MEDIATIZATION STUDIES 1/2018 DOI: 10.17951/ms.2018.1.2.69-84

SVEN BRAUN

NO ACADEMIC AFFILIATION
SB@DEVBRAUN.DE

ANNE-MARIE OOSTVEEN

OXFORD INTERNET INSTITUTE, UNIVERSITY OF OXFORD, GREAT BRITAIN
ANNE-MARIE@SOCIAL-INFORMATICS.NET

Encryption for the masses? An analysis of PGP key usage

Abstract. Despite the rise of alternatives, email remains integral to technology-mediated communication. To protect email privacy the encryption software Pretty Good Privacy (PGP) has been considered the first choice for individuals since 1991. However, there is little scholarly insight into the characteristics and motivations for the people using PGP. We seek to shed light on social aspects of PGP: who is using PGP for encrypted email communication, how and why? By understanding those using the technology, questions on the motivations, usability, and the political dimension of communication encryption can be contextualized and cautiously generalized to provide input for the design of privacy-enhancing technologies. We have greatly extended the scale and scope of existing research by conducting a PGP key analysis on 4.27 million PGP public keys complemented by a survey filled out by former and current PGP users (N = 3,727). We show that a relatively small homogeneous population of mainly western, technically skilled, and moderately politically active males is using PGP for privacy self-management. Additionally, findings from existing research identifying poor usability and a lack of understanding of the underlying mechanisms of PGP can be confirmed.

Keywords. Email communication, Pretty Good Privacy, Privacy Enhancing Technologies, privacy self-management, encryption, usability

1. Introduction

The means and tools of communication are changing over time. Despite the rising popularity of instant messaging on mobile devices within the last decade, email continues to play a significant role as a digital communication technology in everyday

life. As of 2016 using email was the most frequently performed online activity worldwide (Kaspersky 2016), and remains so today (Eurostat 2018; Kaspersky 2017). Alas, email communication is not private by default, but prone to potentially unwanted surveillance by corporations or governments.

Current approaches to regulate privacy provide individuals with a set of rights to manage their personal data, that is "rights to notice, access, and consent regarding the collection, use, and disclosure of personal data" (Solove 2013, p. 1880). In addition to regulation, actively self-managing privacy by taking technical measures is often considered crucial for effective data protection. Hence, for those who wish to keep their digital communication private, end-to-end email encryption becomes a remedy. The privacy-enhancing data and email encryption software Pretty Good Privacy (PGP) is considered the first choice for individuals to secure their email communication (Barenghi et al. 2015). In a political context, the software is being used to protect the communication of witnesses and activists, such as Edward Snowden (Gaw, Edward, Felten 2006; Greenwald 2014; Zimmermann 1996).

Given the importance of email communication in everyday life, and privacy in general, we find it remarkable that existing research is mainly limited to the technical elements of PGP. Regarding more social and political aspects, research has mostly explored the software's usability. In consequence, there is little scholarly insight into who is using PGP for email and data encryption. We seek to shed light on social aspects of using PGP and are guided by the research question of who is using PGP for encrypted email communication, how, and why? By understanding those using PGP, questions on the motivations, usability, and the political dimension of end-to-end encryption can be contextualized and cautiously generalized to provide input for the design of privacy-enhancing technologies.

Zimmermann (1999), the creator of PGP, sought to provide encryption for anyone. Among others, he addressed "ordinary citizens", political activists, and journalists. Securing digital communication to circumvent surveillance is a long-standing practice, with encryption being promoted amongst activists and investigative reporters over the last few years (Aouragh et al. 2015; Carlo, Kamphuis 2014; Gürses, Kundani, Van Hoboken 2016). With this in mind, we presume that, to evade surveillance, encrypted communication is more widespread in contexts of politically related communication, be it to protect interactions between actors such as politicians and other stakeholders or simply to share and discuss political issues. Hence, to understand whether encrypted communication is more prevalent with politically active individuals we will rely on the notion of civic engagement (Adler, Goggin 2005). The concept has more than one dimension, ranging from informal and individual action, such as engaging in political discussions with friends, to collective or formal actions such as running for public office. We located political activity in the center of the continuum, between formal and informal actions, which reflects engaging with different forms of advocacy organizations, contributing to charities, voting, or commenting on politics online.

By providing extensive empirical evidence, we greatly extend the scale and scope of existing research. Our work is based on an analysis of 4.27 million PGP public keys and complemented by a survey filled out by 3,727 current and former PGP users. Our work suggests that a relatively small homogeneous population of mainly western, technically skilled, and moderately politically active males is using PGP for encrypted email. Additionally, findings from existing research that identify poor usability and a lack of understanding of the underlying mechanisms of PGP can be confirmed. Our work contributes to discussions in computer-mediated communication and human-computer interaction and aims at supporting those who design technological solutions for individual privacy protection by providing insights into the hurdles for privacy technology adoption.

The study is divided into five parts: (i), the background on PGP, (ii) a review of related literature, (iii) an explanation of the methodology, (iv) an analysis and (v) a discussion of the results.

2. Background

PGP follows the community-led Internet standard OpenPGP (Callas et al. 2007) and is implemented in numerous software, such as the widely known GNU Privacy Guard (GPG). To use PGP for communications, both the sender and receiver need to self-generate a private and a public key. One encrypts an email with one's previously shared public key. Only with the corresponding private key can the receiver decrypt and read the message.

By providing digital signatures, PGP allows users to detect if data has been altered after being signed and to determine if the data was signed by the person who claimed to do so. Data can be both encrypted and signed, or either of both independently. For instance, open source software packages are often signed to guarantee data integrity and authentication.

Moreover, PGP contains a mechanism to express trust on other people's keys by explicitly signing them. This understanding of trust reflects the verification of *a key* rather than trust in *a person*. For example, if key A trusts key B, key C trusting key A could then decide to trust key B as well. A trust path from C to A to B would emerge. As a whole, signatures and trust paths are referred to as the 'web of trust'.

Public keys may be shared in person or uploaded to PGP public key servers. Once uploaded, keys cannot be deleted to prevent adversaries from uploading forged keys. To signal the validity of a key, users may mark keys or signatures as 'revoked' or with an expiration date after which it is marked as invalid and should no longer be used (Garfinkel 1995; Zimmermann 1995).

3. Related Work

Literature touching upon the social aspects of PGP can broadly be divided into two themes: research on the web of trust focusing on the collective level, and research on usability focusing on the individual level. Studies on the web of trust mostly focus on a subset of keys, the strongly connected component that is the largest connected group of signed keys. Within it, a 'small-world phenomenon' characterized by short trust path lengths could be detected (Čapkun, Buttyan, Hubaux, 2002; Ulrich et al. 2011). Warren, Wilkinson and Warnecke (2007) found that the overall connectivity of the web of trust increased over time, while social distance between subgroups slightly decreased. These changes can be traced back to real life events where people can sign each other's keys, such as Linux conferences. This level of analysis reveals that PGP is at least being used by a connected technical audience interacting with each other through signatures.

With regards to the usability of PGP, Whitten and Tygar (1999) found that it was too complicated for most users. In a usability test, most participants failed to perform basic tasks such as sending encrypted emails and made dangerous errors such as sharing their private keys. In a replication study, Sheng et al. (2006) found that the updated user interface still impairs usability and criticized it for providing little feedback to users. A more recent study concluded that modern PGP clients are still not sufficiently intuitive or usable (Ruoti et al. 2016). In addition to identifying the user interface as a source of problems, Garfinkel and Miller (2005) argue that trust is interpreted differently by users, and most PGP implementations do not effectively communicate the PGP concept of *trust in a key* instead of a person. Lastly it has been argued that different types of users, such as ephemeral or habitual users, have different needs that need to be reflected in the design of email encryption software (Gaw, Felten, Fernandez-Kelly 2006).

Besides usability, existing research provides little insight into how and why PGP is (not) being used for protecting communication. However, it provides grounds for assuming that PGP is used by experienced users and is thus not suitable for the average user.

4. Methodology

We conducted a macro-level analysis of all globally published PGP public keys and subsequently launched a complementary survey approved by our Institutional Review Board. A publicly available data set containing 4,270,992 keys public keys and their signatures as of 13/05/2016 was obtained from pgp.key-server.io. We disregarded keys with implausible creation dates before 1991 and after May 2016 as well as keys having no or malformed email addresses, leaving us with 4,113,983 keys for analysis (see Appendix B).

Our cross-sectional and self-administered survey ran in June 2016 and relied on the web-based Qualtrics platform. The questionnaire comprised 20 questions in

English (see Appendix A). Due to different survey flows a participant was asked a maximum of 19 questions and took approximately 10 minutes to complete. Informed consent and certification of legal age were required. The option to withdraw at any time without penalty was offered. Participants could select a 'Prefer not to say' option for all questions. No financial incentives for participation were awarded.

Almost all survey questions were developed from scratch, including questions on demographics that had to be adapted to a global scale of an unknown population. We conducted two cognitive interviews with PGP users and launched a pilot survey (N = 52) to test and refine the questionnaire. Some could not load the Qualtrics survey design due to privacy preserving web browser plugins, resulting in Likert-scale questions becoming unreadable. Hence, all such items were converted or removed.

Based on the response rate of the pilot survey, we randomly selected 200,000 email addresses to obtain a representative sample. To minimize the probability of sampling the same participant more than once, we combined distinct keys with the same email address (1,062,880 keys), leaving us with 3,051,103 to sample from. To reach ex-users as well, we did not encrypt our invitation email. Unfortunately we could not sign our invitation due to the technical limitation of the survey platform. A total of 59,254 invitation emails could not be delivered (29%). Eventually 3,787 surveys were completed, resulting in a 2.6% response rate after removing ineligible participants who did not meet the legal age requirement or had never used PGP. This response rate is not unusual for surveys where participants are invited over email (Schonlau, Fricker Jr., Elliot, 2002).

It is worth noting that we received about 370 response emails and three phone calls. Respondents were positive about the project, asking for more information, asking why the invitation was neither PGP encrypted nor signed, trying to verify our identity, or complaining about the receipt of unsolicited invitation email. One formal complaint was filed and resolved with the Institutional Review Board. This unusual reaction can clearly be traced back to the scale, but also to the privacy and security aware population that is more suspicious of unexpected emails (Wright, Marett 2010).

On the participant side, we acknowledge several limitations. Firstly, we could only contact those who published their public keys online, therefore our findings may not be fully applicable to those who only share their keys in person. Secondly, a non-response bias due to suspicions can be attributed to technical aspects of the invitation email. For instance, the invitation email contained an individual survey link that looked suspect to potential respondents. Moreover, we assume that those who did not feel safe to share information about themselves did not participate. It is possible that this might apply more often to people living outside Europe or North America. Thirdly, the telescoping error, which is the "tendency of respondents to report events as occurring earlier or later than they occurred" (Eisenhower, Mathiowetz, Morganstein 2004, p. 135), might have affected long-term users. Finally, especially with questions regarding opinions about and motivations to use PGP, respondents might have suffered a recall decay; the inability to properly recall relevant events and

associated memories. To reduce the chance of detecting non-existent associations resulting from this bias in the analysis stage, significance levels are set to 99% ($\alpha = 0.01$) instead of the social science convention of 95% ($\alpha = 0.05$). Nevertheless, readers are urged to interpret the following results with caution.

5. Results

5.1. PGP key analysis

As it is impossible to answer 'why' PGP is being used by conducting a key analysis, we focused on the 'who' and 'how' by looking at the distribution of keys over time, first names by gender, a geographical approximation based on email addresses, as well as on the use of keys and signatures.

Figure 1 depicts the distribution of key creations per year. A large number of keys, between 250,000 to 350,000 keys per year, were created between 1997 and 2001. Thereafter, key creations became less frequent, with about 100,000 to 150,000 keys per year, before taking off again in 2013.

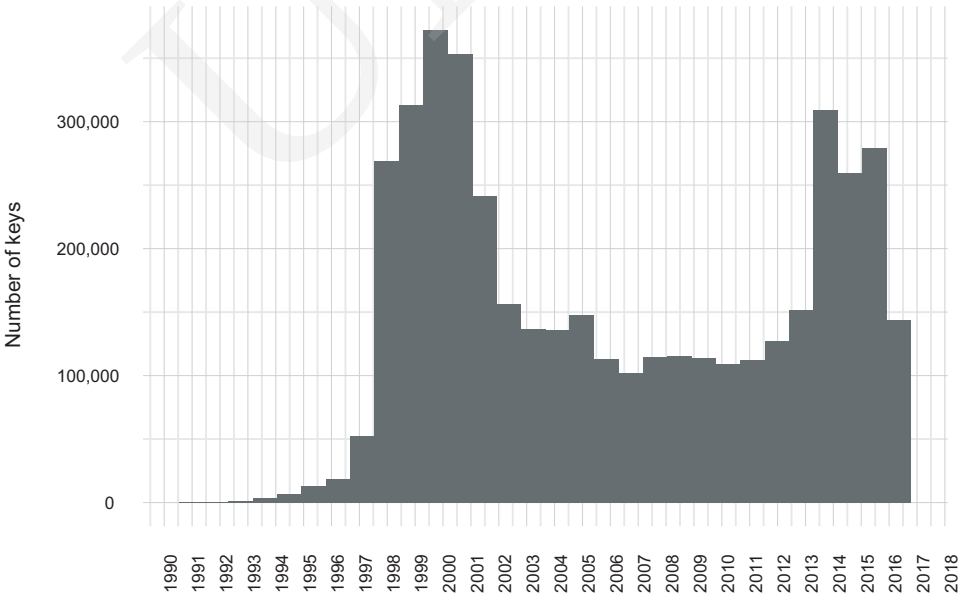

Figure 1. Key creations per year

Users can self-generate more than one key, hence the total number of keys does not translate into the number of users. As we merged keys by email addresses to identify

users with several keys, we observed that there was a large number of keys with distinct email addresses. If we assumed that each email address belonged to a different user, this number would indicate a large number of different PGP users having one key each (Median = 1.0, Mean = 1.3, SD = 1.4, N = 3,065,428). When it comes to all keys that were neither expired nor revoked as of May 2016, a total of 3.67 million keys could be considered as active. While these figures indicated a large number of individual users, in the context of the 27 years of PGP existence, the numbers were actually quite low, especially given that there were 3.39 billion Internet users in 2016 when we conducted the study (ITU 2016).

With regards to signatures, 4.97 million were created in total. However, out of all keys, only about 600,000 (12%) had been signed, and only 400,000 (8%) had signed other keys, resulting in a huge disproportion of signing and signed keys. This indicates that the 'small-world phenomenon' among signed keys detected in earlier research might very well be observed amongst those keys which signed and were signed. However, due to the lack of signatures the vast majority of PGP users were not part of the web of trust, but disconnected from all other keys.

We continued our analysis by looking at the gender distribution of PGP users. While acknowledging that there were more than two distinct genders, an approximation of first names by these binary categories should provide an estimation of the gender balance of PGP users. The first names of all User IDs were analyzed using the names corpus (Kantrowitz, Ross 1994). First names such as Christian or Kim were categorized both as male and female. To mitigate bias, two searches were run, first looking up male and then female names, and vice versa. The mean of both runs was skewed towards male users: 83.4% had male first names, while 16.4% had female first names (N = 1,874,652). This was only an imprecise approximation, as not all keys contained a first name, and in other cases it could not be detected as pseudonyms were often used (Orman 2015).

Thereafter we were interested in finding out where users came from. We examined email addresses as a rough estimation of location; however, this did not yield a sufficiently useful approximation of where users reside. Email addresses are registered with an email provider that is addressable by a domain name, such as gmail.com. However, top-level domains are a weak approximation of location, as global email services mostly offer .com addresses, and it is often possible to register country-code top-level domains even as a non-resident.

5.2. PGP survey analysis

To validate and back-up the findings from the key analysis, we turn to the complementing survey. All sample demographics are given in Table 1. In terms of gender, we could see a large number of males (94.9%), at over 10 percentage points higher than the first name analysis. The vast majority of respondents currently resided in Europe

or North America (90.0%) and identified as Caucasian or North American (84.1%). We also learned that most respondents were under 55 years of age, with about two-thirds between 25 and 44 years of age. The sample was highly educated, with 87.2% having university education or equivalent. The primary work sectors were related to IT (58.4%), followed by science and education (19.7%).

Table 1. Sample demographics

Variable	Value	Percentage	N
Gender*	Male	94.9	3,650
	Female	3.5	
	Transgender/Other/Don't know	1.6	
Age*	18 – 24	11.9	3,665
	25 – 34	33.1	
	35 – 44	29.1	
	45 – 54	17.3	
	≥ 55	8.7	
Area of residence	Europe	67.7	3,703
	North America	22.3	
	Asia	4.2	
	South America	2.7	
	Australia	2.3	
	Africa	0.8	
Ethnicity*	Caucasian / North American	84.1	3,402
	Asian	4.1	
	Russian	2.5	
	Other	9.3	
Education	University or equivalent	87.2	3,674
	Apprenticeship or equivalent	8.2	
	Other	9.3	
Primary work sector*	IT / Telecommunication / Computer & Electronics Manufacturing	58.4	3,236
	Scientific or Technical Services / Education	19.7	
	Other	21.9	

*Collapsed categories

The survey showed that 75.7% of respondents were actively using PGP, while 24.3% had given up. The respondents stated having four keys on average (Median = 4.0, Mean = 5.2, SD = 18.6, N = 3,414). This differed significantly from the mean of one key per person indicated by the key analysis ($t(3413) = 13.58$, $p = 0.00$, Power = 1.0), providing strong support for the assumption that most users had more than one PGP key, and countering our key analysis result.

About three quarters of the respondents used their key for personal reasons (77.1%), followed by 39.7% professional, and 8.5% for other uses (e.g. software development).

Email encryption/decryption is an activity carried out most by respondents with PGP (90.7%), followed by signing and verifying other data, such as downloads (65.3%), as well as data encryption and decryption (55.5%). About half (50.7%) engaged in signing or verifying other people's keys. This did not reflect the 15% of signed keys seen in the key analysis. Rather, this observation indicated that a large number of users verified the authenticity of keys manually, but seldom issued signatures. When using PGP for email encryption, the vast majority did so with only *some* of their contacts (84.5%), 3.3% for *most*, and a minority (0.5%) for *all.*

In explaining why they chose PGP technology in the first place, the majority of respondents indicated that they merely wanted to try PGP out of curiosity (71.2%), followed by those who were responding to government's activities such as surveillance (31.2%). Notably, only 29.1% of users started with PGP as a means to contact one or more people confidentially. An additional 27.9% began using PGP spurred on by the example of their peers. For 19.2% of respondents PGP was required for work.

The vast majority of former users gave up using PGP because they had no one else to communicate with using encryption (72.4%), had no need to encrypt information (25.3%), felt it lacked an intuitive software interface (23.8%), or had no PGP availability on their platforms (such as mobile) (23.6%). The lack of a communication partner indicated the missing network effect of PGP. This is especially consequential given that email encryption is the most reported use.

To understand why only about 15% of keys participate in the web of trust, we asked about the motivations not to sign or verify keys. As seen before, the most prominent reason is that respondents have nobody else to communicate with using PGP (47.2%). About a quarter of respondents (22.8%) had no need for signatures, and 16.7% did not fully understand how signatures worked. Our results only partially support findings from the literature that the main barrier to participation in the web of trust is the lack of understanding of the underlying trust model by PGP users.

Due to the earlier-mentioned political use, it is worth investigating the political activities of PGP users to understand whether email encryption might be more prevalent in political contexts (Figure 2). To identify underlying factors for political activity that we conceptualized as civic engagement, we conducted a Principal Component Analysis on the political variables 'engagement with political advocacy' and 'political activities in the last year'. Regarding engagement with advocacy organizations, respondents were mostly engaged with technology-oriented organizations such as hackerspaces. This, again, speaks to a technically-skilled PGP usership. Apart from technology-oriented associations, only a minority of respondents were active in advocacy. Political activities in the previous year were more evenly balanced than engagement with advocacy organizations. Respondents were less formally organized, but seem nonetheless moderately politically active.

Turning to the analysis, the 'None of the above' options were excluded from the beginning, as they already indicated non-activity. After eliminating three variables that

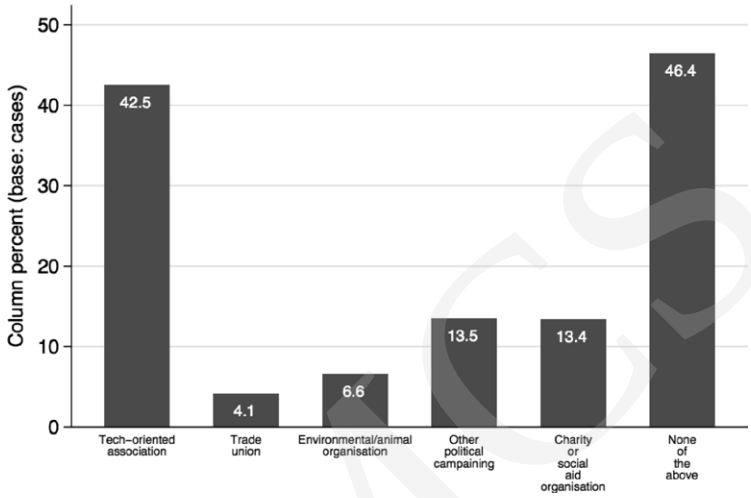

Figure 2a. Engagement with advocacy organizations

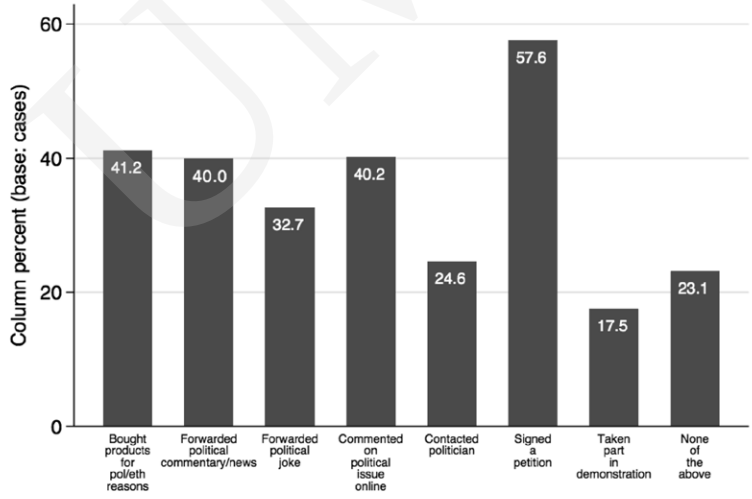

Figure 2b. Political activities in the last year

did not load above 0.3 on any of the components (Blank, Groselj 2014), nine variables were used for the Principal Component Analysis. Throughout, varimax rotations and the Kaiser's criterion were applied to identify two components (see Table 2).

The first component clusters more online-based activities, such as forwarding or sharing political news or funny political content, as well as commenting on political issues online. Signing a petition is the lowest loading on this factor, but in this case might also refer to online petitions. From this component, we constructed an online

Table 2. Political activity factor loadings from Principal Component Analysis. Loadings ≤ |0.3| were omitted or eliminated.

Variable	Online activities	Offline activities
Technology-oriented association		
Trade union		0.35
Environmental / Animal organization		0.51
Other political / campaigning organization		0.49
Charity or social aid organization		0.48
Conscious consumerism		
Forwarded political news	0.54	
Forwarded funny political content	0.54	
Comment on politics online	0.52	
Contacted politician / government official		
Signed a petition	0.32	
Taken part in a demonstration / march		0.32
Eigenvalues	2.28	1.80

political activity scale, ranging from 0 (low activity) to 4 (high activity), with 2.5 being the cutoff for low and high (Median = 1.0, Mean = 1.7, SD = 1.4, N = 3,285). There was a significant difference in the scores for online political activity being ≤ 2.5, the mean value of the scale ($t(3284) = -11.39$, $p = 0.00$, Power = 1.0). This confirms low online political activity among PGP users.

The second component comprises advocacy and offline political activity, which is why membership in different political organizations and taking part in a public demonstration or march are clustered together. Notably, being part of a technology-oriented association did not load high on either component, and can thus not be treated as political activity per se. The second component allowed for an offline political activity scale ranging from 0 (low activity) to 5 (high activity), with 0–2 as low levels of activity and 3–5 as high levels of activity (Median = 0.0, Mean = 0.6, SD = 0.9, N = 3,285). As with online political activity there was also a significant difference in the scores for ≤ 3, the mean value of the scale ($t(3284) = -0.0012$, $p = 0.00$, Power = 1.0). This similarly confirms low offline political activity among PGP users. With regard to demographics, there are no significant differences for both types of political activity. These results suggest that, contrary to our assumption, the population of PGP users is not very politically active overall, neither online nor offline.

6. Discussion

Returning to the literature on the web of trust, we need to stress that the vast majority of key holders do not actively participate in the web of trust due to the lack of communication partners using PGP. However, for those who do, the 'small-world

phenomenon' found in the past can now be explained from a social perspective. Only a minority of users actively engage in signing keys, as at least for some there are barriers to understanding the concept. As Warren, Wilkinson and Warnecke (2007) argued, signing keys may often take place at social events, such as Linux conferences. Such gatherings could most likely be classified as meetings of people with high technical skills, inasmuch as the participants have other people to communicate with, use PGP for software development, and, additionally, meet at least the skills and probably other demographic criteria observed above.

In a global context, PGP users are absolutely unrepresentative. Globally, 49.6% of humans are women, 61% of the population is aged between 15–59 (as compared to 91.3% of PGP users being less than 55 years old), and merely 14.7% of the world population live in Europe or North America compared to 90.0% of the surveyed PGP users. The level of education and primary work sector of respondents is equally unrepresentative (UN 2017; World Bank 2016). With regard to Internet users, the sample population is skewed a little less. In 2014, Internet penetration rates were highest in Europe (79.1%) and the Commonwealth of Independent States (66.6%), followed by 35% in the Americas (ITU 2016). As a result, the sample is disproportionately skewed.

It is worth noting that in some regions, such as China, instant messaging is the prevalent form of technology-mediated communication, rather than email (Horowitz 2017). Moreover, we could only find limited PGP software for Asian languages. In addition to our English-only questionnaire, this might partially explain why we did not see a large Asian participation in encrypted email communication.

Placed in a historic context, PGP exports to outside the US was initially classified as unlicensed munitions exports. In consequence, the software's developer was investigated by the US government, calling attention to PGP and the regulation of cryptography in general. Together with other issues related to encryption, individuals and industry challenged the US government to remove any export restrictions on cryptography in the 1990s, a period known as the Crypto Wars (Kehl, Wilson, Bankston 2015). More recently, in light of global government surveillance revelations (Greenwald 2014), this inherent political dimension to PGP might have re-emerged. These two political periods or events correlate with PGP key generations, peaking at the end of the 1990s and again after 2013 (see Figure 1). Yet, our results suggest that PGP is not used by highly politically active people, at least when conceptualizing political activity by civic engagement. But given that PGP "empowers people to take their privacy into their own hands" (Zimmermann 1999), using the software to protect one's privacy and to challenge governments might itself be seen as an inherent political act to reclaim privacy, even by those who are not otherwise intensely politically active. This contrast can be conceptualized with Kubtischko's (2017) distinction of acting *with* media and acting *on* media. Primarily, we focused on how and in which political contexts people tend to use PGP (acting *with* media). Yet, the engagement by tech-savvy people with a similar social network using encrypted communication

to deal with and evade surveillance itself could be understood as political agency (acting *on* media).

Using PGP to encrypt online communications could thus been seen as an act of "privacy literacy" (Debatin 2011), where users inform themselves on how to protect their communications and take action using a privacy-enhancing technology in order to escape the "surveillance-industrial complex" (Trottier, Fuchs 2015). Interestingly, the self-perception of the use of PGP being a political act is not pronounced among PGP users as only one third of respondents claimed that they did so in response to government actions – as compared to more than two third claiming that they got started with PGP because they wanted to try it out.

Using encryption for mediated communication can be perceived as form of socio-cultural practice that presupposes a collectively generated social, cultural, legal, and technological infrastructure that can be relied on to exercise privacy self-protection practices. Empirical evidence shows that this practice is not wide-spread. Matzner et al. (2016) take a step back and ask whether individuals should be responsible for privacy self-protection at all. They argue that as long as data protection "is not considered a collective, profoundly political endeavor", privacy self-management is an "ill-fated practice" (p. 303).

In fact, most respondents claimed that they do not use PGP because they have no one to communicate with. This indirectly may confirm research on the user interface, finding that it impairs usability. If PGP is really hard to use, users might find only few communication partners for encrypted email communication. In other words, if privacy protection is not designed for, or activated by default to reach a large user base, the consequence is that its impact will be limited.

We found 4.11 million PGP keys published on the key servers containing an email address. Of the 200,000 respondents invited, 29% of survey invitation emails could not be delivered. Extrapolated, at least 1.2 million keys may not be in use any more due to email mortality. Given the fact that users own on average four keys, there might only be about 730,000 users of PGP. After subtracting the 25% of ex-users, PGP might possibly draw on as few as 550,000 active users.

While in nearly three decades PGP may have reached less than one million users and has therefore not achieved encryption for the masses, the mobile communication application WhatsApp reached a billion people in only a few years (Metz 2016). In contrast to emails, commercial products and thus market solutions like WhatsApp build encryption into their instant messaging products and enable it by default. In the context of the emerging use of mobile devices and instant messaging, unprotected communication gradually ceases to exist, providing users with private communications by default.

7. Conclusion

PGP was developed to safeguard privacy in digital communication. Yet, it requires a specific technical skill set and social environment. We found that PGP is used by a well-educated, technologically curious and skilled homogenous male minority. Moreover, we estimate that there might be as little as 550,000 active PGP users. Based on the demographics and key usage, it can be concluded that, practically speaking, PGP does not provide encryption for the masses. To reach the masses, evidence suggests that it should be easy to understand and enabled by default. Otherwise, there is the risk of inequalities in privacy protection between those who can actively self-manage their privacy and those who cannot. When shifting from email to other kinds of technology-mediated communication such as mobile instant messaging, the gap regarding the protection of communication privacy is already partially decreasing.

Turning to the political dimension of technology-mediated communication, PGP users might not be overly politically active when taking civic engagement as a basis – even though one third started using PGP as a reaction to government actions such as surveillance. In this sense, deliberately using software to protect one's digital communication to oppose governments might itself be a political act to reclaim privacy. In contrast, there are more user-friendly corporate-owned market solutions like WhatsApp providing encryption by default. However, it can be questioned whether using such out of the box solutions is a comparable political act in the sense of privacy self-management. Thus, we suggest further research to investigate how the practice of privacy protection is being re-negotiated by shifting from an act of privacy self-protection requiring a certain skill set to a market-provided solution, and consequently how such developments contribute to privacy protection from a broader socio-political point of view.

References

Adler R., Goggin J. (2005). What do we mean by "civic engagement"? *Journal of Transformative Education*, Vol. 3(3), pp. 236–253.

Aouragh M., Gürses S., Rocha J., Snelting F. (2015). FCJ-196 Let's First Get Things Done! On Division of Labour and Techno-political Practices of Delegation in Times of Crisis. *The Fibreculture Journal*, Vol. 26, pp. 209–238.

Barenghi A., Federico A., Pelosi G., Sanfilippo S. (2015). *Challenging the Trustworthiness of PGP: Is the Web-of-Trust Tear-Proof?* In G. Pernul, P. Y A Ryan, E. Weippl (Eds.), *Computer Security – ESORICS 2015*. Springer: Cham, pp. 429–446.

Blank G., Groselj D. (2014). Dimensions of internet use: amount, variety, and types. *Information, Communication & Society*, Vol. 17(4), pp. 417–435.

Callas J., Donnerhacke L., Finney H., Shaw D., Thayer R. *OpenPGP Message Format (RFC No. 4880)*, https://tools.ietf.org/html/rfc4880, 06.10.2018.

Čapkun S., Buttyán L., Hubaux J.-P. (2002). *Small Worlds in Security Systems*. In *Proceedings of the 2002 Workshop on New Security Paradigms*. ACM Press: Virginia Beach, pp. 28–35.

Carlo S., Kamphuis A. (2016). *Information Security for Journalists*. The Centre for Investigative Journalism, https://tcij.org/bespoke-training/infosec/, 06.10.2018.

Debatin B. (2011). *Ethics, Privacy and Self-Restraint in Social Networking*. In S. Trepte, L. Reinecke (Eds.), *Privacy Online*. Springer: Berlin, pp. 47–60.

Eisenhower D., Mathiowetz N. A., Morganstein D. (2004). *Recall Error: Sources and Bias Reduction Techniques*. In P. P. Biemer, R. M. Groves, L. E. Lyberg, N. A. Mathiowetz, S. Sudman (Eds.), *Measurement errors in surveys*. Wiley: Hoboken, pp. 125–144.

Eurostat. 2017. *Community Statistics on Information Society. Individuals – Internet Activities (isoc_ci_ac_i)*, http://ec.europa.eu/eurostat/data/database?node_code=isoc_ci_ac_i, 06.10.2018.

Garfinkel S. (1995). *PGP: Pretty Good Privacy*. O'Reilly: Sebastopol.

Garfinkel S., Miller R. C. (2005). *Johnny 2: A User Test of Key Continuity Management with. S/MIME and Outlook*. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*. ACM Press: Virginia Beach, pp. 13–24.

Gaw S., Felten E. W., Fernandez-Kelly P. (2006). *Secrecy, Flagging and Paranoia: Adoption Criteria in Encrypted E-Mail*. In *Proceedings of the 2006 SIGCHI Conference on Human Factors in Computing Systems*. ACM Press: New York, pp. 591–600.

Greenwald G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books: New York.

Gürses S., Kundnani A., Van Hoboken J. (2016). Crypto and empire: the contradictions of counter-surveillance advocacy. *Media, Culture & Society*, Vol. 38(4), pp. 576–590.

Horowitz J. (2017). *While the rest of the world tries to "kill email," in China, it's always been dead*. Quartz, https://qz.com/984690/, 06.10.2018

ITU International Telecommunication Union (2016). *ITU Key ICT Indicators for Developed and Developing Countries and the World (Totals and Penetration Rates)*, http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx, 06.10.2018.

Kantrowitz M., Ross B. (1994). *Names Corpus, version 1.3*. https://www.cs.cmu.edu/afs/cs/project/ai-repository/ai/areas/nlp/corpora/names/, 06.10.2018.

Kaspersky. 2016. *The Kaspersky Cybersecurity Index H1 2016 Online Activity*. https://index.kaspersky.com/metrics/onlineactivity, 06.10.2018.

Kaspersky. 2017. *The Kaspersky Cybersecurity Index 2017 Online Activity*. https://index.kaspersky.com/metrics/onlineactivity, 06.10.2018.

Kubitschko S. (2017). Acting on media technologies and infrastructures: expanding the media as practice approach. *Media, Culture & Society*, Vol. 40(4), pp. 629–635.

Metz C. (2016). *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*. Wired, http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/, 06.10.2018.

Orman H. (2015). *Encrypted Email. The History and Technology of Message Privacy*. Springer: Cham.

Ruoti S., Andersen J., Heidbrink S., O'Neill M., Vaziripour E., Wu J., Zappala D., Seamons K. (2016). *"We're on the Same Page": A usability study of secure email using pairs of novice users*. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM: Virginia Beach, pp. 4298–4308.

Schonlau M., Fricker Jr. R., Elliot M. (2002). *Conducting Research Surveys via E-Mail and the Web*. Santa Monica: RAND.

Sheng S., Broderick L., Koranda C. A., Hyland J. J. (2006). *Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software*. Poster for the Symposium on Usable Privacy and Security, Pittsburgh, PA.

Solove D. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, Vol. 126(7), pp. 1880–1903.

Trottier D., Fuchs C. (2014). *Theorising social media, politics and the state: An introduction*. In Trottier D., Fuchs C. (Eds.) *Social media, politics and the state*. Routledge: New York, pp. 15–50.

Ulrich A., Holz R., Hauck P., Carle G. (2011). *Investigating the OpenPGP Web of Trust*. In V. Atluri, C. Diaz (Eds.), *Computer Security – ESORICS 2011*. Springer: Cham, pp. 489–507.

UN United Nations Department of Economic and Social Affairs Population Division. (2017). *World Population Prospects: The 2017 Revision. st/esa/ser.a/377*, https://esa.un.org/unpd/wpp/, 06.10.2018.

Verba S., Nie N. H., Kim J.-o. (1978). *Participation and Political Equality: A Seven-nation Comparison*. Chicago: University of Chicago Press.

Warren R. H., Wilkinson D., Warnecke M. (2007). *Empirical analysis of a dynamic social network built from PGP keyrings*. In E. Airoldi, D. M. Blei, S. E. Fienberg, A. Goldenberg, E. P. Xing, A. X. Zheng (Eds.), *Statistical network analysis: models, issues, and new directions*. Springer: Cham, pp. 158–171.

Whitten A., Tygar J. D. (1999). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. In *Proceedings of the 8th USENIX Security Symposium*. McGraw-Hill: Washington, pp. 169–183.

Wright R., Marett K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, Vol. 27(1), pp. 273–303.

World Bank. (2016). *World Development Indicators*. http://data.worldbank.org/indicator/, 06.10.2018.

Zimmermann P. (1995). *The Official PGP User's Guide*. MIT Press: Cambridge.

Zimmermann P. (1996). *Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation*. https://philzimmermann.com/EN/testimony/index.html, 06.10.2018.

Zimmermann P. (1999). *Why I Wrote PGP*. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html, 06.10.2018.