The Black Mirror: What Your Mobile Phone Number Reveals About You

Nicolai Krüger[1(✉)], Agnis Stibe[2], and Frank Teuteberg[1]

[1] Accounting and Information Systems, University of Osnabrueck, Osnabrueck, Germany
nikrueger@uni-osnabrueck.de
[2] TRANSFORMS.ME, Paris, France

Abstract. In the present era of pervasive mobile technologies, interconnecting innovations are increasingly prevalent in our lives. In this evolutionary process, mobile and social media communication systems serve as a backbone for human interactions. When assessing privacy risks related to this, privacy scoring models (PSM) can help quantifying the personal information risks. This paper uses the mobile phone number itself as a basis for privacy scoring. We tested 1,000 random phone numbers for their matching to social media accounts. The results raise concerns how network and communication layers are predominately connected. PSMs will support future organizational sensitivity for data linkability.

Keywords: Privacy · Information privacy · Privacy scoring model · Social media privacy · Mobile phone privacy · Mobile Device Management

1 Introduction

Today, the omnipresence of smartphone use extends far beyond the professional context, as in the past. Instead, it reaches the most private areas of people's lives. With this comes the need for ethical considerations arising from the usage of such technologies and the possibility of either observing or manipulating users' behaviour. Messeging services such as WhatsApp and online social networks (OSN) are very popular and may be underestimated in terms of their sociotechnical concerns.

The public discussion regarding smartphone and social media privacy has changed radically, owing to the last US presidential elections and the scandal concerning the activities of Cambridge Analytica. Prominent security faults such as this might raise the perceived need for privacy in practice. Furthermore, recent literature has highlighted the specific risks pertaining to knowledge leakage and personal information disclosure by mobile devices [1, 2].

As responsible information systems (IS) researchers, we investigate privacy risks that are often overlooked by mobile phone users and mobile service providers. More specifically, this research carries out a study based on telephone numbers as a digital footprint. While the body of literature offers well-elaborated approaches to the measurement of privacy at the application level [3, 4], a research gap exists in terms of the combination of the mobile phone network layer and OSN. First, we hypothesise that an

W. Abramowicz and G. Klein (Eds.): BIS 2020, LNBIP 389, pp. 18–32, 2020.
https://doi.org/10.1007/978-3-030-53337-3_2

individual's phone number can be traced as a footprint throughout OSN. We aim to test our hypothesis using a modified privacy scoring model (PSM).

The relevance of this problem can be derived from several different angles. (i) Existing and well-established systems face new threats owing to the development of new attack models. Data science tools and practices, such as the advanced web scraping and robot process automation (RPA) employed in this study, create a new category of possible privacy attacks. This method of gathering publicly accessible information, referred to as open source intelligence (OSINT), is actively used by police and intelligence agencies [4, 5], and could potentially be misused by other authorities. (ii) De-anonymising of phone numbers is a prevalent problem in academia and business [6, 7]. (iii) Interpreting mobile phone signals has already become a market in its own right, like interpreting mobile phone data to visualize the instore movements of shoppers [8]. (iv) As [9] suggest, a clear sample in terms of technology, use cases and users is needed beyond the existing survey-driven approaches in the body of knowledge. The aim of this paper is to move a step forward in this research direction. Through addressing this dilemma concerning potential privacy issues, the objective of our paper is to enrich the understanding of mobile-network-based privacy attacks that aim to obtain the personal information of users. Thus, we formulate the following research questions:

RQ: Which requirements and implications arise for social media and mobile phone privacy from a privacy scoring model (PSM)?

To answer this question, we build upon a privacy dimension framework [10]. Furthermore, this paper enriches the existing model with the help of knowledge obtained from the body of literature on mobile phone network security, in order to suggest an applied PSM. Subsequently, we randomly select 1,000 phone numbers and test the PSM attributes and dimensions to evaluate our model with real-world data. The paper contributes to research an practice with mainly two artefacts: First, a PSM for the given context (mobile and social media privacy in combination) will be derived from the empirical data. Second, a prototype of a real-life implementation of our paper is presented.

The structure of this paper is as follows: the following section describes the relevant concepts found in the background literature. We then describe the methodology concerning the PSM employed in this paper and build a framework for a PSM that reflects the mobile phone network layer and the selected OSN attributes and dimensions. Following this, we test our model to present the findings and analysis pertaining to personal information disclosure. Lastly, we discuss our results and outline the potential contributions and limitations of our research.

2 Related Work

2.1 Privacy Scoring Models

PSMs are an appropriate method of measuring the individual privacy of a user from a user-centric point of view. A conglomeration of existing approaches for building privacy scores can be found within the PScore, published by Petkos et al. [10]. In general, three separate dominant motives for using PSMs can be found in the existing body of

knowledge. Firstly, they allow for risk monitoring to increase the awareness of users about this topic. Secondly, PSMs provide recommendations for privacy settings. Lastly, they generate a privacy score that also enables a sociological study of the measured (usage) behaviour [11]. This approach was expanded by Vidyalakshmi et al. [12], as their PSM focused on a user's friends within OSN, and aimed to provide a classification of the user's friends and their trustworthiness. Numerous further examples exist in the field of OSN. Hamed and Ayed [13] introduced a privacy score for OSN and carried out an experiment with mobile and stationary users. In their study, they drew the conclusion that the permanent online connection of mobile devices creates a higher risk of tracking and potential privacy threats, as they established a correlation between the browsing time and the privacy scores of mobile users.

In contrast to the PSMs described above, Kaffel and Ayed [14] have drawn attention to web-tracking based on cookies, JavaScript and iFrames. They also propose a specific privacy scoring for this problem. In [13], the researchers' proposed PSM differentiated between mobile and desktop tracking. They subsequently arrived at the conclusion that mobiles are at a higher risk of privacy threats due to their permanent connection to the web. Researchers have also addressed privacy concerns pertaining to the mobile phone network [15, 16].

To the best of our knowledge, no existing PSM includes the mobile phone network layer, as introduced by us in the following section. Our PSM also differentiates from existing models by building a chain of information: instead of measuring single data points and quantifying them, our model builds upon the revealed information of a user and uses these data for further investigations.

2.2 Social Media and Mobile Phone Privacy

The new General Data Protection Regulation (GDPR) of the European Union (EU) has been in force since May 2018, and proclaims privacy to be a human right: "The protection of natural persons in relation to the processing of personal data is a fundamental right" [17]. In future, IS research and curricula might be pressed even more than before to fulfil the task of establishing an educational and scientific body of knowledge on privacy-enhancing technologies (PETs) and privacy by design.

However, [18] addressed the need for upcoming mobile technologies to answer arising privacy concerns. Their study presented several different classes of PETs: identity management, anonymous communication, anonymous access to services, privacy-preserving authorisation and data management. Fundamental research artefacts applying these findings can be found in the recent literature. [12] conceptualises privacy as a service. Several examples can be found in the IS literature that reflect the privacy aspects of OSN and internet communication in general. For instance, [19] presented an approach for de-anonymising users based on pattern recognition within domain name system (DNS) traffic. [20] generated a model of cultural differences in self-disclosure technologies within instant messaging services (IMS). Furthermore, [21] examined an OSN study using Facebook in Turkey. Particularly in the current political situation, privacy concerns are paramount. The researchers identified several privacy threats, and suggested the inclusion of privacy sensitivity within educational programs. Beside political reasons, the complexity of OSN is a reason for continuous research in that field, as recently

shown in [22]. The authors suggest OSN users to make active use of privacy settings, adding less people to their personal network and sharing fewer private data.

Even in the early stages of mobile communication, privacy was a significant matter of concern. At the end of the last century, Kesdogan and Fouletier [23] argued that the privacy of users will be threatened owing to the decreasing size of network cells. In addition, [24] identified the home location register (HLR) as a potential bottleneck for the growing mobile communication sector. Different techniques for mobile phone positioning are available through HLR lookups, network triangulation and silent SMS [25, 26], which can be misused by attackers to achieve information disclosure or to carry out criminal activities in the physical world, such as attempting burglaries as soon as a resident leaves for a holiday abroad. [16] analysed possible solutions for overcoming such privacy threats, although none of the suggested safeguards could be initiated by users; most of these referred to the GSM infrastructure and need to be implemented by the service providers.

3 Methodology

3.1 Towards a PSM for Mobile Phone Number Privacy

By studying existing PSMs, as presented in Sect. 2.1, we learned that the flexibility and rigour of the PScore framework proposed in [10] provides a solid approach for our research purposes. Each privacy dimension needs operationalisation by the researcher, which is well described by the framework. In order to apply the general PScore framework (Fig. 1) to mobile communication systems, the development of a matrix of privacy dimensions, attributes and values within the given domain is the primary step. These dimensions represent the organisational structure of the private or sensitive information of a user. Each dimension has a number of attributes as a sub-categorisation, and each attribute contains a set of values. As stated by Petkos et al. [10], this list of domain-specific values is an iterative set that may evolve in the course of future research; it represents the status quo in terms of the current state of knowledge, the body of literature, and technical possibilities. This point will be considered further in the section describing the limitations of our study.

The PScore framework provides a horizontal structure of dimensions and a vertical structure of scores at each node of the scheme, which are weighted on the basis of their confidence, sensitivity, viability, source of confidence (declared/inferred), support and level of control. We excluded the parameter of sensitivity mentioned in the original framework, and set the parameter of confidence to a constant (=1), since [10] employed a user survey to calculate these parameters. In our setting, we test the PSM using 1,000 phone numbers, meaning that we cannot efficiently build upon user involvement at this scale. Based on the information provided in the previous sections and some test iterations with the data available, we selected (i) HLR, (ii) WhatsApp and (iii) Facebook as the overall dimensions for our scraping activities. Next, we present the privacy dimensions (Table 1) and the parameter setting (Table 2).

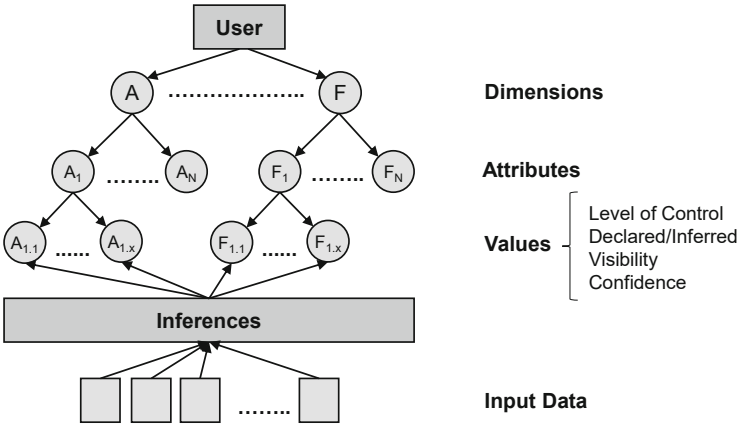

Fig. 1. Privacy scoring framework, adapted from Petkos et al. (2015)

Table 1. Overview of privacy dimensions

	Dimension	Attributes	Values	Range	Level of control	Declared/ inferred	Visibility	Confi-dence
A	HLR	Number	Original provider	{lookup successful = 1; no data = 0}	0	1	1	1
			Ported provider	{lookup successful = 1; no data = 0}	0	1	1	1
		User	Subscriber status	{unknown = 0; all other = 1}	0.25	1	1	1
			Roaming	{lookup successful = 1; no data = 0}	0	1	1	1
			HLR status	{lookup successful = 1; no data = 0}	0	1	1	1
B	Whats-App	User	WA_ Account	{lookup successful = 1; no data = 0}	0	1	1	1
		Profile	Last_Seen	{OCR successful = 1; no data = 0}	1	1	1	1
			Status	{OCR successful = 1; no data = 0}	1	1	1	1
			Profile_Pic	{data accessible = 1; no data = 0}	1	1	1	1
C	Face-book	User/Name	Account	{lookup successful = 1; no data = 0}	1	1	1	1
		Profile	URL	{lookup successful = 1; no data = 0}	0.5	1	1	1
			Timeline	{data accessible = 1; no data = 0}	1	0.5	1	0.5

Table 2. Parameter settings of the PSM

Parameter	Value	Description
Level of control	0	No influence
	0.25	Control is not impossible, but in contradiction to use case
	0.5	User might influence variable (up to the user)
	0.75	Control is possible and not in contradiction to use case (but a potential privacy issue)
	1	User has full control (but a clear threat)
Declared/inferred	0	Inferred
	1	Declared
Visibility	0	Private
	1	Public
Confidence	0	Unconfident
	1	Confident

3.2 Sample Number Creation

Generating random phone numbers, accessing a public HLR provider to verify them, and then using social media APIs to extract profiles is a common method of investigation, as these profiles are immediately converted into accumulated statistics. To test the adapted model, this paper follows the approach taken by [27], employing HLR lookups and data matching to build user profiles. Using this method, we test our PSM under realistic conditions. As a first step in data collection, a valid list of phone numbers is required. We created lists of potential phone numbers based on the service providers list from the federal network agency Germany. As the federal network agency only imposes the rule of a maximum of nine digits in a phone number, we created a list with potential phone numbers to crosscheck their validity, as a first step towards the PSM employing a HLR lookup [28]. We excluded all non-functional numbers in this step to give a final list of 1,000 existing numbers. After this initial preparatory step, the following section will address the primary data-mining part of our project. Using our list of 1,000 validated phone numbers, we wanted to find out which sensitive information we could.

3.3 Using OSINT to Identify Privacy Issues

We executed a thorough HLR lookup for the entire list of 1,000 phone numbers to fill our PSM data flow. We then wanted to investigate the WhatsApp data. At first, we conducted experiments with yosum, an unofficial API for WhatsApp (as no official API existed during the data gathering phase), but we were blocked by WhatsApp due to the massive number of contacts added within a short time frame. However, we were allowed by WhatsApp to add all of the numbers (enriched with pseudonyms) as a CSV file to a dummy phone. We also discovered WhatsApp Web to be an appropriate gateway to overcome the issue of the absence of an API.

We implemented the scraping activities with robot process automation (RPA) and Python scripts, which allowed us to download the current profile picture of each user, his/her status, and the last seen timestamp. It also allowed us to interpret the data using optical character recognition (OCR). In order to find out more personal details about the targets, we wanted to include at least one social network in our research. We discovered that several OSNs utilise phone numbers not only for the purpose of two-factor authentication but also as an identification criterion, for instance, to recover a Twitter or Facebook account in case of forgotten passwords. However, at the time when the project data were collected, parsing a specific phone number for a Facebook search was technically allowed, although this was stopped after the Cambridge Analytica leak. We implemented a Python script that processed all the generated phone numbers and searched for them on Facebook. When successful, our script saved a Facebook hyperlink to our database. Because of using RPA technology, we could avoid accessing Facebook only via official APIs. It was then possible for us to open the unique Facebook hyperlink and scrape the profile information. With respect to the users' privacy and research ethics, we did not mine the user data itself, but only classifier, e.g. if we were able to access sensitive information. Doing so, we computed the individual privacy score based on the dimensions and attributes described above.

4 Data Analysis and Results

The following sections present the results of the four steps of data collection and a combined analysis of the privacy scoring. We present the data in chronological order as generated during the research and aggregated in our PSM.

In total, we initially generated more than 3,000 phone numbers, from which we were able to verify 1,030 active and connected devices via HLR lookups (Fig. 2). This allowed us to further trace activities. The conversion rate of almost 30% indicated that our phone number generation procedure was adequate. In comparison with other research articles, this seems to be a good basis for creating a list of numbers for telephone surveys [7]. Furthermore, our script generated a wide spread over the most common mobile network providers.

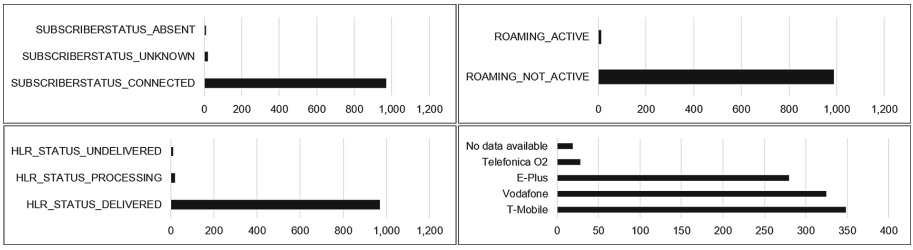

Fig. 2. HLR lookup results

The majority of cases were connected to the GSM network, delivered a valid HLR status signal, and were registered in their home country. However, we identified 11 users

in roaming mode. Although we do not publish personal status information in this section, we provide a classification of the status messages (Table 3) that were found.

Table 3. WhatsApp status analysis

Status classification	Total amount	Total percentage	Percentage of WhatsApp users
Not available: The status of the WhatsApp contact was invisible to unauthorised contacts	168	16.31%	33.47%
Empty: Ability to access the status was granted, but there was no input by the user	23	2.23%	4.58%
Standard status: The user selected one of the standard WhatsApp status messages such as "Hello there"	130	12.62%	25.90%
Individual status: The user input an individual status message	181	17.57%	36.06%
$\sum$	502	48.76%	100%

Sharing the last online timestamp with any contact is currently a pre-selected functionality of WhatsApp. In other words, about 40% users deactivated this feature. As mentioned above, we only captured the last-seen variable once and not as a time series, which would easily have been possible. Online-experiments[1] have shown that very accurate sleep/wake profiles of users can be generated in this way. In total, our approach revealed the targeted WhatsApp data in 20.50% of the total number bucket.

In a similar way to WhatsApp, we scraped the Facebook data by looking up personal profiles based on their phone numbers. To protect the privacy of the randomly chosen users, we first verified whether a Facebook account matched a phone number. In case of success, we handed that parameter over to a target list and only stored a categorisation of the information accessible (0 = nothing found, 1 = person identified and some information accessible, 2 = person identified and all information accessible). Full data access was on this OSN possible in 16 cases (1,6%). Assuming that these profiles are no fake but real profiles, this means a full deanonymization plus access to personal information.

The personal data itself, such as home town and so forth, was not downloaded but was available in several cases (Table 4). Once again, we observed a correlation between the WhatsApp and Facebook profiles, as we found zero cases where a Facebook profile was present but no WhatsApp profile was found.

By default, the link between the cellphone numbers and personal profiles of users is activated after users have entered their personal mobile numbers on Facebook. Thus, 72

[1] See https://www.onlinestatusmonitor.com, last accessed 2019/12/01.

Table 4. Facebook profile analysis

Status classification	Total amount	Total percentage	Percentage of WhatsApp users
1 = Person identified and some information accessible	55	5.34%	76.39%
2 = Person identified and all information accessible	17	1.65%	23.61%
$\sum$	72	6.99%	100%

users were confirmed as having a linked Facebook account. There are likely to be more users without a linked phone number or with higher data privacy settings.

Finally, we computed our PSM based on the results shown above and categorised the PSM scores in groups of zero and one PSM points (Fig. 3). We also weighted some PSM attributes higher than others in order to increase the mean of the PSM score: complete de-anonymisation of a phone number should have a high impact on the PSM score, even when other attributes are more secure. Thus, we chose factor three for the real name; highly sensitive information (gender and age) and sensitive information with a strong privacy impact (timeline data and profile picture) were weighted with factor two; and roaming information was weighted with factor 1.5. This was also done to give better coverage of the PSM groups with respect to a normal distribution.

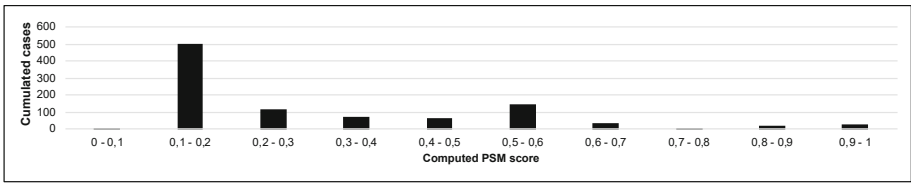

Fig. 3. Categorised PSM results

5 Discussion

Figure 4 shows grouped, weighted and visualised PSM model for further analysis. Three dimensions and six attributes were defined and tested with 1,000 users. This paper addresses a new aspect of data linkability in the privacy domain of IS research and thus provides several theoretical and practical contributions.

5.1 Theoretical Contribution

Research by [9] encouraged IS privacy researchers to conduct sample-driven, well-contextualised studies. Our research contributes to IS knowledge in exactly this field:

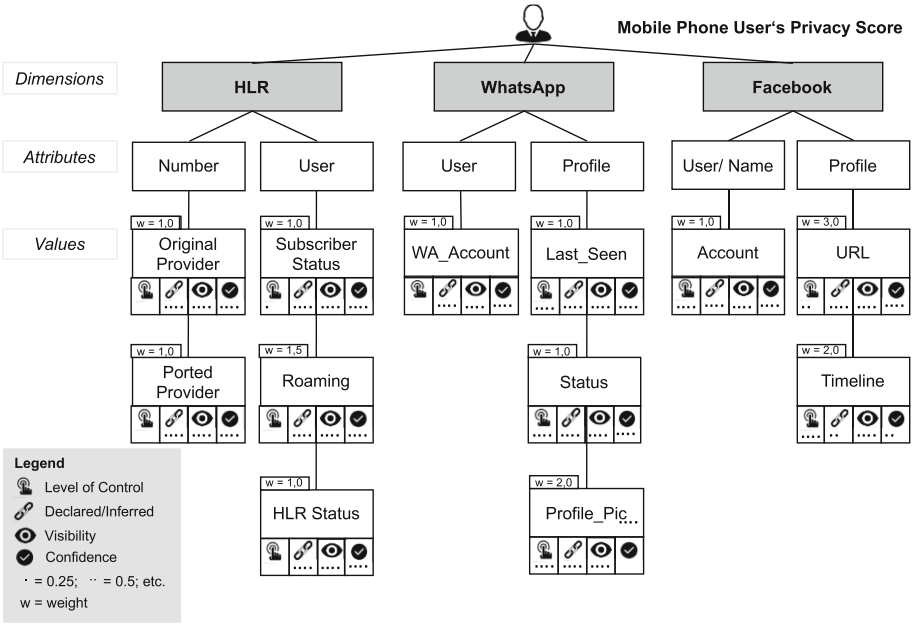

Fig. 4. Applied PSM model for mobile phone privacy

we recommend a PSM for mobile phone users as an indication of the perceived privacy of users and their behaviour in terms of a careful choice of security settings. Previous research has shown that awareness about privacy concerns when using a mobile social network does not influence users' behavioural intentions [29]. Our research builds upon this, as our hypothesis involved the underlying technical layer. We verified our hypothesis that a phone number represents an easily traceable footprint in both the GSM mobile phone network and the online network (OSN in particular) and should definitely be considered a personal privacy risk. Our research also included the body of literature with respect to privacy from an IS perspective, mobile phone privacy and PSM. This is IS research, since IS artefacts and their effects on users are studied, and particularly their privacy concerns. With respect to PSM as a quantification of users' privacy behaviour, we built our PSM based on an existing PSM framework [10] and selected dimensions, attributes, and values for the given domain. Due to the nature of this method, it can be assumed to be rigorous and to generate a reproducible result; we followed the framework of [10] and carefully documented all of the research steps for our part. The addition of an applied PSM to the existing body of knowledge is, in our view, an important step within the IS discipline.

The lack of literature addressing privacy issues at the GSM layer (and also in relation to the online communication layer) has been presented in the literature review section of this paper. To fill this gap, this study answers the research question by presenting an approach to user tracing across different communication layers and services. Our findings can be associated with privacy by design and privacy-enhancing technologies (PET) within IS research: storing unencrypted mobile phone numbers of the users of

a system could be problematic with respect to the GDPR, as this paper verifies our hypothesis of linkability. From a broader perspective, this paper aims to contribute to the overall IS privacy and security research activities in the context of big data. In our view, IS plays a major role in ethical and moral discussions about the usage of OSINT and other applied big data disciplines, particularly following the Cambridge Analytica scandal. With its interdisciplinary approach, IS should communicate within and beyond the research community about privacy issues and approaches for self-protection. As shown above, the model presented works well with real-life OSN data, and we hope to deliver new insights to researchers in the field of mobile communication privacy.

5.2 Practical Contribution

Our findings have important practical implications. Firstly, it is useful for the protection of minors. Children and young people use smartphones intensively, sharing their mobile phone number for many purposes (such as activating an online profile). Parents and schools need to educate children, and to let them know that using their phone number in a mobile app or service can be used to track their behaviour and online usage patterns. This educational aspect also serves to impede child pornography and sexual violence against children and young people [29]. We do not aim to stop the digitalisation of schools; however, for good reasons related to data protection, some federal states of Germany prohibit the use of WhatsApp as an official communication tool between children and teachers [30]. Thus, tools with better privacy options and GDPR-compliant services should be preferred. At the very least, parents should carefully monitor the privacy settings of both the messenger services and OSNs of their children and educate them about potential risks.

Secondly, our findings have shown that simply requesting data from the HLR can be an anchor point for further attacks, and particularly those that focus on political VIPs, enterprises or infrastructural organisations. We present a practical, useable and verified approach in Fig. 4 to test a user's mobile phone number for privacy issues. Pentesters or IT security managers can follow our PSM data flow to create a user-centric visualisation (comparable to a data-driven mindmap) in Maltego Teeth, which is a widely used pentesting tool for Linux. We will cover that important aspect in Fig. 5, considering also the further point.

Thirdly, IT security managers should (where it matters) blacklist at least those messaging apps where no restrictive privacy settings can be applied. A good practice here is to use Threema, in which communication partners can add each other without uploading their contact databases to the provider [31]. Although WhatsApp updated its privacy setting options during the writing of this paper, tracking the online status of a user is still possible [2].

As a further artefact of our research, we present a prototype of a single-page application (SPA) using the RPA technology in the background.[2] IT managers in organizations will have the possibility to calculate the PSM of a mobile phone number. By this automized approach, a privacy audit of Mobile Device Management (MDM) becomes feasible. Further, individual users can also specify which privacy aspects matter for them.

[2] The prototype can be accessed via https://github.com/swingingcode/bis2020_blackmirror.

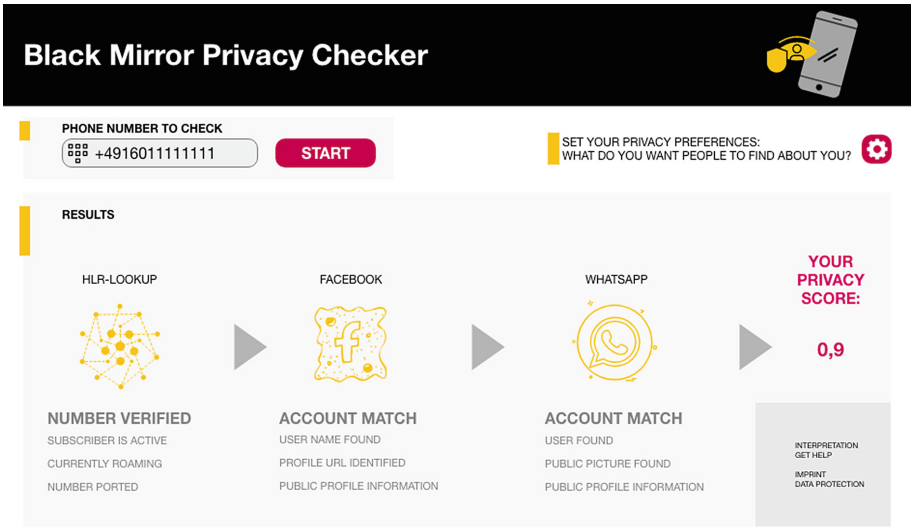

Fig. 5. Prototype of an RPA-implementation as single-page web application frontend

Thus, finetuning of the personal PSM configuration will be possible. As we developed the privacy checker on an open-source base, it will be easily applicable, for instance to other OSNs or company-specific aspects (e.g. LinkedIn visibility).

6 Conclusion

Privacy and security concerns are becoming extremely important, as human nature faces challenges in keeping pace with the ongoing technological revolution that we are all currently experiencing. Although some people are more cautious, and carefully review each new technology that they use, many others, especially younger people, grow up with rather careless attitudes towards the potential privacy risks that new mobile services can generate [32]. As previous research has shown, the behavioral goal of users in OSN, which is sharing information with as many as people as possible, contradicts with strict and limiting privacy settings [22]. The present study provides concrete evidence for this vulnerability and calls for closer attention from all the stakeholders in this context, especially scholars, professionals, and users.

Today, the omnipresence of mobile phones in all corporate, institutional and personal infrastructures offers major opportunities for seamless communication and comfortable user experiences. Although mobile phone privacy was already an important research field before the most recent leaks regarding Facebook, through the subsequent massive media coverage, a global wave of awareness of profiling activities based on online services has been created. We investigated users' behaviour in terms of their security settings and the role of phone numbers in this context, grounded on the hypothesis that mobile phone numbers could be used as a footprint and a link between the GSM network and an OSN. Based on the literature concerning privacy scores, we extended existing

approaches to measure privacy issues by quantifying data points in the HLR and selected online networks. We verified that a simple phone number is a sufficient starting point for gathering information about a victim's mobile phone status, OSN usage, and in some cases even for gathering the real name and further sensitive information such as gender, age, and so on. Such privacy attitudes can be transformed using novel design methods in human-technology interaction [33].

Our study has certain limitations. Firstly, the phone numbers used in our study represent only phone numbers from Germany. Secondly, a distinction between corporate and private phone users was outside of the scope of this work. Thirdly, we did not actively include users within the research process, as we wanted a large sample of test data. Thus, it was up to the research team to adjust the parameters within the PSM framework.

Future work could build upon our PSM to include further OSNs and other data sources. IoT devices connected via 5G networks will play a major role in future privacy issues, for instance privacy threats due to connected cars or smart devices. Dedicated search engines for this purpose already exist and will underline the linkability of mobile phone numbers and organizational data more.[3] Future IS research could make use of our GSM-based PSM and enhancing IoT privacy.

References

1. Agudelo-Serna, C.A., Ahmad, A., Bosua, R., et al.: Strategies to mitigate knowledge leakage risk caused by the use of mobile devices: a preliminary Study. In: ICIS 2017: Transforming Society with Digital Innovation, pp. 1–19. Seoul (2017)
2. Holland, M.: WhatsApp ermöglicht weiterhin Überwachung beliebiger Nutzer. https://www.heise.de/newsticker/meldung/WhatsApp-ermoeglicht-weiterhin-Ueberwachung-beliebiger-Nutzer-3857506.html. Accessed 07 Dec 2019
3. Dwyer, C., Hiltz, S.R., Passerini, K.: Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. Am. Conf. Inf. Syst. **123**, 339–350 (2007)
4. Bundesnachrichtendienst: OSINT. http://www.bnd.bund.de/DE/Auftrag/Informations-gewinnung/OSINT/-osint_node.html. Accessed 07 Dec 2019
5. Europol: Cyber Intelligence. https://www.europol.europa.eu/activities-services/services-support/intelligence-analysis/cyber-intelligence. Accessed 07 Dec 2019
6. Meffert, H., Burmann, C., Kirchgeorg, M.: Marketing. Grundlagen Marktorientierter Unternehmensführung. Springer, Wiesbaden (2012)
7. Kunz, T., Fuchs, M.: Pre-call validation of RDD cell phone numbers. A field experiment. In: JSM Proceedings (2011)
8. T-Systems International GmbH: Den Überblick über die wichtigen Orte haben. https://www.t-systems.com/blob/384750/cdfde6863685cf0f08068a53e9e18a84/DL_Flyer_Motionlogic.pdf. Accessed 07 Dec 2019
9. Bélanger, F., Crossler, R.E.: Privacy in the digital age: a review of information privacy research in information systems. MIS Q. **35**(4), 1017–1041 (2011)
10. Petkos, G., Papadopoulos, S., Kompatsiaris, Y.: PScore: a framework for enhancing privacy awareness in online social networks. In: 10th International Conference on Availability, Reliability and Security, pp. 592–600 (2015)
11. Liu, K., Terzi, E.: A framework for computing the privacy scores of users in online social networks. ACM Trans. Knowl. Discov. Data **5**(1), 1–30 (2010)

[3] An example of such a search engine is http://shodan.io, last accessed 2019/12/07.

12. Vidyalakshmi, B.S., Wong, R.K., Chi, C.H.: Privacy scoring of social network users as a service. In: Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015, New York, pp. 218–225, New York (2015)
13. Hamed, A., Ayed, H.K.B.: Privacy scoring and users' awareness for Web tracking. In: 6th International Conference on Information and Communication Systems, pp. 100–105. Fort Worth (2015)
14. Kaffel, H., Ayed, B.: Privacy risk assessment for web tracking. In: 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Vancouver (2016)
15. Fife, E., Orjuela, J.: Mobile phones and user perceptions of privacy and security. In: International Conference on Mobile Business, p. 23, Delft (2012)
16. Rechert, K., Meier, K., Wehrle, D., et al.: Location privacy in mobile telephony networks – conflict of interest between safety, security and privacy. In: IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, pp. 508–513. Dalian (2011)
17. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Official Journal of the European Union, pp. 1–88 (2018)
18. Deswarte, Y., Aguilar Melchor, C.: Current and future privacy enhancing technologies for the Internet. Ann. Telecommun. **61**, 399–417 (2006)
19. Herrmann, D.: Privacy issues in the domain name system and techniques for self-defense. IT-Inf. Technol. **57**(6), 388–393 (2015)
20. Lowry, P.B., Cao, J., Everard, A.: Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures. J. Manag. Inf. Syst. **27**(4), 163–200 (2011)
21. Külcü, Ö., Henkoglu, T.: Privacy in social networks: an analysis of Facebook. Int. J. Inf. Manag. **34**, 761–769 (2014)
22. Lankton, N.K., McKnight, D.H., Tripp, J.F.: Understanding the antecedents and outcomes of Facebook privacy behaviors: an integrated model. IEEE Trans. Eng. Manag. 1–15 (2019)
23. Kesdogan, D., Fouletier, X.: Power control in cellular radio systems. In: IEEE Wireless Communication System Symposium, pp. 35–40, London (1995)
24. Palat, S.K., Andresen, S.: User profiles and their replication for reduction of HLR accesses and signalling load. In: Proceedings of ICUPC 5th International Conference on Universal Personal Communications, IEEE, pp. 865–869, Cambridge (1996)
25. Arapinis, M., Ilaria Mancini, L., Ritter, E., et al.: Analysis of privacy in mobile telephony systems verifying interoperability requirements in pervasive systems. Int. J. Inf. Secur. **16**(5), 491–523 (2016)
26. Eren, E., Detken, K.-O.: Mobile Security. Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit. Carl Hanser Verlag, München, Wien (2006)
27. Costin, A., Isacenkova, J., Balduzzi, M., et al.: The role of phone numbers in understanding cyber-crime schemes. In: 11th Annual Conference on Privacy, Security and Trust, pp. 213–222, Tarragona (2013)
28. Bundesnetzagentur: Numbering plan for the numbering space for public telecommunications. https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/NumberManagement/numbering_space/NP_numbering_space_2016.pdf?blob=publicationFile&v=1. Accessed 07 Dec 2019
29. Abramova, O., Krasnova, H., Tan, C.-W.: How much will you pay? Understanding the value of information cues in the sharing economy. In: ECIS 2017 Proceedings, pp. 1011–1028, Guimarães (2017)
30. Baden-Württemberg, Kultusministerium.: Kommunikationsplattformen am Beispiel WhatsApp. https://it.kultus-bw.de/,Lde_DE/Startseite/IT-Sicherheit/Kommunikations-plattformen?QUERYSTRING=whatsapp. Accessed 07 Dec 2019

31. Karaboga, M., Masur, P., Matzner, T., et al.: Selbstdatenschutz. In: Schütz et al. (ed.) Schriftenreihe Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe (2014)
32. Frischmann, B., Selinger, E.: Re-Engineering Humanity. Cambridge University Press, Cambridge (2018)
33. Stibe, A., Cugelman, B.: Social influence scale for technology design and transformation. In: Lamas, D., Loizides, F., Nacke, L., Petrie, H., Winckler, M., Zaphiris, P. (eds.) INTERACT 2019. LNCS, vol. 11748, pp. 561–577. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-29387-1_33