is considered as to large by users, e.g. because of fast-changing terms of use (Buxmann, 2015, p. 143) As a result, they feel that they are losing control over their data (Degli-Esposti et al., 2017). One example is a value-driven approach to privacy. Buxmann focuses on the value people attach to their data. He surveyed users' opinions on data driven business models in social networks and their behavior if they disapprove of those. In 2012, 62% and in 2014 even 75% of respondents disapproved such business models – at the same time only 14%, especially older users, refused to use those services (Buxmann, 2015).Simultaneously, users appear to refuse to pay a significant amount of money for more privacy-friendly services. This can be explained with the privacy paradox, but factors such as awareness, knowledge, motivation and considered effort need to be analyzed in more detail than this concept allows.

The picture crystallizing of people's perception of surveillance is similar to the one of privacy in social media. Often people perceive surveillance as an inevitable art of the digital revolution. Even if they are aware of it, they think they need to accept it to avoid important social or economic disadvantages (Turow et al., 2015). Only a minority of people "try to avoid, evade or circumvent surveillance by adopting different strategies, from the intentional provision of inaccurate information, to the adoption of anonymization and privacy-preserving tools" (Degli-Esposti et al., 2017). Ball stresses that although people tend to do little to counter surveillance, this does not mean that surveillance is meaningless for them. It may be accepted or even approved of because providing data can satisfy individual anxieties, or patriotic or participative values. Another factor is that there is often no identifiable observer who exercises perceivable control. Furthermore, the pleasure of performative display overrides the scrutiny that comes hand-in-hand with self-revelation (Ball, 2009, p. 641).

Looking at surveillance from the privacy angle, Kasper (2005) introduces a sophisticated typology of privacy breaches, which will be introduced in further detail below, and finds that forms of intrusions are covered with different intensities in US newspapers. Thus, the public perception of privacy strongly depends on the context and on the type of invasion in it, and is subject to change: Kasper (2005) finds that – possibly due to historical events and changes in state practice – perceptions of invasions into privacy changed in the period of 1990 to 2003, for example increasing the relevance of clandestine forms of data gathering in the public debate (which she calls *stockpiling*).

2.3 Research Gap

Research on the question when and under what conditions people are willing to either, allow the state access to a well-defined set of information on them, restricted to the period of time constituted by a severe crisis or disaster, or, grant the state rights to conduct long-term surveillance efforts, in order to increase public security – remains unanswered by previous research. Reuter & Spielhofer (2017) indicate that mistrust and lack of a clear purpose are reasons for people to reject using social media in emergencies. It remains unclear under what conditions inhabitants support their use if this improves crisis management. The research of Degli-Esposti et al. (2017) shows that the "current security policies and solutions are somehow perceived as inadequate by citizens, whose demands, opinions and perceptions need to be further explored" (Pavone et al., 2017). Kokolakis demands further research in his work to "build a clearer picture of the relation between privacy attitudes and behavior" (Kokolakis, 2017). Therefore, this paper addresses these questions concerning conditions and kind of data as well as the view on surveillance measures.

3 RESARCH DESIGN AND METHODOLOGY

This paper addresses the yet unclear perception of privacy by people concerning social media monitoring and surveillance in cases of crisis. In 3.1 we outline our theory approach and the design of survey questions, 3.2 explains the survey design and conduction and 3.3 presents the respondent's characteristics.

3.1 Theory and Design of Questions

To be able to contribute to the perception of privacy we use Kasper's approach of privacy. She identified several problems with existing definitions of privacy: 1) definitions appear to be not properly specified, i.e. they are too broad or too narrow, 2) they have a strong cultural bias and 3) "tend [...] to be value-driven" (Kasper, 2005). Therefore, she developed a typology of privacy by understanding privacy "from the standpoint of its invasion" (Kasper, 2005). This typology for invasion accounts "for all possible ways in which one's privacy can be invaded and to identify distinctive characteristics associated with each type of invasion" (ibid.). Our interest expands over the typology's categories e*xtraction* and *observation*. To measure public perception of forms of *observation*, the

third question (called Q13, for the exact wording of the questions see Fig. 1-4) on different fictional laws was asked. The question addresses *observation*, because the state is granted intrusive rights to collect and store information on and metadata generated by its citizens, which comprises different forms of surveillance. Kasper (2005) defines *observation* to "mainly consist of 'watching,' [which] refer[s] to surveillance in general" (Kasper, 2005). She subclassifies *observation* into *physical observation* (i.e. "surveillance of a physical entity" (ibid.), e.g. by surveillance cameras), *communication observation* (i.e. "the interception and/or surveillance of communication in any form: telephone, mobile phone, e-mail, fax [...] and so forth" (ibid.)) and *behavioral observation* (i.e. "the explicit monitoring of a behavior" (Kasper, 2005), such as "track[ing] consumers' buying *habits*" (ibid.)). Question 13 addresses these forms of *observation* separately, by first asking whether respondents would be willing to grant the state the right to surveil them via CCTV (*physical observation*), via internet communications (*communication observation*) and lastly, all information available, which includes the former two, but adds the possibility of observing *behavioral* habits. Nonetheless, the differentiation of the categories is made difficult by the fact that both physical and communication observation include the possibility to observe individual's habits. Therefore, we will not draw any conclusions on the perception of behavioral observation as a single category, but rather as an implicit possibility taken into account by respondents when answering the questions on the first two, and particularly when considering exhaustive surveillance methods.

We will continue by considering types of information *extraction*, defined by Kasper (Kasper, 2005) as "involv[ing] a deliberate effort to obtain something from an individual or group" (Kasper, 2005). Here, opposed to observation (i.e. surveillance), data is not collected over a long period of time, but situationally and with particular effort. To measure public perception of forms of *stockpiling*, Q11 on fictional state access to private information in times of crisis was asked. The question addresses *stockpiling*, because the state is granted intrusive rights to collect and store information on its citizens, which in and of itself, is not harmful for the individuals concerned. This access however is limited in time, here to the acute crisis situation. The data is not automatically used, but stored and potentially used to ensure people's wellbeing. Though agreeing to the access to their information, people "remain largely unaware and uninformed of what happens to the information after it has been collected" (ibid.). *Appropriation/disclosure* is not covered by the questionnaire, because the state has no reason to collect potentially damaging personal information in order to disclose it later on (Kasper, 2005).

Inner-state extraction is covered by Q14, asking whether and in which cases people are willing to give up parts of their privacy in social media in order to track terrorists. The data collected is meant to provide information of the political and religious views of individuals, as well as their mental state or willingness to harm members of the public. These are not "externally knowable" (ibid.), and the judgement made on their basis decides over whether further policing steps are taken or not. Thus, the "stakes are higher than in *stockpiling*, and the purpose more specific than in *appropriation/disclosure*" (ibid.). Individuals are "usually aware of this" (ibid.), as the presence of laws allowing intrusion of this sort is known (particularly in case of the respondents who are made aware of it by the question), however (in line with Kasper's definition) it is possible that people are ignorant of the intrusion or its scope.

In her analysis of newspaper articles discussing intrusions into privacy from 1990 to 2003, Kasper (2005) finds that while data extraction is discussed most (constantly over 50% of newspaper articles), its percentage shows a declining trend. Observation however, takes increasing importance in the debate of privacy intrusions, whereas intrusion roughly stagnates (Kasper, 2005). Taking a closer look at extraction, i.e. dividing it into its subtypes, Kasper (2005) finds that while appropriation/disclosure used to be the main type discussed in the 1990s, its importance has sharply declined since. Not close to its importance in the 1990s, stockpiling is overtaking it in importance in 2003, so that the two categories roughly share the entirety of coverage on extraction in 2003. Of much smaller importance in the debate is inner-state extraction, not reaching the 10% mark of over-all privacy intrusion coverage. In the case of observation, levels of coverage are lower across categories, however physical and communication observation slightly gain importance across years (Kasper, 2005).

Kasper concludes that "[t]he instances of privacy invasion mentioned with increased relative frequency in the news are *stockpiling* extraction and *physical* observation" (Kasper, 2005). Putting this into the context of its time, i.e. 2003, we can conclude that the US' political situation of fear of terror and increasing surveillance is not unlike Germany's in 2018, although methods of surveillance have become significantly more sophisticated. Nonetheless, looking at the development of the possibilities and the debate induced by Snowden and other whistle-blowers, it can be speculated that the importance of observation in the discussion has since been increasing. Therefore, we expect to find similar, or possibly more extreme perceptions, especially regarding observation, as knowledge on security service practices of observation has increased since 2003. Kasper provides several explanations for this trend: surveillance takes place more often (ibid.), the consciousness of public has increased, therefore "people are more sensitive to such invasions" (ibid.) and the interaction of these two factors (ibid.). Concerning both types of privacy invasion (i.e. stockpiling and physical observation) people have "little knowledge and even less control" (Kasper, 2005). In addition, the already explained role of lacking awareness (Kasper, 2005) and a resignation

concerning *appropriation/disclosure extraction* and *autonomy intrusion* declined (Kasper, 2005).

3.2 Survey Design and Conduction

The study forming the basis of this paper is a representative survey of 1,024 subjects throughout Germany, adjusted according to the adult population from the age of 18 to 65 and the respective distribution of sociodemographic factors, namely gender, age, education, income, and region. It consists of an item-battery with four questions (Q11 to Q14) and lays its focus on privacy. Each question was designed to be Likert-scaled and closed-ended. The questions were developed based on a pilot study (Reuter et al., 2016). The hypotheses of this explorative study with 61 participants are tested with this quantitative approach.

The survey was conducted in German so that all participants understood the questions. The survey presented in this paper is a translation. Due to financial limitations no questions were included that checked the participants' attention or the frequency of their answers. The study was performed from 24th July to 7th August 2017.

3.3 Characteristics of Survey Subjects

The sample of survey respondents (N = 1024) was adapted to the distribution of gender, age, region, education, and income (Table 1) of the general German population by the preselection of an external survey panel provider (GapFish). In addition, solely consistent and complete answers were included. Therefore, our adapted sample consisted of 49.5% female (n = 507) and 50.5% male (n = 517) respondents. They were between 18 and 64 years old, nearly half of them being 45 and older (n = 492, 48%). Recruited participants live in all German federal states with the largest samples from North Rhine-Westphalia (n = 228, 22%) and Bavaria (n = 165, 16%). All participants are inhabitants of Germany, not necessarily German citizens. Furthermore, and important for this analysis, the subjects were classed based on their educational background: 69.2% of the subjects possess a secondary school graduation (from German Haupt- and Realschule). The other educational qualifications are distributed almost evenly over the remaining 30.8%. Only 1% (n = 9) of participants did not graduate from a school, while 15% (n = 160) held a degree from a university or college. Over two-thirds (n = 707, 69%) had an income between 1.500€ and 3.500€.

Table 1. Distribution of gender, age, education and income among participants.

Variables	Categories	Percent of respondents
Gender	Male	50.49
	Female	49.51
Age	18-24	11.82
	25-34	19.34
	35-44	20.70
	45-64	26.37
	65 and older	21.68
Education	No diploma	1
	General secondary school	33
	Intermediate secondary school	37
	High school diploma	14
	Polytechnic degree	7
	University degree	8
Income	Below 1,500	19
	1,500-2,500	29
	2,500-3,500	40
	Above 3,500	12

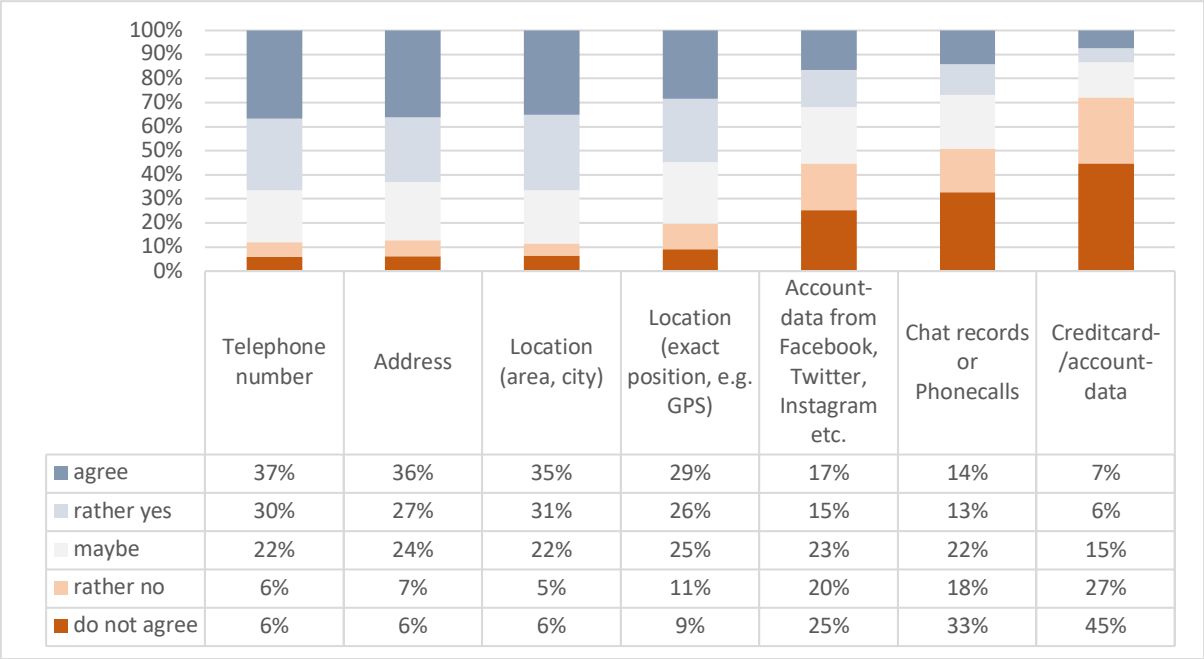
The responsible external survey panel provider recruited the respondents solely passively by advertising online (80%) and offline in TV commercials and newspapers (20%). There was no active recruitment via telephone or similar. The participants were chosen randomly and preselected concerning the above described criteria. They received small financial incentives between 0.5 and 2 Euros.

4 RESULTS

In the following sections, we present the results of our survey. The segmentation is based on the chronological structure of the item-battery, consisting of three questions concerning topics about the kind of personal data (potentially) accessed by state authorities, (fictional) state laws allowing surveillance and the conditions under which people would limit their privacy in social networks.

4.1 Access to Private Information by State Authorities

The first question (Q11) of the item-battery is: Which of your private data would you allow to be accessed by state authorities to combat an urgent crisis (e.g. terroristic attack or natural disaster)? The question is Likert-scaled: To each kind of private information, subjects were given different response possibilities. We included a wide range of information in order to assess peoples' general willingness to cede different private data. This allows us to roughly spot the average boundary of good will when it comes to sharing private information. Not all categories are therefore helpful to authorities in reality. A divide in the given answers is easily spotted, depending on the type of private data:



	Telephone number	Address	Location (area, city)	Location (exact position, e.g. GPS)	Account-data from Facebook, Twitter, Instagram etc.	Chat records or Phonecalls	Creditcard-/account-data
agree	37%	36%	35%	29%	17%	14%	7%
rather yes	30%	27%	31%	26%	15%	13%	6%
maybe	22%	24%	22%	25%	23%	22%	15%
rather no	6%	7%	5%	11%	20%	18%	27%
do not agree	6%	6%	6%	9%	25%	33%	45%

Figure 1: Access to Personal Information: Which of your private information would you allow to be accessed by state security services to combat an urgent crisis (terrorism, natural catastrophe) (Q11)?

The majority of the subjects would allow access to phone numbers, addresses and inaccurate GPS location data. In addition to this, accurate geolocations would be shared by most of the subjects as well. This approval of sharing private information sinks rapidly with other kinds of personal data: Access to profiles of social media accounts, contents of chats or telephone calls and financial account data would only be shared by a minority of subjects (Figure 1). Roughly 65% of the subjects agree to allow access to data like addresses, telephone numbers and geolocation-data, while only 32% would grant access to authorities to their social media profiles, 27% to contents of chats or phone calls, and only 13% would allow the mining of their financial account data (Figure 1).

4.2 Surveillance

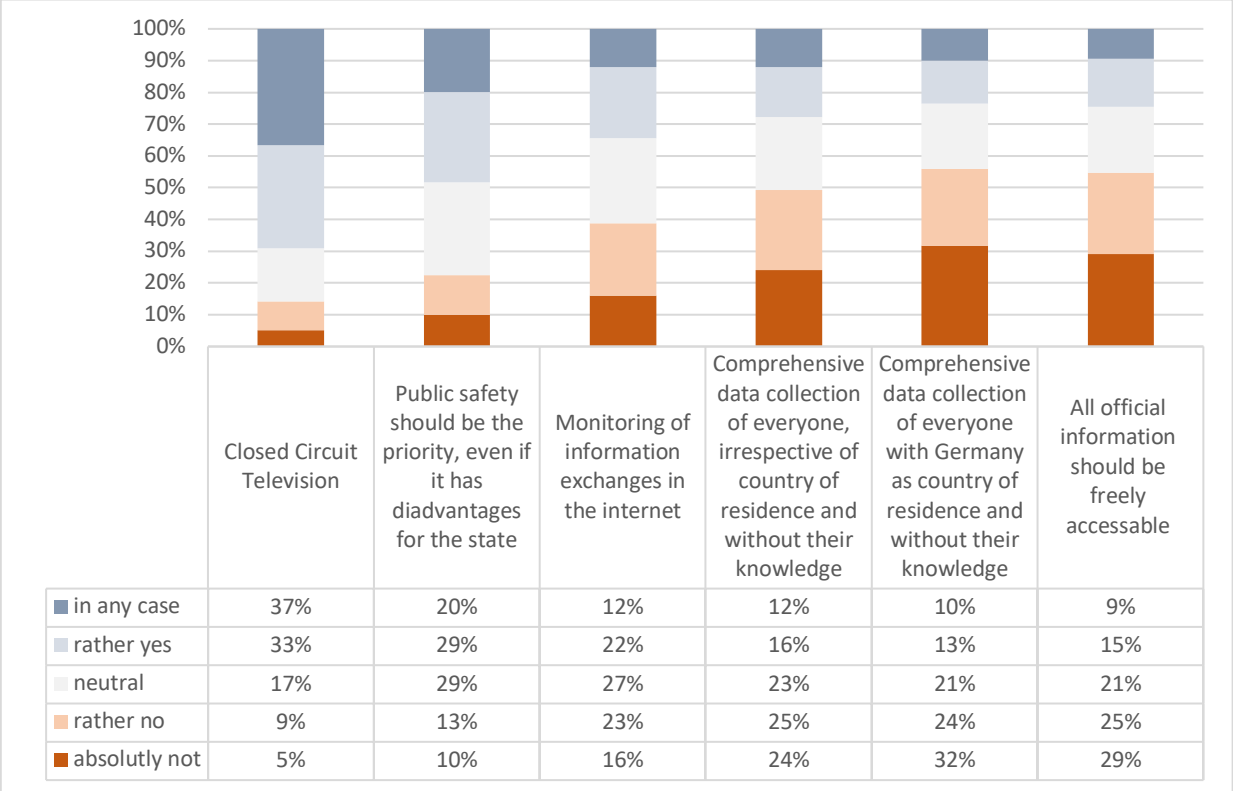
The third (Q13) question dealt with (fictional) state laws allowing surveillance, which were discussed in German mass media. Subjects were asked to support or reject those state laws. The question was whether authorities should have the following right to establish higher public security. We included this more general question in order to account for the fact that in reality, user data is not only assessed in times of acute emergencies, but also collected and used to prevent them. Public debate in Germany has mainly focused on this type of privacy intrusion, as well as the transparency and effectiveness of the measure. Therefore, the answers to this question indicate general willingness to give up data for the more or less definite, and highly subjective goal "security" is. Figure 2 gives an overview of the response possibilities and the answers given by the subjects.

Here too, there is a differentiated view regarding authority rights and the answers given: While the majority supports video surveillance of public spaces (approx. 70%) and the statement that public security should be paramount, even if this was adverse for the government (approx. 49%), the support falls for the rest of the stated laws and rights (Figure 2).

Monitoring of the internet and global information collections are considered ambiguously by the subjects, while the collection of information about German citizens without the knowledge of those involved is rather rejected. It is also striking that more than half of the subjects reject transparency in terms of a policy of freely available information about governmental intelligence for the public.

By bringing the variables into a binary form and creating a polarized mood image Figure 5 (in the Appendix) shows such a polarized tendency concerning the heavily debated issue of video surveillance. The majority of the subjects, 707 out of 853 (approx. 83%), would support video surveillance in public spaces.

Video surveillance in Germany is a frequent subject of debate in German media and therefore shall be examined in depth in Model 1. We see that people willing to allow surveillance of all exchange of information via the internet are significantly more likely to be in favor of introducing video surveillance. People opting for transparency (and against secrecy) on parts of the state, i.e. granting access to all information the state has, are significantly less likely (on a 1% level of significance) to opt for wide-spread video surveillance. Interestingly, people with a higher net income are significantly (on 1% level) more likely to favor video surveillance than people with a lower income.



	Closed Circuit Television	Public safety should be the priority, even if it has diadvantages for the state	Monitoring of information exchanges in the internet	Comprehensive data collection of everyone, irrespective of country of residence and without their knowledge	Comprehensive data collection of everyone with Germany as country of residence and without their knowledge	All official information should be freely accessable
in any case	37%	20%	12%	12%	10%	9%
rather yes	33%	29%	22%	16%	13%	15%
neutral	17%	29%	27%	23%	21%	21%
rather no	9%	13%	23%	25%	24%	25%
absolutly not	5%	10%	16%	24%	32%	29%

Figure 2: (Fictional) Rights of Officials: Should authorities in Germany in your opinion have or have not the right to the following to ensure public security better (Q13)?

Another subject of debate in German media is internet surveillance. 34% of the subjects rather support such surveillance, the rest rejects it. To have a closer look at the trends concerned, we use an OLS model of internet surveillance (see Model 2), i.e. granting the state the right to monitor all information exchange via the internet. People willing to allow video surveillance and notably, the collection of data on all people living in Germany without their knowledge, are significantly more likely (on 1% level) to opt for internet surveillance. Contradictorily, people both in favor of more transparency and more secrecy on parts of the state concerning the data it has, are significantly (on a 5 and 1% level, respectively) more likely to be positive about data gathering on information exchange via the internet. Simultaneously, having a higher education significantly (5% level) reduces the likelihood of opting for internet surveillance.

In Model 3, we regress respondents' disposition towards comprehensive data gathering on the entire population of Germany. While the answers to questions regarding video surveillance and secrecy in the perceptional part, and education and net income in the demographic part remain insignificant, questions such as allowing internet surveillance, international data collection and transparency are all positive and highly significant.

This points in an interesting direction: On the one hand, people who are prepared to allow the state highly intrusive access to their privacy are in other questions more likely to allow comprehensive data gathering. On the other hand however, people demanding transparency from the state - i.e. wishing that the state makes accessible all data it has on the population - expressly taking into consideration the adverse effect this might have on national security, are also significantly more likely to allow non-discriminatory, Germany-wide collection of data. Thus, transparency might be a necessary condition in the eyes of many skeptics to allow data collection in Germany.

This is an interesting point, because transparency and the accessibility of all data does not make the intrusion into privacy smaller, if anything, it increases it.

In the demographic part of the regression, age is the only variable with a significant effect (on 10% level), providing evidence that older people are more likely to allow comprehensive data gathering.

Table 2. OLS models of willingness to grant authorities privacy-intrusive rights

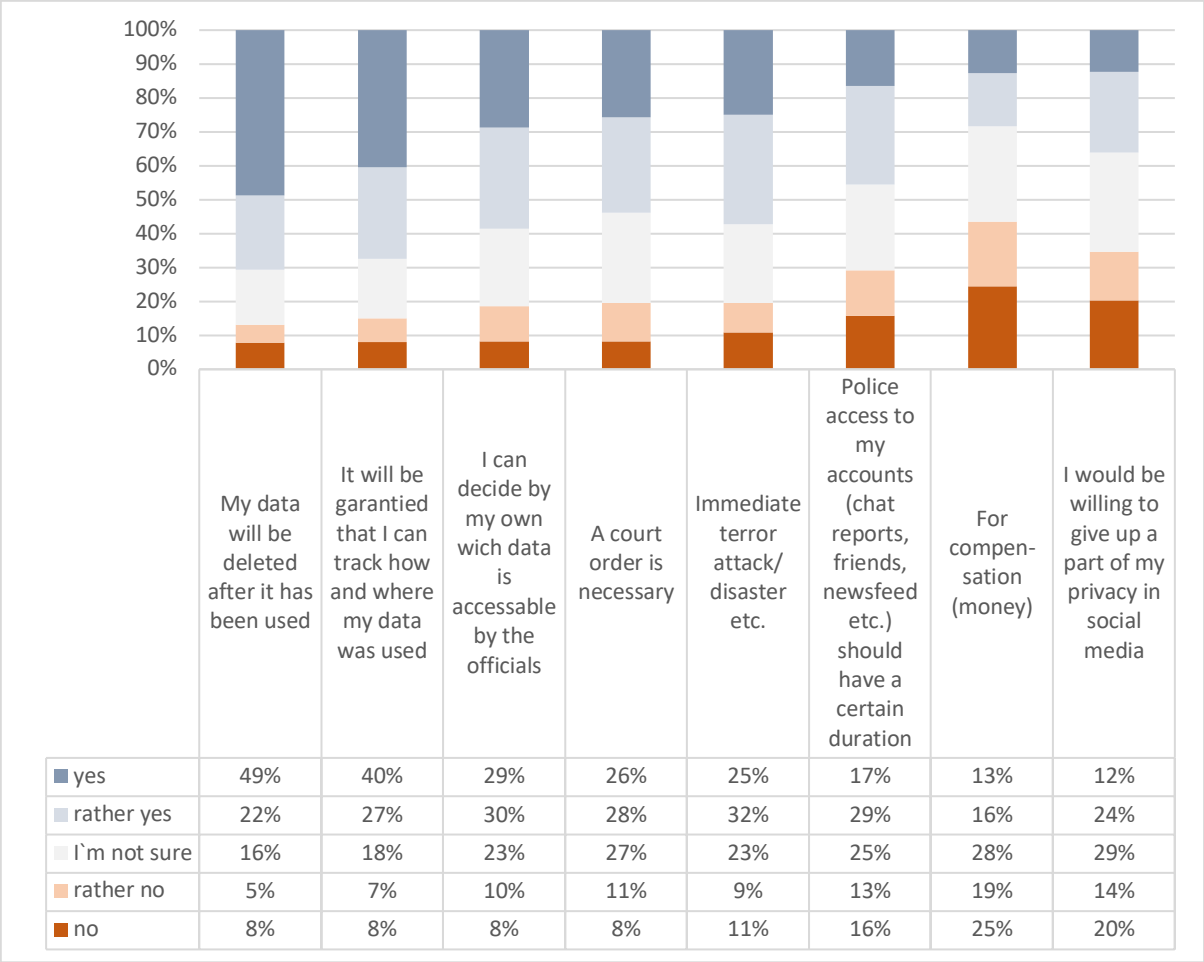
Variables	**Model 1** *Video Surveillance*	**Model 2** *Internet Surveillance*	**Model 3** *Data Gathering Germany*
Video Surveillance		0.281***	0.034
		(0.026)	(0.025)
Internet Surveillance	0.374***		0.386***
	(0.034)		(0.026)
Data Gathering Germany	0.053	0.458***	
	(0.039)	(0.031)	
Data Gathering World	0.055	0.046	0.475***
	(0.036)	(0.031)	(0.024)
Transparency	-0.121***	0.048**	0.086***
	(0.025)	(0.022)	(0.020)
Secrecy	0.177***	0.100***	0.039
	(0.030)	(0.026)	(0.024)
Age	0.021	-0.011	0.032*
	(0.023)	(0.020)	(0.019)
Education	-0.011	-0.051**	0.016
	(0.025)	(0.022)	(0.020)
Net income	0.101***	-0.039	0.006
	(0.033)	(0.028)	(0.026)
Constant	1.925***	0.422***	-0.577***
	(0.164)	(0.151)	(0.138)
N	1024	1024	1024
R^2	0.343	0.578	0.681
Adjusted R^2	0.337	0.575	0.679

*** $p \leq 0.01$, ** $p \leq 0.05$, * $p \leq 0.1$

4.3 Security and Privacy

The last question (Q14) addresses whether respondents would give up parts of their privacy in social networks if this would include tracing of terrorist organizations, and if so, under which conditions. When looking at Model 4, we observe that the respondents with a high general willingness to give up their privacy are significantly less likely to favor the necessity of a court order for access to personal data (on a 1% level of significance). This tendency of people preferring well-defined, limited access to personal data opting for court orders applies to quite some variables. Among others it applies to people willing to share their personal data with the authorities only in the case of immediate emergencies, who are also significantly more likely to prefer court orders. Similarly, people willing to share personal data only if the duration of usage is clearly defined, are significantly more likely to support the necessity of court orders for access. Equally significantly positive is the effect of pledging for self-determined usage of data by authorities.

However, this trend of people with high standards of data protection is not as consistent as it might first seem. There is no significant connection between demanding the deletion of data after usage and preferring court orders. The same is true for the demand of transparency in the states' handling of personal data and court orders. Interestingly, people with higher age and education are also more likely to favor court orders as necessity to allow for access to personal information. The effect of education is not significant in either of the other two models. Age has a significantly positive effect (on 5% level) on making the deletion of data a necessary condition for access to personal data on social media, but not on sharing data in case of an immediate emergency.



	My data will be deleted after it has been used	It will be garantied that I can track how and where my data was used	I can decide by my own wich data is accessable by the officials	A court order is necessary	Immediate terror attack/ disaster etc.	Police access to my accounts (chat reports, friends, newsfeed etc.) should have a certain duration	For compen-sation (money)	I would be willing to give up a part of my privacy in social media
yes	49%	40%	29%	26%	25%	17%	13%	12%
rather yes	22%	27%	30%	28%	32%	29%	16%	24%
I`m not sure	16%	18%	23%	27%	23%	25%	28%	29%
rather no	5%	7%	10%	11%	9%	13%	19%	14%
no	8%	8%	8%	8%	11%	16%	25%	20%

Figure 3: Conditions of Renouncing Privacy: Would you be willing to waive parts of your privacy on social media when it was used to detect terrorists and, if so, under what conditions? (Q14)

Looking at Model 5 in greater detail, we see that all other answers given to the question described above, predict the answer to sharing data in cases of immediate emergency rather well. The only significantly negative effect can be observed with wishes for self-determination of the data used. All other positive answers, be they in favor of more privacy or not, have significantly positive effects. One answer that we should highlight in this context is granting a monetary incentive for sharing personal data. This demand has no significant effect in either of the other two models. Here however, people willing to sell their data are also significantly more likely to be willing to share their data on social media. The demographic controls are all insignificant. Furthermore, all people, be they defenders of data privacy or not, are willing to share their personal data in social networks in cases of emergencies. Notably, emergencies include both natural disasters and terrorist attacks. It could be argued that this effect might be driven by the mere inclusion of terrorist attacks into the scope of 'emergencies', as the debate on political violence, particularly Islamist violence, is increasingly securitized. The control question (Q12) asked on people's willingness to share their data on social media with the authorities across different types of emergencies however, contradicts this notion.

The deletion of data after usage, as modeled in Model 6, is significantly (on a 1% level) predicted by the willingness to share data in cases of emergency, the demand for more transparency on the part of the German state, a defined duration of usage, as well as self-determination in the scope of data used. The effects of demanding a court order and a high over-all level of privacy are not significant. This implies that having a high standard of privacy, as modeled by these two variables, does not significantly predict demanding the deletion of data. Nonetheless, we find that higher age significantly (on 5% level) increases the probability of answering that deletion of data is a necessary condition for sharing personal data.

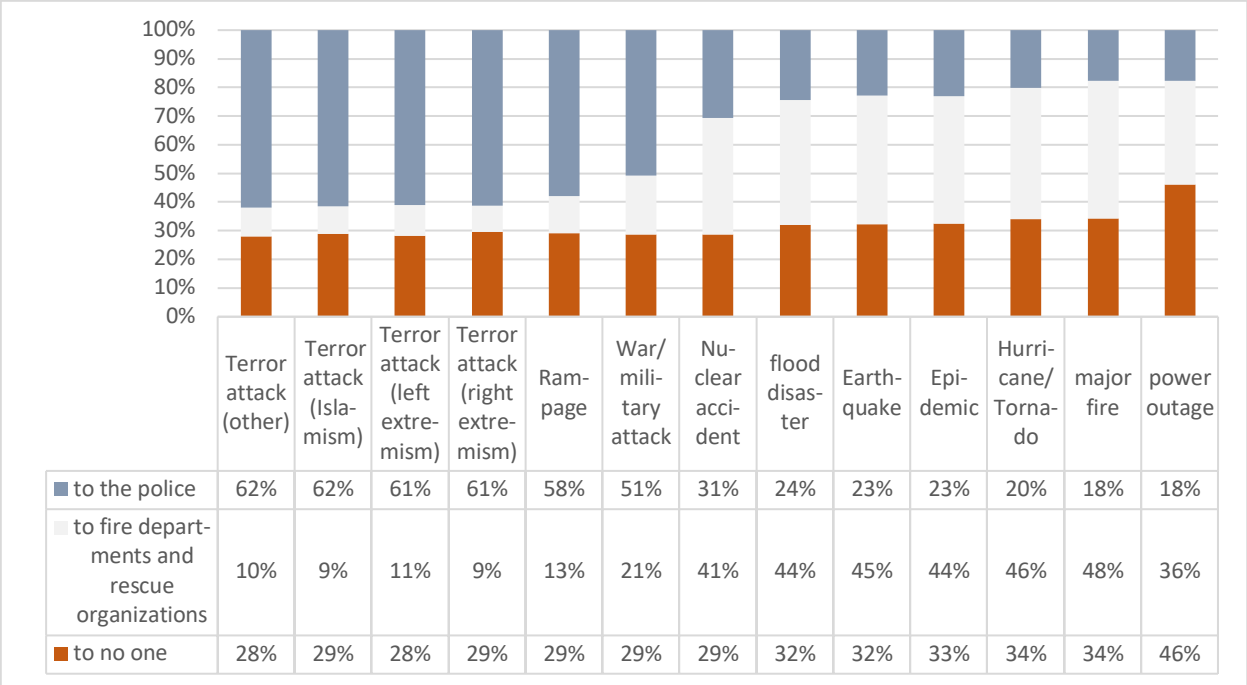


Figure 4: Situation differentiation: In the context of which acute threats would you waive parts of your privacy in social networks and to whom (e.g. by generally collecting private messages) and in which not? (To emergency response by the police, to emergency response not by the police (fire department, rescue teams), to nobody) (Q12)

Table 2. OLS models of willingness to give up privacy in social media

Variables	**Model 4** ***Court Order***	**Model 5** ***Immediate Emergency***	**Model 6** ***Deletion***
Privacy	-0.102***	0.293***	0.017
	(0.033)	(0.025)	(0.023)
Immediate Emergency	0.134***		0.176***
	(0.038)		(0.026)
Deletion	0.019	0.251***	
	(0.046)	(0.037)	
Transparency	0.071	0.165***	0.620***
	(0.046)	(0.038)	(0.025)
Court Order		0.090***	0.009
		(0.026)	(0.022)
Temporary	0.1***	0.144***	0.070***
	(0.031)	(0.026)	(0.022)
Self-determination	0.316***	-0.112***	0.076***
	(0.032)	(0.028)	(0.023)
Monetary incentive	-0.019	0.126***	-0.021
	(0.028)	(0.023)	(0.019)
Age	0.064**	0.036	0.049**
	(0.028)	(0.023)	(0.019)
Education	0.131***	-0.022	0.031
	(0.029)	(0.024)	(0.020)
Net income	0.020	-0.010	0.001
	(0.038)	(0.031)	(0.026)
Constant	0.918***	0.287*	0.196
	(0.208)	(0.172)	(0.144)
N	1024	1024	1024
R^2	0.225	0.507	0.652
Adjusted R^2	0.218	0.502	0.649

*** $p \leq 0.01$, ** $p \leq 0.05$, * $p \leq 0.1$

5 DISCUSSION

So far, we presented the results of our work and made a first analysis of the gathered data. In the following sections we carry out a deeper examination of the findings. For this we return to our initial research questions and try to address the research gap.

5.1 Social Media in Crisis Management

Respondents are willing to cooperate with authorities and disclose information in situations of acute danger. Our models suggest that generally speaking, older and well-educated respondents are more likely to fall into the group of privacy-aware people. However, this trend is not constant and depends on the content made available to state authorities. In the case of an immediate terrorist attack, 74.5% of the subjects (when deleting neutral answers, n = 786) would give up their privacy in social media and make data accessible. Our insight on the context-sensitivity of subjects with regard to their willingness to provide information in crisis situations coincides with the findings of Ur et al. (2012). In this context, the central aspect of trust in the responsible authorities stands above all as a basis to the willingness to co-operate. This is also confirmed by Phelan et al. (2016) and Leon et al. (2015). The principle of context-dependency we have identified with regard to the information willingness of the subjects is also supported by various studies (Acquisti & Gross, 2006; Denning, 2014).

Overall, the willingness to disclose personal information in situations of acute danger (terror, war, natural disasters, etc.) is as follows: The more intimate the type of information, the lower the approval of the subjects. Telephone numbers, addresses and location information belong to the data that is not considered critically intimate and would be communicated by a large portion of subjects.

5.2 Perception of Privacy in Social Media and Surveillance

Regarding wishes and needs of citizens' concerning privacy as well as a possible monitoring of ethics by the state, we were able to obtain the following findings: More than half of the subjects approve of video surveillance of public space and regard public safety as a central task and the first and most important priority of the state (Figure 2, answer option "Security first"). Opinions in favor of video surveillance are made more likely by a generally positive view of surveillance, as approximated by consenting to internet surveillance and secrecy (as opposed to transparency), as well as a high net income. Possible causes for these views may lie in the Islamist terrorist attack by Anis Amri in Berlin in December 2016, or the various Islamist motivated attacks in Belgium, France or Great Britain since 2015. Especially the approval for video surveillance is plausible, since it has proven to be effective in relation to other crimes and their clarification. The general focus on security is also demonstrated by the fact that the subjects refuse public access to state information. Interestingly however, the relationship between opposing transparency and favoring surveillance is not constant.

Both data collection in Germany and on a global level are rejected by the subjects, especially the collection of information via internet is viewed critically by respondents. These could be impacts of the Snowden revelations, as well as general mistrust of internet surveillance measures, such as Degli-Esposti et al. (2017) describe it. But also with regard to this topic, large shares of neutral answers remain. This may be due to subjects not being sufficiently informed, simply not sure or in favor of measures for public safety but unable to oversee their consequences. Also, people endorsing transparency seem to be significantly more likely to consent to data gathering in Germany; although these two answer possibilities logically oppose each other in terms of security policy. All this makes clear that there is a need for enlightenment on measures to increase public safety. The same can be observed regarding the conditions for the abandonment of privacy: Above all, this means being aware of the nature of data potentially used by authorities. It becomes apparent, following Degli-Esposti et al. (2017), that subjects are not in need of an increased implementation of existing security measures, but rather a different implementation of existing and alternative security policies.

With regard to citizens' willingness to cooperate, we found that greater transparency and clarification by the authorities is required. Citizens are basically willing to make "superficial information", such as addresses and telephone numbers, accessible in dangerous situations. Given appropriate transparency on parts of the state, this also applies to parts of their privacy in social networks. The group opposing such measures seems to depend on the specific data to be shared. Although some models show the tendency that more educated and older people are less likely to share their data, this trend does not apply to model 3, which shows that older people are more likely to support Germany-wide surveillance. Similarly, a higher income raises the probability to support the implementation of video surveillance (model 1). A closer examination of the group in favor of privacy is necessary to make specific statements about the reasons underlying these trends. However, a non-linear effect of age on privacy attitudes might be a possible reason for what might seem at first sight to be contradictory outcomes. A first assumption can be made by relating to social media-affinity of the younger age groups and their need to express themselves on social media, while middle aged groups, not used to the openness of social media, are more likely to hide their private information. The older age groups could lack media expertise and therefore be willing

to share information (Reuter et al., 2017). Hence, the government has the obligation to provide specific education and enlightenment of its citizens, in order to increase their understanding of methods used by authorities. In this context, information transparency can be seen as a key factor to provide certain knowledge and foster a better understanding of these methods (Acquisti et al., 2015; Awad & Krishnan, 2006).

In general, a certain part of the population is prepared to give up parts of their privacy. People show a high willingness to share personal data in cases of immediate emergencies, even when demanding transparency, deletion of data, court orders, monetary incentives and self-determination about the usage of their data. At the same time, people with a low standard of privacy do not demand a law necessitating court orders for access to personal information.

Many neutral answers point out that the subjects have too little knowledge, are inhibited or simply cannot decide, respectively have concerns. In line with findings of Degli-Esposti et al. (2017; also see Kokolakis, 2017), a part of the respondents are not sufficiently informed to have an opinion. Especially the question concerning the willingness to give up parts of privacy in social media. Here, the most frequently chosen answer is "I'm unsure" (29%).

6 CONCLUSIONS AND PERCEPTIONS

In the following, we summarize the key findings of our study and focus on the most significant factors influencing the potential willingness of the subjects to cooperate. Finally, we discuss the limitations of our work, present possible perspectives for future research based on our findings and position our findings in the context of previous research.

6.1 Central Results: People Are Willing to Conditionally Give Up Privacy

The central question of our work on the willingness of the (German) population to resign parts of their privacy under certain conditions for crisis management and surveillance must be answered ambivalently. On the one hand, people are willing to do this to a certain extent. For this purpose, however, an adequate information-policy and transparency by authorities are needed. In particular, this includes self-determination in the use (about 59% consent) and confidentiality of the data, as for example the "right to be forgotten" allows (about 71% consent). Only then citizens no longer feel powerless and at the mercy of the state's surveillance activities.

A subject-related dichotomy with regard to the willingness to cooperate in social media in relation to the release of private information was identified above all by two characteristics: In particular, age and level of education have an influence on whether citizens make their private information available to the authorities. In terms of age, the regressions paint a diverse picture; age influences privacy-affinity positively in some respects and negatively in others. The educational level has a positive impact, however not constantly so: The higher it is, the more privacy-restricting authority rights are rejected (such as increased internet surveillance) and regulatory laws supported (such as court orders).

6.2 Limitations of our Work and Perspectives for Future Research

Our paper and the underlying survey have limitations concerning the methodological approach as well as the scope of the results. Because the survey was conducted online, neither an introduction nor any kind of background information were given to the participants. On the one hand, it must be stated that the respondents, although understanding the questions in general, did not necessarily understand the meaning of concepts used in the questions. On the other hand, this ensured unbiased answers of the respondents. However, in future research the used concepts should be introduced to participants to be able to get a more detailed and unambiguous insight into their mind set and opinion. Although a representation of the results and the subjects' socioeconomic properties are given, the online conducted survey only covers people who were willing to be part of this study. A bias towards internet affinity of the respondents is therefore possible. This would contradict the notion of the older participants lacking the necessary knowledge to be more critical towards surveillance. However, a general internet affinity does not necessarily imply an awareness for privacy. On the contrary, it can be assumed that people who are willing to register and share their opinion for a reward in such a panel are less concerned about their privacy than average citizens. Therefore, the analysis based on those participants is likely to underestimate skepticism towards privacy intrusions and the effect of education on it.

The sample is restricted to the German population, nonetheless our findings suggest to implicate more general correlations which may be apparent in other liberal democracies. Neither the expectations of German participants towards state authorities nor their interest in protecting their legal rights may be due to a specific German context. Furthermore, correlations between certain variables like income or education and people's attitude towards cooperation via social media may prove stable across borders as well. Nonetheless, the German historical background has to be taken into account, as it could cause a special relation to aspects of privacy and surveillance

by the state.

Our work can be elaborated with further questions regarding people's perception of privacy concerning social media and surveillance as our analyzed item-battery consisted of only three questions. Despite the meaningful results of our study, further and more in-depth questions are needed to interpret the neutral answer options. Relevant insights into the level of awareness people have concerning data exploitation and privacy intrusions in general, would encompass illuminating the reasons for people's opinions, as well as the consequences for their online behavior: The questions of why some people are more aware than others, and if higher awareness has any behavioral consequences are of central relevance. Moreover, the applied statistical methods, especially the multiple regression analyses, can be expanded. Qualitative methods should also be used to elaborate on this topic, especially to understand the neutral answers. Open questionnaires and interviews are suitable with a subsequent qualitative content analysis to cluster categories of the subjects. To get a deeper insight into the perception of privacy further research should focus on the connection between awareness for privacy and general knowledge about privacy issues, social media monitoring and surveillance measures.

6.3 Differentiation to Previous Research and Scientific Added Value

The theoretical premises of this paper are based on the work of Kasper (2005). We found that under some conditions (such as deletion after usage and transparency), a high number of people (26%) are willing to give up parts of their privacy in social media in order to detect terrorists. Thus, the threshold to allow for *inner-state* invasions (Kasper, 2005) is surprisingly low, given that the consequences (i.e. police measures against suspected terrorists) are rather severe. As shown in Model 5, in cases of emergencies even people with high standards for privacy (proxied by several conditions for state access to their data) are more likely to share their data. Keeping to forms of extraction, stockpiling, as covered by the first question (Q11), seems to be a differentially perceived form of privacy invasion. While most people are willing to share their address or telephone number, only few people are willing to share more intimate information, such as contents of chats or credit card details.

Now turning to forms of observation, a majority of respondents (70%) approves of *physical observation* as modeled by CCTV coverage of public spaces, whereas observation of *communication* and *behavior* are regarded critically by most. *Communication* was measured by granting the state access to exchanges of information via internet, which of course partly covers behavioral observation. The approval rate for this type of surveillance was 34%. An all-encompassing form of observation, i.e. gathering data on all German inhabitants without their knowledge, gained 23% positive answers. Thus, when combining several forms of *observation*, approval rates are particularly low. However, it needs to be kept in mind that with modern forms of communication and surveillance, every type of observation will reveal information belonging in either or both of the other two categories. Overall it can nonetheless be said that surveillance of communication and behavior, as well as extraction of intimate information, are particularly negatively perceived within the population. Keeping this in mind, it would be interesting to further examine people's opinions on data exploitation, as this encompasses most intimate data, but the discussion still has a very limited audience.

As Reuter & Spielhofer (2017) have shown, fundamental cooperation readiness is apparent but partly this seems to be associated with obligations of the state regarding transparency. We also considered the remarks by Degli-Esposti et al. (2017) on the unclarity of the population with respect to surveillance measures, the inherent frustration and the apathy-inducing effect on citizens.

ACKNOWLEDGEMENTS

This work was supported by the German Federal Ministry of Education and Research (BMBF) as well as by the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within CRISP as well as by the DFG within the CRC 1119 CROSSING.

We would like to thank Robin Gellert and Gordian Geilen for supporting the development of the survey items. In addition, their pilot study (Reuter et al., 2016) was a very valuable basis for this study.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy Enhancing Technologies* (pp. 36–58). Berlin, Heidelberg: Springer Berlin Heidelberg.

Acquisti, A., & Grossklags, J. (2006). What can behavioral economics teach us about privacy? In *ETRICS* (pp. 1–13).

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, *30*(1), 13–28. Retrieved from http://www.jstor.org/stable/25148715

Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information Communication and Society*, *12*(5), 639–657. https://doi.org/10.1080/13691180802270386

Buxmann, P. (2015). Big Data: Neue Geschäftsmodelle für die Future Internet Economy. In *Digitales Neuland* (pp. 139–153). Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-09692-2_9

Degli-Esposti, S., Pavone, V., & Santiago Gómez, E. (2017). Aligning security and privacy - The case of Deep Packet Inspection. In M. Friedewald, J. P. Burgess, J. Čas, R. Bellanova, & W. Peissl (Eds.), *Surveillance, Privacy and Security: Citizens' Perspectives* (pp. 71–80). London, UK: Routledge. Retrieved from https://www.researchgate.net/publication/315657622_%0AAligning_security_and_privacy_-_The_case_of_Deep_%0APacket_Inspection

Denning, T. (2014). Human-Centric Security and Privacy for EmergingTechnologies. University of Washington.

Dobel, S. (2016). Pressesprecher im Porträt. Die Stimme der Münchner Polizei: Marcus da Gloria Martins.

Hagar, C. (2007). The information needs of farmers and use of ICTs. In B. Nerlich & M. Doring (Eds.), *From Mayhem to Meaning: Assessing the social a nd cultural impact of the 2001 foot and mouth outbreak in the UK*. Manchester, United Kingdom, United Kingdom: Manchester University Press.

Kasper, D. V. S. (2005). The evolution (or devolution) of privacy. *Sociological Forum*, *20*(1), 69–92. https://doi.org/10.1007/s11206-005-1898-z

Kaufhold, M.-A., & Reuter, C. (2019). Cultural Violence and Peace in Social Media. In C. Reuter (Ed.), *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden, Germany: Springer Vieweg.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *2017*(7).

Leon, P. G., Rao, A., Schaub, F., Marsh, A., Cranor, L. F., & Sadeh, N. (2015). Privacy and Behavioral Advertising: Towards Meeting Citizens' Preferences. In *Symposium on Usable Privacy and Security (SOUPS) 2015*. Ottawa, CAN.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2018). The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126. Retrieved from http://www.jstor.org/stable/

Palen, L., & Liu, S. B. (2007). Citizen Communications in Crisis: Anticipating a Future of ICT-supported Public Participation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 727–736). New York, NY, USA: ACM. https://doi.org/10.1145/1240624.1240736

Palen, L., Vieweg, S., Liu, S. B., & Hughes, A. L. (2009). Crisis in a Networked World: Features of Computer-Mediated Communication in the April 16, 2007, Virginia Tech Event. *Social Science Computer Review*, *27*(4), 467–480. https://doi.org/10.1177/0894439309332302

Pavone, V., Ball, K., Esposti-Degli, S., Dibb, S., & Santiago-Gómez, E. (2017). Beyond the security paradox: Ten criteria for a socially informed security policy. *Public Understanding of Science*, 0963662517702321. https://doi.org/10.1177/0963662517702321

Phelan, C., Lampe, C., & Resnick, P. (2016). It's Creepy, But It Doesn'T Bother Me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 5240–5251). New York, NY, USA: ACM. https://doi.org/10.1145/2858036.2858381

Reuter, C. (2019). *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden, Germany: Springer Vieweg.

Reuter, C., Backfried, G., Kaufhold, M.-A., & Spahr, F. (2018). ISCRAM turns 15: A Trend Analysis of Social Media Papers 2004-2017. *Proceedings of the Information Systems for Crisis Response and Management (ISCRAM)*, (May), accepted.

Reuter, C., Gellert, R., & Geilen, G. (2016). Reception of Terror in Germany – Security, Privacy and Social Media. In Wohlgemuth, V., F. Fuchs-Kittowski, & J. Wittmann (Eds.), *Environmental Informatics – St ability, Continuity, Innovation. Current trends and future perspectives based on 30 years of history. Adjunct Proceedings of the EnviroInfo 2016 conference* (pp. 151–156).

Reuter, C., Hughes, A. L., & Kaufhold, M.-A. (2018). Social Media in Crisis Management: An Overview of Crisis Informatics Research. *International Journal on Human-Computer Interaction (IJHCI)*.

Reuter, C., & Kaufhold, M.-A. (2018). Fifteen Years of Social Media in Emergencies: A Retrospective Review and Future Directions for Crisis Informatics. *Journal of Contingencies and Crisis Management (JCCM)*, *26*, 1–17. https://doi.org/10.1111/1468-5973.12196

Reuter, C., Kaufhold, M.-A., Spielhofer, T., & Hahne, A. S. (2017). Social Media in Emergencies: A Representative Study on Citizens' Perception in Germany. *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing*, *1*(2), 1–19. https://doi.org/10.1145/3134725

Reuter, C., & Spielhofer, T. (2017). Towards social resilience: A quantitative and qualitative survey on citizens' perception of social media in emergencies in Europe. *Technological Forecasting and Social Change*, *121*, 168–180. https://doi.org/10.1016/j.techfore.2016.07.038

Schillat, F. (2016). Der Social Media-Chef der Polizei München zu Facebook und Twitter: „Da dürfen wir uns nicht raushalten``. *MEEDIA (29.07.2016)*.

Turow, J., Hennessy, M., & Draper, N. (2015). *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*. Philadelphia. https://doi.org/http://dx.doi.org/10.2139/ssrn.2820060

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 4:1----4:15). New York, NY, USA: ACM. https://doi.org/10.1145/2335356.2335362