Glencora Borradaile*, Kelsy Kretschmer, Michele Gretes, and Alexandria LeClerc

The Motivated Can Encrypt (Even with PGP)

Abstract: Existing end-to-end-encrypted (E2EE) email systems, mainly PGP, have long been evaluated in controlled lab settings. While these studies have exposed usability obstacles for the average user and offer design improvements, there exist users with an immediate need for private communication, who must cope with existing software and its limitations. We seek to understand whether individuals motivated by concrete privacy threats, such as those vulnerable to state surveillance, can overcome usability issues to adopt complex E2EE tools for long-term use. We surveyed regional activists, as surveillance of social movements is well-documented. Our study group includes individuals from 9 social movement groups in the US who had elected to participate in a workshop on using Thunderbird+Enigmail for email encryption. These workshops tool place prior to mid-2017, via a partnership with a non-profit which supports social movement groups. Six to 40 months after their PGP email encryption training, more than half of the study participants were continuing to use PGP email encryption despite intervening widespread deployment of simple E2EE messaging apps such as Signal. We study the interplay of usability with social factors such as motivation and the risks that individuals undertake through their activism. We find that while usability is an important factor, it is not enough to explain long term use. For example, we find that riskiness of one's activism is negatively correlated with long-term PGP use. This study represents the first long-term study, and the first in-the-wild study, of PGP email encryption adoption.

Keywords: PGP, usability, human-factors

DOI 10.2478/popets-2021-0037

Received 2020-11-30; revised 2021-03-15; accepted 2021-03-16.

1 Introduction

Controlled lab studies have identified usability issues that are particular to secure communications technology, and addressing these issues can increase security through correct tool use. Whitten and Tygar's seminal "Johnny Can't Encrypt" paper, as well as replications of their method, have found persistent usability issues with end-to-end encrypted (E2EE) PGP email over the past 20 years [17, 51, 56, 61]. Others have sought to understand what roles key exchange, trust, and transparency have on the usability of PGP [4, 5, 50]. Each of these studies were in a time-limited laboratory setting with participants who are largely first-time users recruited from university campuses. These studies tend to be forward-looking through suggesting design improvements and testing proof-of-concept prototypes.

However, despite usability issues, there exists a population of users with an immediate need for private email communication who cannot wait for improvements to be made to existing PGP email solutions. Activists, journalists and lawyers have a need to use secure communication technology, specifically email, but often face obstacles in adoption [25]. E2EE messengers such as Signal [21] provide easier-to-use alternatives, but because these tools lack certain functionality, users continue to opt for less secure alternatives in order to work effectively [1, 5, 26, 29, 33].

Surveillance against social movement work has been long-standing and persistent [9, 11, 28–30, 55]. The US government has long been known to use surveillance to

***Corresponding Author: Glencora Borradaile:** School of Electrical Engineering and Computer Science Oregon State University, E-mail: glencora@oregonstate.edu
Kelsy Kretschmer: School of Public Policy Oregon State University, E-mail: kelsy.kretschmer@oregonstate.edu
Michele Gretes: School of Electrical Engineering and Computer Science Oregon State University, E-mail: mgretes@riseup.net
Alexandria LeClerc: School of Electrical Engineering and Computer Science Oregon State University, E-mail: leclerca@oregonstate.edu

support interference of social movements as was notable during the Civil Rights Era through COINTELPRO, resulting in such extreme outcomes as the murder of Black Panther Party leaders. Surveillance and interference tactics have continued into the modern era [40], despite formal protections through the First and Fourth Amendment that should protect dissent and public engagement through activism. Only E2EE provides mathematically formal protections against illegal search.

Starting in 2014, in partnership with the Civil Liberties Defense Center (CLDC), a non-profit which provides legal support to US social movement groups, a subset of our research team developed and deployed digital security workshops for social movement groups including one on PGP email encryption. The CLDC encourages the use of E2EE technologies as robust backup to the legal protections of "I do not consent to this search" and to counter the chilling effect created by mass surveillance [39]. Our experience with the CLDC's use of PGP and with workshop participants' use of PGP over the span of several years suggested that these users had better success with PGP email than PGP usability research would indicate. We deployed a follow-up survey of PGP workshop attendees in order to understand if this was true, and if so, why.

In this research, we ask: How do users with concrete privacy threats respond in the long term to training that aims to overcome the documented usability issues of PGP email encryption?

We do not seek to uncover what aspects of a particular tool should be changed to increase the ease with which a user can learn to use the tool for the first time as in PGP usability studies. Rather we seek to understand what conditions lead to success or failure to overcome usability issues with PGP email encryption in the long term. We hypothesize that our workshop participants are more motivated to get PGP working than the average user and that this motivation stems from the activities in which they engage.

We adopt a method of analysis from political science to understand the combinations of conditions that explain the outcome (adopting or not adopting long-term PGP use). While we consider ease of use as one factor, we explore the interplay of this factor with other factors such as motivation and the risks that individuals are undertaking (Section 3). We look at two types of motivation: individual (wanting to protect one's own information) and group (wanting to protect a group's information or activities). We look at risk in terms of the potential consequences (including loss of employment, fines or criminal charges). We describe how we measure these factors in Section 4.4.

We perform a Qualitative Comparative Analysis (QCA, Section 4.3). QCA is not a statistical method, but is rather a reproducible means of organizing descriptive data for qualitative analysis. QCA is appropriate for understanding a small number of detailed cases, such as our sample ($n = 19$).

We find that the participants who adopted PGP in the long term are characterized by finding PGP relatively easy to use, *and*

- being individually motivated to adopt PGP, *or*
- not engaging in activism or engaging only in low-risk activism.

On the other hand, the participants who did *not* adopt PGP in the long term are characterized by:

- finding PGP difficult to use *and* belonging to a community using other secure communications technology; *or*
- finding PGP difficult to use *and* engaging in high-risk activism; *or*
- not being individually motivated to adopt PGP *and* engaging in high-risk activism.

The negative correlation with risk is disappointing, as digital security trainers would prefer that higher-risk individuals take their digital security more seriously (see Section 6.2).

This analysis uncovers aspects that may help guide digital security trainers: certainly there is a need to overcome usability barriers, but it may also help to understand what brought an individual to the training and tailor the training to that. For example, making sure high-risk individuals understand what they may individually gain through increasing their digital security.

Our study is the first long-term study of PGP email encryption. It is also the first in-the-wild (e.g. out of the laboratory) study of PGP email encryption adoption as our participants were not research subjects at the time of training. Our study population is unique, and a challenging one from which to recruit. We recruited 17 members of social movement organizations, including direct-action groups, and 2 individuals not engaged in social movement organizing but who participated in the workshops. These subjects provide insight into the ability of motivated individuals to overcome usability issues in encryption technologies. This work also reflects the importance of motivation, as found from McGregor et al. [35] as well as contextualizes the obstacles outlined

by Renaud et al. [45] and Abu-Salma et al. [2] in the uptake of secure communication.

2 Context and Motivation

The focus of this work is activists who use email for their organizing and whether they adopt PGP email encryption in the long term following a training. In this section we give context for why this is our focus and why it is relevant. Partly, the focus on email and PGP is a result of when this research started (before simpler E2EE communication options were widely used). However, despite the movement of activist organizing onto E2EE messaging apps, many activist groups continue to use email in addition to other targeted groups (such as journalists and lawyers).

2.1 Why Activists?

In social movement groups across the political spectrum, individual activists frequently valued both transparency in their organizing work, and have deep concerns about surveillance and privacy. For example, Agarwal et al. [3] found that members from Tea-Party groups (on the political right) and communities spurring from Occupy Wall Street (on the political left) expressed similar concerns about security of both group and personal information, but at the same time they wanted their group's decision-making processes to be transparent. This creates a critical dilemma for activists; they need open communication within their communities, at the same time those communities are increasingly fearful of surveillance from corporations and the government. Members must find a balance for these conflicting needs given the risk that members will disengage if they fear their information is not secure, or when they feel their fears are not attended to by leaders [3, 34, 48].

These fears are not unfounded. Digital attacks on social movement groups have been well documented [11, 28–30, 55], and digital surveillance has been able to breach what were previously established safe-havens from surveillance [28]. The integration of technology into everyday life allows for greater, and richer data collection, that requires more expertise to secure.

The unique demographics and needs of activists in terms of socio-economic status, education, and access to technology influence how activists use technology. In her study of how class shapes digital activism, Schradie [54] found that working class activists frequently lacked the financial means to develop internet communication skills and, when faced with technological challenges, lacked the knowledge to fix them [19, 38]. Self-education can also be complicated; even though information on secure practices is widely available, users have a hard time prioritizing what is important, and what they do prioritize is often not aligned with what experts recommend [44]. Additionally, even established organizations that support or conduct social movement work often face the same threats as private sector or government organizations, but have access to far fewer resources by comparison [11, 55].

Compared to the participants of evaluations held on university campuses, users involved in social movements differ from what is considered the average user. Their risk level, including potential consequences may provide stronger motivation for secure communication than the typical user. While this may mean our observations would not generalize to *average* users, we believe that our observations will have impacts for at-risk groups (e.g. lawyers, journalists and broader communities of resistance), which we discuss further in Section 6.

2.2 Why Email?

In most groups, email serves as a vital tool in their organizing work and communicating openly with other community members. Activists find email useful in every part of social movement activism, from debating issues within groups, announcing actions, and planning for the future. Research in both left-wing and right-wing activist groups have found that activists prefer to communicate by email because it is widely available and offers the potential for higher levels of privacy, especially in comparison to carrying out these organizing tasks on social media sites [3]. Despite its primacy among activists, many remain concerned about the threat of government and corporate surveillance of email. At the time of our PGP email workshops (starting in 2014) from where we recruit participants, the simple plug-and-play E2EE apps that exist now were not available as potential alternatives to insecure email, and group messengers such as Slack were not yet in popular use. Even though simpler options were available at the time of the survey (in 2018), the groups supported by our collaborating non-profit were still using email for organizing.

2.3 Why PGP?

End-to-end encrypted email, in the form of PGP email, offers protection against this surveillance, and applications implementing PGP have been available for years. However, the seminal paper by Whitten and Tygar [61] and its replications, [17, 51, 56] have consistently found PGP email difficult to uptake for the average user. While originally theorized to be limitations of the user interface, other hypotheses have been examined as to why PGP is difficult to uptake such as: the complexity of key management [5, 17], the reliance on popular email platforms [4, 50], as well as how the system displays feedback to the user [5, 52]. As of our PGP email workshops, there were not any readily available solutions to these established problems.

Out of necessity to continue to use email, the CLDC promoted PGP email encryption for their supporting groups, given their own internal success with its use. While general-use PGP has been studied from a usable-security perspective as just highlighted, research on PGP email focused toward targeted groups such as social movements is lacking, with a few notable exceptions: Gaw et al. studied a single non-violent, direct-action organization ethnographically [18]; Lerner et al. sampled lawyers and journalists in order to evaluate a prototype PGP email client [25]; and, McGregor et al. investigated the success of security measures, including PGP, in the Panama Papers project [35]. We discuss how our work relates to these three papers in the Section 6.

3 Hypotheses

Our study seeks to understand the real communication choices of people operating in particular social circumstances and provides deeper insight into how individual and collective conditions jointly shape technology decisions. In this section, we discuss a mix of individual and collective conditions that are likely to affect technology decisions and which we study in this work. We examine their relationship to social movement participants in particular and hypothesize how these conditions would impact the adoption of PGP email encryption.

Ease of Adoption

Given the well-documented difficulty with learnability of PGP email encryption, we expect that an individual's **ease in adopting new technologies** and **technological confidence** should be the most important condition determining continued use. In their work on the role of technology among activists, Dencik and Cable [12] found that while individual group members were concerned about surveillance, they frequently chose to coordinate their activism on widely available and insecure social media platforms, reporting that their lack of technical ability meant reliance on widely available and user-friendly platforms that were known to be insecure. Activists' lack of access to resources (including technology and IT support) can also result in lower tech ease and confidence [19, 38, 54]. Given the documented gaps in technical skills and abilities among activists, *we expect that the ability to adopt the tool easily to be important for continuing to use encryption technologies.*

Personal Motivation

Beyond technical abilities, people vary significantly in their **personal motivation** to protect their communications from surveillance [12, 13]. Personal motivations matter a great deal in social movement contexts. Activists often work in groups, and the security practices of the collective are only as strong as the commitment of all individual members [13, 24]. *We expect that the presence of personal concern or fears about surveillance to be important for adopting and continuing to use encryption technologies.*

Group Motivation

Just as personal motivation varies across individuals, we should expect that some respondents will be more concerned about protecting their group's communication than their personal communications. Individuals who are cognizant of the communal benefits of encryption (offering protection from surveillance for whole communities)—that is, individuals with **group motivation**—are likely to find their social relationships and their role in their communities as salient motivations for pressing through difficulties with encryption technologies. Previous studies have revealed that a strong sense of group cohesion is critical for successfully implementing new technologies: when individuals care about security, the unwillingness or inability of other group members prevents them from incorporating secure practices in their group [13, 24]. Conversely, groups in which individual members lack a commitment to each other or that have unstable memberships struggle to change the ways their members communicate [3]. *We expect that*

the presence of group motivations to be important for adopting and continuing to use encryption technologies.

Secure Community

Secure technologies require more than an individual commitment. *We expect that individual users are more likely to adopt a technology when they have a* **community** *that also uses the technology.* For encrypted communication, the access to a community is partly due to the network effect [14]. For the network to stay private, all parties must also be using encryption correctly, thus the encrypted communication is only as strong as the weakest user. Research has also found that if the user knew many people were using a secure tool [2, 26], as well as whether or not there were even a minimal number of influential (e.g. spouse, family members) people using the tool, then this affected their decision to use the tool [26].

Additionally, social influence within a community affects a user's adoption of encrypted technology through those around them using or talking about the technology [27, 47], and in the case of secure technology specifically, through cautionary tales and advice from friends, family, and coworkers [10]. For people who lack technical confidence, belonging to a network of encryption-users provides a social resource for troubleshooting. Gaw et al. made similar observations in a non-violent, direct-action organization that used email encryption [18].

However, given the timing of our study, we expect that an individual belonging to a community that uses secure technologies will be correlated with not using PGP. While our PGP trainings started prior to the widespread release of Signal (in late 2015 [21]) and other secure messengers, our survey was deployed in early 2018, well after widespread adoption of secure messenging apps. *We expect that even if an individual starts using PGP, they may stop upon their community's adoption of another easier, secure communications technology.*

Risk

Many activists are aware of surveillance threats that might derail their planned actions, or increase the severity of the consequences, but the consequences of surveillance vary substantially. In interviews with activists, Dencik's respondents emphasized that their activism was oriented to the public, so the benefits of being transparent in their planning and communication served a reason to not take up encryption [12]. Given free-speech protections of most developed democracies (such as the US, where our research is based), activist groups engaged in low-risk activities are likely less worried about surveillance, and thus may be less motivated to protect their communications with each other. In contrast, higher-risk activism includes activities such as delegitimizing the state, direct-action interference and acts of civil disobedience that are more likely to end in arrest or serious sanctions. Such activism was subject to state suppressions during the COINTELPRO era [9], and still is today [11, 28–30, 40, 55]. The successful planning and carrying out of high-risk activism requires greater concealment, and it seems likely that individuals engaged in these activities would be more likely to make encryption a continuing part of their organizing strategy, as Gaw et al. observed in their study [18]. That is, at the outset of this work, *we expected that level of risk be positively correlated with continued use of encryption.* However, our analysis uncovers a contraindicative relationship.

In summary, we expect that ease in adopting new technologies or technological confidence, motivation (either individual or group), membership in a community that uses secure technologies, and risk level to have an impact on the adoption and continued use of encryption technologies. We seek to understand each condition separately, as well as how these conditions might combine to explain long-term use of PGP email encryption. We do so using Qualitative Comparative Analysis, as described in Section 4.3. We describe how we measure the above factors in Section 4.4.

4 Methodology

Prior to the development of our research questions, a subset of our research team had developed and deployed digital security workshops for a local non-profit that provides legal support to social movement groups. These workshops included both general workshops on surveillance risks and specific, hands-on workshops, including one for PGP email encryption in which the training team helped workshop participants get set up with PGP email encryption using Thunderbird with the Enigmail plugin (herein referred to as Thunderbird+Enigmail). Thunderbird+Enigmail was chosen by the training team because of its inter-operability, active development and robustness. The PGP encryption training works through a worksheet (available in the Appendix) with 20 steps,

with different worksheets for each of the main operating systems (Mac, Windows, Linux). The workshops ranged from one-on-one (often over phone or video call) to in-person workshops with as many as 8 participants to 1 trainer. Across all workshops over 100 participants used the appended worksheet and only one participant failed to send an encrypted email by the end of the workshop.

Our follow-up survey (available in the Appendix) evaluated whether PGP workshop attendees still encrypted their email, along with a variety of other conditions that may shape their decision to adopt encryption following a training session.

4.1 Recruitment

Workshop participants were recruited in the following ways: activists and social movement organizations requesting email encryption trainings through the CLDC; paid student workers or volunteers prepared to carry out drop-in center digital security trainings at a regional conference that activist groups attend; and, personal or professional acquaintances of the training team. None of the participants of the workshops were current users of PGP. All of the workshops took place before this follow-up research study was conceived.

In early 2018, we sent emails to participants of the PGP workshops for whom we had contact information to request their participation in our research survey (available in the Appendix). This was 6 to 40 months after participants were trained in Thunderbird+Enigmail. Of 71 invited individuals, a total of 26 respondents returned at least partial surveys, leaving us with a response rate of 37% (an acceptable response rate for email recruitment [22]). Of these, three were removed from the final analysis because their surveys were missing information used for key conditions or the outcome. Another four were dropped because they had been paid computer science student workers, recruited to teach others, required to complete the workshop *and* received more in-depth training on how to teach others to encrypt emails. These respondents are qualitatively different from other respondents who voluntarily sought encryption training.

Our final set of respondents includes 19 individuals, which is similar in size to previous PGP evaluations [17, 51, 56, 61]. We have assigned randomly chosen English words to each individual to refer to them throughout the remainder of the paper.

Nine participants identified as masculine, eight as feminine, and two as gender non-conforming or genderqueer. One participant identified as both Indian and white, while the rest of the participants were white. The participants' ages skewed young, with a majority falling between 20 and 39 (see Table 1). All participants were on the political left, ranging from center left to far left, as self-identified in the survey. We address the limitations resulting from this biased recruitment in Section 6.3.

Table 1. Participant Ages

Age	20-29	30-39	40-49	50-59	60-69	70+
N	3	11	1	1	1	2
%	16%	58%	5%	5%	5%	11%

4.2 Ethical Principles

Our research was approved by our Institutional Review Board under exempt category 2. The population we recruit from is one with unique risks, and we aimed to preserve their privacy as much as possible. The CLDC consults several smaller, independent social movement groups and organizations, and it is these independent groups from which we sampled. These groups are targeted by both law enforcement and groups with opposing ideology, and we take care to maintain trust and to avoid undue harm to these vulnerable groups participating in this research.

We created pseudonymous links to the Qualtrics survey; only the study staff held the mapping to real identities. The initial PGP email workshops avoided collecting attendance information from participants and any contact information was given completely voluntarily. This was done to minimize risk, as well as to assure the community that their confidentiality would be preserved. We borrow these practices from the field of sociology, where certain data collecting limitations are accepted in order to protect, and establish trust with, vulnerable communities.

We offered the recruitment sample a PGP refresher training one month after survey deployment.

4.3 Qualitative Comparative Analysis

In order to understand the pathways leading to (or away from) the adoption of PGP, we employ a Qualitative Comparative Analysis (QCA). Given the small sample

size and the exploratory nature of this work, a qualitative approach best utilizes our rare data, over say, a quantitative statistical analysis. This choice of analysis also reflects the interdisciplinary nature of our collaboration (between sociology and computer science) that aims to ultimately tease apart the group dynamics involved in adopting secure communications technology.

QCA was developed as a method to infer the configuration of causal[1] factors that lead to a given outcome and is generally used to analyze a smaller number of cases for which many details are known (for example, nation-states). While QCA is *not* a quantitative method, it brings standardized rigidity and reproducibility to qualitative analysis that helps organize patterns and correlations among themes. While our cases are a far cry from those of nation states, more recent work has successfully applied the method to individual respondents [6, 43, 60] and QCA has seen widespread use beyond political science [49]. Refer to Ragin's book *Redesigning Social Inquiry* for a thorough background of QCA methodology [42]. QCA best practices suggest that QCA is appropriate for our number of cases (19) and level of detail about each case [46]. QCA has been applied to datasets of similar size and level of detail, including studies of social movements [20, 32].

In the *crisp set* form of QCA, each case is described by a set of binary conditions and a binary outcome. (Our cases and their binary descriptions are given in Table 2 with each condition denoted by an all-caps name.) Crisp-set QCA uses Boolean minimization (via the Quine-McCluskey algorithm or equivalent [15]) to find a Boolean formula in disjunctive normal form of minimum size that infers the outcomes. The Boolean minimization acts over the complete truth table of condition combinations with each row having a corresponding (binary) outcome. Generally, different formulae are uncovered to infer the positive outcomes separately from the negative outcomes (as we will discuss further in Section 5.5). Each clause in a formula is referred to as a *causal pathway* in the QCA literature. While there are other forms of QCA, such as "Fuzzy-Set" which uses sliding scale values to organize outcomes, we employ the "Crisp-Set" (binary) method, which is more suitable to the size of our data set and the nature of our conditions, most of which were naturally binary or easily dichotomized, as we describe in Section 4.4.

However, the given cases may not cover all possible combinations of conditions, and may indeed only represent a fraction of the rows of the complete truth table (referred to as *limited diversity*). Further, multiple cases may have the same combination of conditions but have conflicting outcomes. QCA handles the configurations for which we have no cases (known as *remainders*) of conflicting cases in three basic ways, resulting in three types of QCA solutions [59]. We describe these in terms of inferring the positive outcome; symmetric processes and definitions hold for the negative outcome [46].

In the *conservative solution*, Boolean minimization is performed over the truth table composed of all the positive outcomes, and treats all the remainders as well as negative and conflicting outcomes as negative. The resulting Boolean formula evaluates to true *only* for the combinations of conditions for which all the cases have positive outcomes.

In the *parsimonious solution*, Boolean minimization is performed over the truth table composed of all the positive outcomes, treats all the negative and conflicting outcomes as negative, and treats all the remainders as *don't cares*. The resulting Boolean formula evaluates to true for the combinations of conditions for which all the cases have positive outcomes, evaluates to false for the combinations of conditions for negative or conflicting cases, and evaluates to true or false for the remainders.

An *intermediate solution* lies between the conservative and parsimonious solutions and is obtained by making hypotheses about the direction in which literals should influence the outcome [42].

For all three solutions, a conflicting outcome may be treated as either positive or negative via a threshold, for example as positive if at least 70% of the cases are positive. Further, one may relax how perfectly any given pathway infers positive outcomes, allowing a pathway to capture some small fraction of negative outcomes, a notion formalized by consistency.

Consistency

For a logical formula, *consistency* is the fraction of cases satisfying the logical formula that have positive outcomes. For example, of our 11 cases with the condition EASE=1 (see Table 2), 9 continue to use PGP (ENCR=1). Therefore, EASE $\Rightarrow$ ENCR has consistency $9/11 = 0.82$. Consistency scores of individual conditions (or their negations) for our data set are given in Table 3. QCA scholars use consistency scores of ≥ 0.8 as goals for analysis [42]. Indeed the pathways we uncover all achieve perfect consistency ($= 1.0$), and so we are

1 The literature around QCA anecdotally uses the term *causal*, while the true relationship is generally correlational.

Table 2. Truth Table: Cases and their conditions. Note that Confident and Kindred have the same set of conditions but have a conflicting outcome (in this case, $\text{ENCR}_{\text{Confident}} = 1$ and $\text{ENCR}_{\text{Kindred}} = 0$). Condition definitions are given in Section 4.4.

Conditions					Outcome	Cases	
EASE	MOT-I	MOT-G	COMMS	RISK	ENCR	#	pseudonyms
0	0	1	1	1	0	3	Cranial, Sitter, Passover
0	1	0	0	0	1, 0	2	Confident, Kindred
0	1	0	0	1	0	1	Afterlife
0	1	0	1	1	0	1	Gracious
0	1	1	1	0	0	1	Resent
1	0	1	0	0	1	1	Olive
1	0	1	0	1	0	1	Evacuee
1	0	1	1	0	1	1	Resale
1	0	1	1	1	0	1	Handmade
1	1	0	1	0	1	1	Democracy
1	1	0	1	1	1	3	Cargo, Drab, Problem
1	1	1	1	1	1	3	Sixtieth, Snowsuit, Vendetta

able to avoid relaxing the constraints for Boolean minimization described above.

Coverage

Coverage is of secondary importance to consistency. The coverage of a logical formula is the fraction of cases with positive outcome whose conditions satisfy the formula. For example (see Table 2), of the 10 cases who continue to use PGP (ENCR=1), 9 have the condition EASE=1. Therefore, EASE $\Rightarrow$ ENCR has coverage $9/10 = 0.9$. Coverage scores of individual conditions (or their negations) are given in Table 3. There are no thresholds for coverage established in the literature, but generally, the higher the value, the more relevant a logical formula is for explaining the occurrence of an outcome.

In this work, we use the *parsimonious solution*. In analyzing the parsimonious solution, we will discuss the remainders (configurations for which we have no cases) that are covered by the pathways of the resulting parsimonious solutions (Section 5.6). Given our limited cases, the pathways of even the intermediate solutions are either very similar to those of the parsimonious solution or have such low coverage as to only explain one or two cases, making the parsimonious solution more useful at this stage of research.

We use the software fsQCA 3.0 for the QCA-style Boolean minimization [41].

4.4 Measurement of the Conditions

We measure the conditions we hypothesize to be important for adopting PGP email encryption as binary variables reflecting the presence or absence of that condition. Our conditions are either dichotomous by nature or easily dichotomized via thresholding at a naturally occurring gap in a scaled response, according to the best practices of QCA methodology. The conditions were derived from responses on the survey and the in-depth knowledge the training team had of the survey participants. We define the conditions below and explain how we derive the measured conditions from the original responses on the survey and give examples of relevant qualitative responses. The measurements for our 19 cases are given in Table 2. The pseudonym for each case is a randomly selected word.

Continues to use PGP Email Encryption—ENCR

The outcome condition was a simple binary value indicating whether the respondent was still using a PGP email encryption system at the time of the follow-up survey. The outcome condition was coded as true if the respondent replied "yes" to at least one of the following two survey questions:

1. Do you continue to use Thunderbird+Enigmail?
2. Do you use an email encryption system other than Thunderbird+Enigmail?

For the two respondents who selected "no" for the first question and "yes" to the second, we confirmed that the email encryption system they referred to in question

2 was indeed a PGP email encryption system through their answer to the survey question "Which system, and why do you use it? Please list and discuss all systems you use and why." (In both cases, the respondents indicated they adopted "Mailvelope" sometime after the Thunderbird+Enigmail training.)

Technological Ease—EASE

In our survey, we included a subset of the validated System Usability Score (SUS) questions [7] for Thunderbird+Enigmail and computer self-efficacy questions [8]. We found little variation in the self-efficacy responses among our study participants, giving little discriminatory power for QCA. However, among the usability questions, we found sufficient variation to provide a useful condition for QCA. We used the responses on six questions about study participants' experience being trained on and using Thunderbird+Enigmail:

- I found Thunderbird+Enigmail unnecessarily complex.
- I thought Thunderbird+Enigmail was easy to use.
- I think that I would need the support of a technical person to be able to use Thunderbird+Enigmail.
- I found Thunderbird+Enigmail cumbersome to use.
- I felt confident using Thunderbird+Enigmail.
- I need to learn a lot of things before I could get going with Thunderbird+Enigmail.

Respondents were asked to indicate their level of agreement with these statements on a five point Likert scale with 1 being strongly disagree and 5 being strongly agree. All questions were coded or recoded so that a score of 5 indicated more technical confidence or ease of use with technology. Scores were then combined to give each respondent a raw score between 6 and 30. Eight cases fell at 18 or below; 11 fell at 20 or above. The score 19 offers a natural cut-off point between the lower group and the higher group: we code a participant with EASE=1 if they have a score of 20 or above.

Motivation for Learning Encryption—MOT-I & MOT-G

Respondents were asked the open ended question, "Why did you want to learn to use email encryption? What was your reason for the training?" We used responses to these to code whether respondents were motivated to participate in a PGP email workshop for personal (individual) or communal (group) reasons. Responses were inductively coded along themes that emerged in their responses [58], using true to represent the presence of the given type of motivation:

- *MOT-I:* Respondents with *individual motivation* present were those whose responses included references to their personal concern about surveillance from the state or from corporations or curiosity. For example: "I was curious about it and the instructors offered a free lesson while I was at work. Thought it might be useful in the future if I needed to feel secure that I was communicating confidentially." and "I wanted to understand the technology and know how to use it so that I would be able to."
- *MOT-G:* Respondents with *group motivation* present were those whose responses included references to planning direct-action activism, a desire to keep group communication secure, or the desire to provide cover to activists. For example: "To be able to institute the practice in my organizing collective." and "In case some direct action needed to use more secure email."

These categories were not mutually exclusive; respondents could be coded as having both conditions simultaneously. We expect that the presence of motivation (either group or individual) will be important for continued use of PGP email encryption.

Community Using Secure Technology—COMMS

Respondents were asked the yes/no question "Are you part of a community of people who use technologies for secure communication?" We coded the responses accordingly.

RISK

It would pose needless hazard to the human subjects of our research to collect as part of the survey their self-reported risks they face through their activism, and it may dissuade participants from completing their response. In order to evaluate the risk of the subjects' social movement activities, the training team member who conducted all of the PGP trainings assessed each participant for the risk they faced of arrest and/or other sanction. These assessments were based on the trainers' deep knowledge of each respondent's activism. We coded individuals as high risk (RISK=1) if their activities could result in measurable negative consequences given current US laws and practices (from loss of employment to fines or criminal charges). Remaining individuals were coded as low (or no) risk (RISK=0). While we hypoth-

esized that risk be positively correlated with continued use of encryption technologies, our QCA has borne out a contraindicative relationship, and so we include both positive and negative correlations in Table 3.

We describe above only those conditions for which we have hypotheses that were borne out in the data. We investigated other conditions (such as nature of and time since training, and demographics) using QCA and found no discernible pattern. We describe this further in Section 6.3. In our survey, we asked "Are you part of a community of people who use email encryption?" We were surprised that this condition did not present in pathways through QCA. It may be that respondents interpreted this question in different ways (temporally, for example). Or it may be that network and community affects highlighted by QCA were more usefully encoded by RISK or COMMS. However, the question did fill the role of *attention check* with everyone answering yes to this question also answering yes to "Are you part of a community of people who use technologies for secure communication?"

5 Results

Table 3. Consistency and coverage scores of conditions for which we have defensible hypotheses

	⇒ENCR			⇒ ¬ENCR	
	cons.	cov.		cons.	cov.
EASE	0.82	0.90	¬EASE	0.88	0.78
MOT-I	0.67	0.80	¬MOT-I	0.71	0.56
MOT-G	0.45	0.50	¬MOT-G	0.38	0.33
RISK	0.46	0.60	¬RISK	0.33	0.22
¬RISK	0.67	0.40	RISK	0.54	0.78
			COMMS	0.43	0.67

5.1 Coverage and Consistency of Conditions

In Table 3, we give the consistency and coverage of each hypothesized causal condition for each outcome of interest (ENCR=1 and ENCR=0), as calculated using the formulae outlined in Section 4.3. Note that we do not include COMMS or ¬COMMS as a condition for the positive outcome, as we do not have a hypothesis for this in the causal pathway for the positive outcome as earlier discussed. We include all directions of correlation for RISK, as the result has been counter to our initial hypothesis regarding RISK.

Only EASE and ¬EASE reach the 0.80 threshold for consistency for ENCR and ¬ENCR, respectively. In this light, we should expect that technical confidence is likely to be relevant within the causal pathways in the next set of analyses. Whatever other conditions play a role in continued encryption use, they are likely to build on existing technical confidence and ease in respondents. This makes sense given the technical requirements of PGP email encryption that require tasks not usually associated with email or other common programs.

Note that RISK is more consistent with ¬ENCR than ¬RISK, and, likewise, ¬RISK is more consistent with ENCR than RISK, giving the first indication that the correlation of RISK with ENCR is negative and seemingly contradictory, or at least certainly opposite to what security professionals would hope—that individuals at higher risk would take more precautionary steps.

5.2 Truth Table and Diversity of Cases

In Table 2, we present the binary conditions of our 19 cases, collapsed to common combinations of conditions. Only two cases with a common combination of conditions (participants Confident and Kindred) conflict in their outcome, with Confident continuing to use PGP and Kindred not.

The outcomes are quite balanced, with 10 individuals continuing to use PGP and 9 not. This makes our case set very suitable for QCA analysis. This is also a quite different outcome from PGP usability studies in which participants are rarely able to successfully encrypt a single email.

We note that while our cases only cover 12 of the 32 possible combinations of conditions, all but one of the remainders fall into (partially overlapping) groups with accompanying explanations:

– All 8 condition combinations corresponding to MOT-I=0 and MOT-G=0 are remainders. An individual with neither individual nor group motivation is very unlikely to participate in a training. We expect such individuals to be unlikely to adopt a complex tool such as PGP, but more accurately this combination (low motivation) of conditions is simply out of the scope of the present research.

- 6 of the 8 condition combinations corresponding to RISK=1, COMMS=0 are remainders. All the high-risk participants in this study would be aware of state and corporate surveillance as part of our training. With the prevalence of secure messengers by the time of the survey and our experience with supporting the digital security needs of direct-action activists, we believe that most high-risk activists adopt some sort of secure communications. Indeed, the two cases with RISK=1, COMMS=0 (participants Afterlife and Evacuee) are engaged in social change through their employment, whereas our other participants with RISK=1 are engaged in grassroots social change. Afterlife and Evacuee may not have control over the adoption of E2EE technologies in their employment.
- 11 of the 16 combinations with RISK=0 are remainders. Many of our PGP workshop attendees seek out training through or are recommended for training by our collaborating non-profit that provides legal support for front-line activists. This non-profit is more likely to recommend digital security training such as our PGP workshop to activists who are in groups who have required legal support, indicating higher risk, in order to protect legal communications.

The remainder that doesn't fall into these groups is: EASE=0, MOT-I=1, MOT-G=1, COMMS=1, RISK=1.

5.3 QCA for the Positive Outcome

The parsimonious solution for the positive outcome (ENCR=1) uncovers the following logical formula:

$$(\text{EASE} \wedge \text{MOT-I}) \vee (\text{EASE} \wedge \neg\text{RISK}) \Rightarrow \text{ENCR} \quad (1)$$

This logical formula has perfect consistency (all the cases which satisfy the antecedent have ENCR=1) and coverage 0.9 (of the 10 cases with ENCR=1, 9 satisfy the antecedent of Formula (1)). The logical formula only fails to cover the case of participant Confident who continues to use PGP; however, Confident conflicts with participant Kindred—therefore, it is impossible to uncover a formula which achieves both perfect consistency and perfect coverage.

Formula (1) is equivalent to:

$$\text{EASE} \wedge (\text{MOT-I} \vee \neg\text{RISK}) \Rightarrow \text{ENCR} \quad (2)$$

which highlights that while technical ease (EASE) is necessary for both causal pathways, it is not sufficient, and that it needs to be combined with either individual motivation (MOT-I) or low risk (¬RISK).

The first causal pathway, EASE ∧ MOT-I, requiring that technical ease be combined with personal motivation, is consistent with both the literature and our expectations that most people who take up higher-level security measures need to have at least some technical confidence, and need to be fairly concerned about the risks of surveillance for their personal information. It is also likely that many of those with higher-level technical skills and confidence are more aware of surveillance risk, even when compared with other respondents who also sought out encryption training. This causal pathway achieves coverage 0.7.

The second causal pathway (EASE∧¬RISK) covers the cases of participants Olive, Resale, and Democracy (coverage 0.3), with Democracy also satisfying the first causal pathway. In an intermediate solution, this pathway also includes MOT-G; in fact, MOT-G ∧ ¬RISK only implies ENCR when the individuals also had technical ease. This occurs in two cases (Olive and Resale), both emerging from a single informal group of retired friends who sought training together. Of the three members of the low-risk group that sought training, only two continued to use PGP. A third member (Resent) also reported MOT-G but not EASE, and this member was the only one to discontinue using PGP. This underscores the importance of technical comfort as an issue that must be dealt with among those advocates seeking to increase the use of encryption.

This second pathway provides useful insight for the surprising role of risk in predicting individual behavior. We revisit this in Section 6.2.

5.4 QCA for the Negative Outcome

QCA does not assume symmetry when predicting an outcome versus predicting its absence: we separately assess combinations of conditions leading to discontinued use of PGP encryption. This also provides a check on the relevance of the conditions in the causal pathways to the continued use of encryption. As we noted above, we can be more confident that the causal paths we have discovered are meaningful if we can also demonstrate that their absence is important when explaining the outcome's absence.

The parsimonious solution for the negative outcome (ENCR=0) uncovers the following logical formula:

$$(\neg\text{EASE} \wedge \text{COMMS}) \vee (\neg\text{EASE} \wedge \text{RISK}) \vee(\neg\text{MOT-I} \wedge \text{RISK}) \Rightarrow \neg\text{ENCR} \quad (3)$$

This logical formula has perfect consistency (all the cases which satisfy the antecedent have ENCR=0) and coverage 0.89 (of the 9 cases with ENCR=0, 8 satisfy the antecedent of Formula (1)). The logical formula only fails to cover the case of participant Kindred who discontinues PGP use. However, Kindred conflicts with participant Confident. Therefore, as with the pathway for the positive outcome, it is impossible to uncover a formula which achieves both perfect consistency and perfect coverage.

We can immediately observe that the factors that lead to the adoption of PGP play a role in the discontinued use of PGP in their negated form, confirming the relevance of the conditions EASE, RISK and MOT-I.

Each clause in formula (3) achieve a coverage of 0.56 with 5 of the 9 cases satisfying each clause. As a result these pathways have a high degree of overlap. Participants Passover, Cranial and Sitter satisfy all three pathways; participant Gracious satisfies the first two pathways.

Formula (3) highlights the importance that a lack of technical ease (EASE=0) and a higher-risk persona (RISK=1) have to discontinued use of PGP email encryption. Given that EASE is pivotal to continued use of PGP (ENCR=1), it is natural that a lack of technical ease is important to discontinued use of or failure to adopt PGP. That RISK helps to explain 6 cases (pathways 2 and 3), we have additional proof that it is risk aversion that drives a continued commitment to encryption, rather than a sense that respondents have an objective risk level that requires greater security.

In the third pathway for the negated outcome, a lack of individual motivation is combined with risk ($\neg$MOT-I $\wedge$ RISK). This makes some theoretical sense, given that those who are the least worried about security in their communications are likely to be those who are willing to take some larger risks in their activism.

The first pathway for failing to adopt PGP email encryption uncovers the role played by having a community who use secure communications technology. Notably, if an individual both belongs to a community using a E2EE communications tool such as Signal *and* they do not have technological ease, they fail to adopt PGP email encryption. This confirms our hypothesis regarding COMMS along with a natural combination with $\neg$EASE.

We asked our respondents: "If you no longer use Thunderbird+Enigmail, why?" Two individuals cited technical problems (both with EASE=0): participant Cranial switched to a new computer and failed to set PGP up again and participant Passover forgot "how to do the key thing with other users." Participant Evacuee wanted cross-compatibility with their smartphone. Six individuals referred to leaving the GMail interface as being the main barrier (including the two users who switched to Mailvelope to access PGP): "Hooked on the convenience of non-encrypted Gmail." (participant Resent). Three individuals cited a lack of need. Participant Sitter noted "I have found something that is easy to replace email [with] is signal." Only one respondent (Handmade) echoed the fatalist opinion found widespread among leftist groups post Snowden [13], saying "The vast majority of my emails are not activist related and my online, financial, and public behavior, if a law enforcement agency wanted them, would be public."

5.5 Asymmetric Pathways

As you can see from Formulae (1) and (3), QCA returns asymmetric pathways to explain positive and negative outcomes. This is natural as positive outcomes generally have simpler explanations than negative outcomes: there are often many more ways and reasons to stop doing something than to continue. The pairs of positive and negative pathways, interesting in their own right, also lend extra credibility to those conditions that appear in both pathways. Indeed those conditions appearing in both pathways (EASE, RISK, MOT-I) occur negated in the opposite pathway.

5.6 Covered Remainders

In Figure 1, we illustrate Formulae (1) and (3) in the Venn diagram of the case space. Since MOT-G did not appear in the pathways of the parsimonious solutions, we omit MOT-G from this illustration. This highlights those combinations of conditions for which our parsimonious solutions are making predictions, for example EASE=1, MOT-I=1, COMMS=0, RISK=0 (in the bottom right). These are potentially interesting cases that we haven't observed, and indeed, as discussed in Section 5.2, may not be possible to sample.

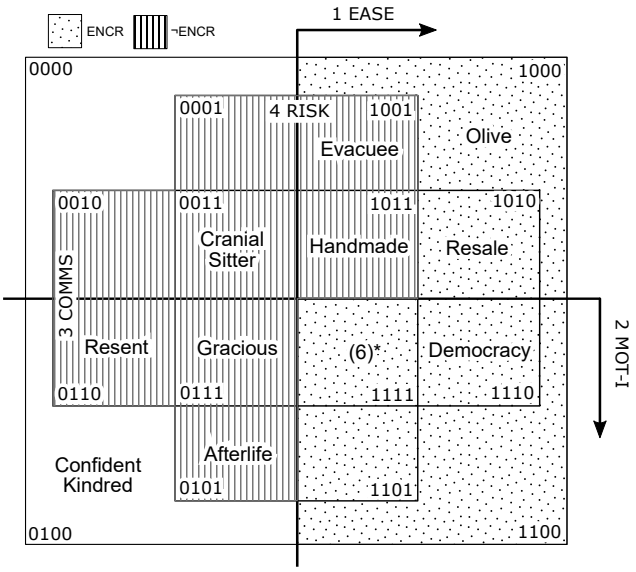

Fig. 1. A Venn diagram of the condition space over the conditions: EASE, MOT-I, COMMS and RISK. The combinations of conditions captured by the parsimonious solution for ENCR (Formula (1)) is given by the dotted area while the striped areas are the combinations of conditions captured by the parsimonious solution for ¬ENCR (Formula (3)). (6)* refers to the six participants: Cargo, Drab, Problem, Sixtieth, Snow, and Vendetta.

6 Discussion & Related Work

The literature on PGP email encryption use has consistently found that it has poor learnability in laboratory settings. We test these findings with individuals in their natural social context, assessing how this context might make encryption use more likely. Indeed, we find that the rate of long-term PGP use by our respondents is over 50%, seeming to counter the poor learnability uncovered by laboratory studies. Indeed, in our original PGP email workshops, all but one participant were able to successfully send and receive PGP-encrypted emails.

Renaud, Volkamer, and Renkema-Padmos identify a sequence of seven steps that users must overcome in order to uptake E2EE from understanding through ability and deployment [45]. Our respondents who did not engage in long-term PGP use (and surveyed months after the workshop) are still making it through to step five ("Knows E2EE Helps") or six ("Able to Use E2EE") based on the survey responses, but are not making it to the seventh and final step "Is Not Side-Tracked": They are able to successfully use PGP email at least once, but still fail to adopt in the long-term for another reason.

While our research is unique in trying to understand the social factors that lead to success in that last step, there are two earlier papers with which our work dovetails.

Gaw, Felton, and Fernandez-Kelly performed an ethnographic study of a non-violent, direct-action social movement organization ("ActivistCorp") that used PGP email [18]. While they find that members of ActivistCorp manage to adopt PGP, it is not without complaint. Counter to the respondents of our survey, ActivistCorp uses internal authority in order to enforce and support the use of PGP by the individuals of the organization. Despite this, there was variance in the degree to which ActivistCorp members used PGP for internal emails, from encrypting all emails to only encrypting sensitive emails. Gaw et al. found that this variance was explained by both technical and social factors, from annoyance (as there was technical overhead to managing the encrypted emails) to views on secrecy (such as over-encryption indicating paranoia). There are similarities between the factors that Gaw et al. describe and our factors of EASE and MOT-I. Although we only determine whether or not our respondents are continuing to use PGP (and not the degree to which they are using PGP), we can draw a comparison between ActivistCorp members who use PGP more (and whose comments indicate a higher level of individual motivation and ease of use with the technology) and our respondents who continue to use PGP (and have EASE = 1 and/or MOT-I = 1).

McGregor, Watkins, Al-Ameen, Caine, and Roesner investigated the success of security measures in the Panama Papers project [35]. Despite collaboration of 354 journalists working remotely across the globe on the same project, the project avoided breaches using tools such as two-factor authentication and PGP email. This is largely accredited to the resources of the organization and the strong security culture instilled on the collaborators. The project-specific tools are also to credit as they employed user-centered and security-by-design, providing features valued by the collaborators [37]. While the resources of the Panama Papers collaboration far exceeds those of the groups our respondents represent, we may be able to infer that the instillation of security culture gave collaborators individual motivation (MOT-I = 1) and that the tailoring of the tools to the users increased the ease of their use (EASE = 1).

6.1 Group vs. Individual Factors

Gaw et al. and McGregor et al.'s work each focus on a single organization, and so cannot comment on group factors that may come into play, as we begin to with

this research since our respondents hail from different organizing groups. While MOT-G did not play a role in the causal pathways, other group factors did (RISK and COMMS). RISK is determined by potential consequences of a group's actions and COMMS measures a group's commitment to digital security if they use secure communications for organizing work. COMMS and RISK may more reliably measure group-based motivation than our coding of responses to the open-ended questions "Why did you want to learn to use email encryption? What was your reason for the training?" that was used to encode MOT-G.

However, individual level factors seem to matter most for people when choosing to continue with encryption. While the role of EASE (which we measure using a subset of the standard usability questions) has been studied before, the interplay of this condition with others has not. Level of confidence with the technology (EASE) carried the most weight. Beyond ease with the technology, there were two pathways that lead to continued encryption use, one based only on individual level factors, and one which includes group factors. At the individual level, respondents needed to feel personally concerned about surveillance. The second pathway encompassed respondents who belonged to low-risk movement groups, yet their commitments to each other seemed to offer a boost to their individual commitments to using encryption. These group commitments did not matter for all members equally, however. Lacking technical confidence seems to cancel out the commitment to group protection.

Existing research indicates that if the functionality of the secure software inhibits or slows down the users' ability to perform essential tasks, users will either elect not to use it [2, 29, 33], or if users are required to use secure software (such as through an organizational requirement) users will attempt to work around it [29, 34]. To further support this, in the project reviewing the success of the release of the Panama Papers, McGregor et al. note how users were able to accept security requirements when their general technology needs were addressed by the secure system they were using [35].

6.2 The Unfortunate Role of Risk

It has previously been established that many individuals partake in a privacy paradox: they often have stronger beliefs about privacy behaviors and ideals than their actions would indicate [36]. However, the phenomenon may not be so paradoxical. A users' privacy concerns may be at odds with their access to, knowledge of, or ability to perform counter measures [23]. Renaud et al. establish a sliding scale of interpretations for the privacy paradox that consist of different combinations of level of understanding, access to technology, and ability to perform protective actions [45]. Abu-Salma et al. highlight the more nuanced obstacles to adoption of secure communication tools, namely that users have knowledge gaps when making decisions about how to protect their communication, and make flawed threat models based on these flawed mental models [2].

In this work we find a risk paradox—that risk does not play the role that most security professionals would likely hope: that individuals undertaking riskier activities would be more likely to adopt a higher security profile by adopting PGP email encryption. Rather, we find the latter, with risk negatively impacting adoption of PGP. This may be because higher-risk activists were already accustomed to planning riskier actions only in face-to-face meetings, and thus felt no need to incorporate secure communication. It is also possible that in contrast to the risk-averse respondents, respondents who engage in riskier activism may simply have a higher tolerance for risk in their communication. One respondent reported their sense that even "militant" civil disobedience did not require secure email, and that much of their personal information would be available online to state authorities anyway. From this perspective, activists may consider increased email security an unnecessary step. Regardless, the relationship of risk-taking to security practices would be interesting to investigate through a more generalizable study.

6.3 Limitations

Our study is retrospective. The workshops in which participants learned to use PGP email encryption had taken place before this study was designed. A number of the limitations stem from the difficulty in studying use of secure communications technology in the wild, particularly in a particular population (social movement participants) using a relatively rare technology (PGP email). This study, though, was made possible through our partnering with the CLDC. This results in a number of limitations:

Workshop Variation

As we noted, there is a fair amount of variation in the workshops. However, a number of factors were con-

trolled: the same trainer (a member of the research team) hosted every workshop, Thunderbird+Enigmail was consistently used as the platform, and all trainings followed the same worksheet (see Appendix). Despite this, there was still unavoidable variations: trainer-to-participant ratios ranged from 1:1 to 1:8, workshops could occur as a drop-in center or a fixed-time workshops, and sometimes were conducted over phone or video.

Time Since Workshop

We investigated whether time was a factor in measuring continued use of PGP email encryption. There are two hypotheses for how this time interval could be a confounding factor. First, the longer the time between a workshop and follow-up, the more opportunities there are to stop using PGP email encryption. In contrast, the more time passes, the less likely someone may be to respond to a recruitment email, and this may be further confounded by the response biases we describe next. We investigated time as a factor that could affect our respondents' outcomes and found that time since training did not affect the outcome.

Response Bias

While all studies that recruit human subjects are vulnerable to response bias, we reflect here on those aspects particular to our study. A workshop participant who continues to use PGP email encryption may be more likely to respond to our survey as they may have more interest in the study. Conversely, a workshop participant who does not continue to use PGP email encryption may be embarrassed by this fact and be less likely to respond to the survey. Participants from two workshops were inaccessible to us due to the way in which the workshop was convened, without the trainer or partnering nonprofit having a list of workshop attendees. These workshop participants were from tightly-knit, highly-private groups that engaged in higher-risk activism. In these cases, we did attempt to recruit through the workshop convener, but did not receive any responses this way. As such, we may have lower response rates from higher -risk workshop participants. This bias is in the opposite direction of that among recruitment for training (as we comment on in Section 5.2), where higher-risk activists are more likely to be recommended for digital security training.

Left Bias

The participants all identify with being on the political left. This bias is a result of partnering with the CLDC which supports mostly environmental and social justice groups, which tend to engage left-leaning individuals. However, the work of Agarwal et al. [3], which studied the values and technology choices of both left- and right-wing social movements found that security and privacy concerns were similar on both ends of the spectrum. This may mitigate the concerns of the political bias of our participants.

Demographic Bias

We acknowledge that our participants' demographics are skewed young and white; this reflects the demographics of the population from which we recruit in Oregon, which is approximately 85% white.

7 Conclusion & Recommendations

Work exploring how motivated users in communities impacted most by surveillance interact with new or novel secure technologies and evaluating usability is useful, such as in the work of Lerner, Zeng, and Roesner [25]. Lerner et al. sampled lawyers and journalists in order to evaluate the development of Confidante, a prototype PGP email client using Keybase.io's key management to address key exchange issues. However, Confidante is still restricted to use in a lab setting, and the project is still in beta with no planned release as of this writing, restricting its accessibility for users with immediate needs. Gaw et al.'s study of ActivistCorp looked at how an at-risk organization adopted existing (and difficult-to-use) technology. While their contributions cannot be understated, significant exposures about surveillance have come to light since their 2006 paper, as well as significant technological progress, which may limit its continued relevance. Our work follows in the footsteps of Gaw et al., seeking to understand how at-risk communities interact with and adopt (or do not adopt) existing technologies, as the motivation to counter surveillance may be enough for users to overcome some of the lesser usability problems found within the existing software.

7.1 Recommendations for Future Research

The variations and biases inherent in our study (Section 6.3) are a consequence of the nature of retrospective research and the difficulty in recruiting from at-risk groups, and as such our research should be viewed as exploratory. While the variation may be a confounding factor, at the same time, it mimics what happens in the real world: people are trained to use technologies in different settings according to their needs and may adopt technologies for different periods of time. In the end, this is exploratory work, but provides a richer base of information vis-à-vis lab studies.

Existing controlled lab studies that evaluate PGP have unveiled important usability issues with PGP and have provided a framework for future improvements in the design of secure communication. However, the highly controlled nature of these studies neglects to address the use of PGP in the hands of users with a threat model lending itself to motivation to adopt secure communication in the moment. Here we have found a higher adoption rate and long-term use of PGP than one would expect from the Johnny Can't Encrypt papers, which focus on the impact of usability on learnability. While the learnability challenges of these tools cannot be discounted, we have found that motivated users are able to overcome usability issues in existing software.

Until applications follow the practices of success stories such as the Panama Papers collaboration, and are made more appropriate for all user groups, we must figure out how to support users with tools that are readily available. Researchers should take greater efforts to understand tools over long periods of time, in the field, to understand usability from more than the angle of learnability. Such work can complement rigorous, controlled lab studies of convenience samples in order to form a holistic picture of the use of these secure communication technologies.

The timing of our research was during a time in which newer, easier E2EE communications technologies (namely, secure messengers) were becoming available and popular [21]. These applications fare better than PGP in terms of network effect, and in fact this is a bigger influence in adoption than privacy or security [2, 26]. While the factors we uncover as having an impact on adoption or non-adoption of PGP (EASE, RISK, MOT-I, COMMS) are not specific to PGP and would likely play a role with other technologies, we expect that EASE may play less of a role with an easier technology. The reduction in importance of EASE may have non-trivial impacts on the importance of RISK, MOT-I, and COMMS or on other factors. Replicating this or a similar study with other technologies would shed further light. This would complement the ongoing work of understanding the security needs of particular groups, such as Elliott and Brody's study of surveillance concerns of African-American New Yorkers [16], Sierra's survey of Mexican journalists and bloggers [57], Samarin et al.'s survey of civil society organizations [53], as well as Citizen Lab's continued work understanding the threats faced by civil society organizations.

7.2 Recommendations for Trainers

Whether these factors play precisely the same role for other technologies, we believe they will still have an impact on adoption. Therefore, we recommend that trainers should take into account the attributes of trainees (e.g. risk, comfort with technology, motivation) in tailoring their training to make sure trainees are adequately supported to maximize tool adoption. While PGP email does pose unique technical challenges for users [31], in addition to helping users work past the technical facets, trainers should prioritize motivating trainees about the importance of secure communication, and supporting those who are less confident in their technological skills. It is worth noting here that one's perception of their own skills can be more influential than their actual ability or experience with technology. As such, these users have the required ability but need to be reassured by trainers. Indeed, we should not ask users who require the functionality of tools with poor usability to wait on design improvements that may not come to fruition in time to benefit those users. Our study population has shown that PGP was a viable option before Signal became available and widely adopted by activist communities.

Counter to models of security practices and teachings, risk may be negatively associated with secure communication adoption for this population. This could be because those that participate in real-world activities that are high risk simply have a higher tolerance for risk, and therefore are comfortable with taking more risks with their communication as well. This warrants further study: can this tendency be overcome? Formulae (1) and (3) indicate directions for investigation: for example, can trainings reduce the technical barrier sufficiently and increase individual motivation?

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1915768. We thank our partnership with the Civil Liberties Defense Center.

References

[1] R. Abu-Salma, E. M. Redmiles, B. Ur, and M. Wei. Exploring User Mental Models of End-to-End Encrypted Communication Tools. In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*, 2018.

[2] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153, San Jose, CA, USA, May 2017. IEEE.

[3] S. D. Agarwal, M. L. Barthel, C. Rost, A. Borning, W. L. Bennett, and C. N. Johnson. Grassroots organizing in the digital age: considering values and technology in Tea Party and Occupy Wall Street. *Information, Communication & Society*, 17(3):326–341, 2014.

[4] E. Atwater, C. Bocovich, U. Hengartner, E. Lank, and I. Goldberg. Leading Johnny to Water: Designing for Usability and Trust. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, pages 69–88, 2015.

[5] W. Bai, D. Kim, M. Namara, Y. Qian, P. G. Kelley, and M. L. Mazurek. An Inconvenient Trust: User Attitudes Toward Security and Usability Tradeoffs for Key-Directory Encryption Systems. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, pages 113–130, Denver, CO, 2016.

[6] C. Borgna. Multiple paths to inequality. How institutional contexts shape the educational opportunities of second-generation immigrants in Europe. *European Societies*, 18(2):180–199, Mar. 2016.

[7] J. Brooke. SUS: A 'quick and dirty' Usability Scale. In *Usability Evaluation in Industry*, pages 189–194. Taylor and Francis London, 1996.

[8] D. R. Compeau and C. A. Higgins. Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly*, 19(2):189–211, June 1995.

[9] D. Cunningham. *There's Something Happening Here: The New Left, the Klan, and FBI Counterintelligence*. University of California Press, 1st edition, 2004.

[10] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong. The Effect of Social Influence on Security Sensitivity. *In 10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 143–157, 2014.

[11] R. Deibert. *Communities @ Risk: Targeted Digital Threats Against Civil Society*. U of T Policy Reports. University of Toronto, 2014.

[12] L. Dencik and J. Cable. The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*, 11:763–781, 2017.

[13] L. Dencik, A. Hintz, and J. Cable. Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, 3(2):205395171667967, Dec. 2016.

[14] R. Dingledine and N. Mathewson. Anonymity Loves Company: Usability and the Network Effect. *WEIS*, page 12, 2006.

[15] A. Dusa. *QCA with R: A Comprehensive Resource*. Springer International Publishing, 2019.

[16] A. Elliott and S. Brody. Design Implications of Lived Surveillance in New York. *ACM Conference on Human Factors in Computing Systems (CHI)*, 2016.

[17] S. L. Garfinkel and R. C. Miller. Johnny 2: a user test of key continuity management with S/MIME and Outlook Express. In *Proceedings of the 2005 symposium on Usable privacy and security - SOUPS '05*, pages 13–24, Pittsburgh, Pennsylvania, 2005. ACM Press.

[18] S. Gaw, E. W. Felten, and P. Fernandez-Kelly. Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 591–600. ACM, 2006.

[19] J. J. George and D. E. Leidner. From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, 29(3):100249, Sept. 2019.

[20] M. Giugni and A. Nai. Paths towards Consensus: Explaining Decision Making within the Swiss Global Justice Movement. *Swiss Political Science Review*, 19(1):26–40, Mar. 2013.

[21] A. Greenberg. Signal, the Snowden-Approved Crypto App, Comes to Android. *Wired*, Nov. 2015.

[22] A. Keller. What is an acceptable survey response rate?, Nov. 2014.

[23] S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64:122–134, Jan. 2017.

[24] O. Leistert. Resistance against Cyber-Surveillance within Social Movements and how Surveillance Adapts. *Surveillance & Society*, 9(4):441–456, June 2012.

[25] A. Lerner, E. Zeng, and F. Roesner. Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists. In *IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 385–400. IEEE, Apr. 2017.

[26] A. D. Luca, S. Das, M. Ortlieb, I. Ion, and B. Laurie. Expert and Non-Expert Attitudes towards (Secure) Instant Messaging. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 147–157, Denver, CO, June 2016. USENIX Association.

[27] Y. Malhotra and D. Galletta. Extending the technology acceptance model to account for social influence: theoretical bases and empirical validation. In *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers*, page 14, Maui, HI, USA, 1999. IEEE Comput. Soc.

[28] B. Marczak, J. Scott-Railton, and S. McKune. Hacking Team Reloaded, Mar. 2015. Library Catalog: citizenlab.ca.

[29] W. R. Marczak and V. Paxson. Social Engineering Attacks on Government Opponents: Target Perspectives. *Proceedings on Privacy Enhancing Technologies*, 2017(2):172–185, Apr. 2017.

[30] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson. When Governments Hack Opponents: A Look at Actors and Technology. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 511–525, San Diego, CA,

2014. USENIX Association.

[31] J. R. P. Mauriés, K. Krol, S. Parkin, R. Abu-Salma, and M. A. Sasse. Dead on Arrival: Recovering from Fatal Flaws in Email Encryption Tools. In *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2017)*, pages 49–57, 2017.

[32] D. McAdam, H. S. Boudet, J. Davis, R. J. Orr, W. Richard Scott, and R. E. Levitt. "Site Fights": Explaining Opposition to Pipeline Projects in the Developing World1: Opposition to Pipeline Projects in the Developing World. *Sociological Forum*, 25(3):401–427, Aug. 2010.

[33] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner. Investigating the Computer Security Practices and Needs of Journalists. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 399–414, Washington, D.C., Aug. 2015. USENIX Association.

[34] S. E. McGregor, F. Roesner, and K. Caine. Individual versus Organizational Computer Security and Privacy Concerns in Journalism. *Proceedings on Privacy Enhancing Technologies*, 2016(4):418–435, Oct. 2016.

[35] S. E. McGregor, E. A. Watkins, M. N. Al-Ameen, K. Caine, and F. Roesner. When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers. In *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017.*, pages 505–522, 2017.

[36] P. A. Norberg, D. R. Horne, and D. A. Horne. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41(1):100–126, June 2007.

[37] D. A. Norman and S. W. Draper, editors. *User centered system design: new perspectives on human-computer interaction*. L. Erlbaum Associates, Hillsdale, N.J, 1986.

[38] J. Ortiz, A. Young, M. D. Myers, R. T. Bedeley, and D. Carbaugh. Giving Voice to the Voiceless: The Use of Digital Technologies by Marginalized Groups. *Communications of the Association for Information Systems*, 45:21, 2019.

[39] J. W. Penney. Chilling Effects: Online Surveillance and Wikipedia Use. 2016. Publisher: btlj.

[40] W. Potter. *Green is the new red: an insiders account of a social movement under siege*. City Lights Books, San Francisco, 2011.

[41] C. Ragin and S. Davey. Fuzzy-Set/Qualitative Comparative Analysis, 2016.

[42] C. C. Ragin. *Redesigning Social Inquiry: Fuzzy Sets and Beyond*. University of Chicago Press, Chicago, 47116th edition edition, Oct. 2008.

[43] C. C. Ragin and P. C. Fiss. *Intersectional Inequality: Race, Class, Test Scores, and Poverty*. University of Chicago Press, Dec. 2016. Google-Books-ID: Q3SpDQAAQBAJ.

[44] E. M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens, and M. L. Mazurek. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pages 89–108, 2020.

[45] K. Renaud, M. Volkamer, and A. Renkema-Padmos. Why Doesn't Jane Protect Her Privacy? In E. De Cristofaro and S. J. Murdoch, editors, *Privacy Enhancing Technologies*, volume 8555, pages 244–262. Springer International Publishing, Cham, 2014. Series Title: Lecture Notes in Computer Science.

[46] B. Rihoux and C. Ragin. *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*. SAGE Publications, Inc., 2455 Teller Road, Thousand Oaks California 91320 United States, 2009.

[47] M. Rogers and G. Eden. Digital Citizenship and Surveillance| The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures. *International Journal of Communication*, 11:22, 2017.

[48] D. A. Rohlinger and J. Klein. From Fervor to Fear: ICT and Emotions in the Tea Party Movement. In N. Van Dyke and D. S. Meyer, editors, *Understanding the Tea Party Movement*, pages 125–148. Routledge, New York, 2016.

[49] N. Roig-Tierno, T. F. Gonzalez-Cruz, and J. Llopis-Martinez. An overview of qualitative comparative analysis: A bibliometric analysis. *Journal of Innovation & Knowledge*, 2(1):15–23, Jan. 2017.

[50] S. Ruoti, J. Andersen, S. Heidbrink, M. O'Neill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons. "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*, pages 4298–4308. ACM Press, 2016.

[51] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons. Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client. *arXiv preprint arXiv:1510.08555*, 2015.

[52] S. Ruoti, N. Kim, B. Burgon, T. Van Der Horst, and K. Seamons. Confused Johnny: when automatic encryption leads to confusion and mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 5. ACM, 2013.

[53] N. Samarin, C. Cheshire, A. Frik, S. Egelman, and S. Brooks. Cybersecurity for High-Risk Users: Case Study of Civil Society Organizations. In *Conference on Human Factors in Computing Systems*, page 6, 2020.

[54] J. Schradie. The Digital Activism Gap: How Class and Costs Shape Online Collective Action. *Social Problems*, 65(1):51–74, Feb. 2018.

[55] J. Scott-Railton. Security for the High-Risk User: Separate and Unequal. *IEEE Security & Privacy*, 14(2):79–87, Mar. 2016.

[56] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security (SOUPS)*, pages 3–4, 2006.

[57] J. L. Sierra. *Digital and Mobile Security for Mexican Journalists and Bloggers*. Freedom House, 2013.

[58] A. Strauss and J. Corbin. *Grounded Theory in Practice*. SAGE Publications, 1997.

[59] A. Thiem and A. Dușa. Boolean Minimization in Social Science Research: A Review of Current Software for Qualitative Comparative Analysis (QCA). *Social Science Computer Review*, Mar. 2013.

[60] J. Warren, J. Wistow, and C. Bambra. Applying qualitative comparative analysis (QCA) in public health: a case study of a health improvement service for long-term incapacity benefit recipients. *Journal of Public Health*, 36(1):126–133, 2013.

[61] A. Whitten and J. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *8th USENIX Security Symposium*, 1999.

A Survey Instrument

1. Why did you want to learn to use email encryption? What was your reason for the training? (text box)
2. Are you part of a community of people who use technologies for secure communication? (yes/no)
3. Are you part of a community of people who use email encryption? (yes/no)
4. If the answer is yes to either of the previous two questions, describe how decisions are made in this community? Please describe the decision-making process in any of the communities or groups that you belong to that use email encryption or technologies for secure communications, more generally. (text box)
5. Please rate your experience in using Thunderbird+Enigmail for email encryption (5-point Likert from strongly disagree to strongly agree):
   (a) I remember the basics of what Thunderbird+Enigmail is.
   (b) I think that I would like to use Thunderbird+Enigmail frequently.
   (c) I found Thunderbird+Enigmail unnecessarily complex.
   (d) I thought Thunderbird+Enigmail was easy to use.
   (e) I think that I would need the support of a technical person to be able to use Thunderbird+Enigmail.
   (f) I found the various aspects of Thunderbird+Enigmail were well integrated.
   (g) I thought there was too much inconsistency in Thunderbird+Enigmail.
   (h) I would imagine that most people would learn to use Thunderbird+Enigmail very quickly.
   (i) I found Thunderbird+Enigmail cumbersome to use.
   (j) I felt confident using Thunderbird+Enigmail.
   (k) I needed to learn a lot of things before I could get going with Thunderbird+Enigmail.
6. Do you continue to use Thunderbird+Enigmail? (yes/no)

   Please answer questions 7 through 9 with respect to the Thunderbird+Enigmail system:
7. **After** the training, have you done any of the following tasks? For each, select all of the following responses that apply:
   – I have done this.
   – I have not done this.
   – I can't recall if I have done this.
   – I don't know what this means.
   (a) sent someone your public key
   (b) received a public key from someone
   (c) retrieved someone's public key from a keyserver
   (d) downloaded someone's public key from a website
   (e) verified the fingerprint of someone's public key
   (f) verified your public key fingerprint with someone else
   (g) received an encrypted or signed message with an attachment
   (h) sent an encrypted or signed message with an attachment
   (i) sent an encrypted message to multiple people at the same time
   (j) backed up your private key
   (k) created a new public/private key pair
   (l) mistakenly sent an unencrypted email that you intended to be encrypted
   (m) tried to send an encrypted message but were unable to
   (n) sent an encrypted message that the recipient was unable to read
   (o) received a public key that you were not able to use/import
   (p) received a message that you couldn't decrypt
   (q) received a message with an encrypted attachment that you couldn't decrypt
   (r) forgot your passphrase
   (s) asked someone for help with email encryption
   (t) helped someone else with email encryption
8. For any of the difficulties indicated above, please give any applicable details that you recall. (text box)
9. Did you have any other problems with email encryption using Thunderbird+Enigmail after the training? (text box)
10. Do you use an email encryption system other than Thunderbird+Enigmail? Which system, and why do you use it? Please list and discuss all systems you use and why. (text box)
11. Which email encryption system do you use most frequently use? (text box)

    [Questions 7-9 asked with respect to the system that used most frequently]

12. If you no longer use Thunderbird+Enigmail, why? (text box)
13. If you no longer use email encryption, why? (text box)
14. For the following questions, select all that apply (never/in the past/sometimes/often/always):
    (a) Do you encrypt emails even if their contents aren't considered personal/sensitive?
    (b) Do you use email encryption for personal email?
    (c) Do you use email encryption for activist/organizing/volunteer work?
    (d) Do you use email encryption for paid work?
15. Which of the following ways do you regularly access the email account(s) that you use for sending and receiving encrypted emails, e.g. to read or send unencrypted email from the same account (select all that apply):
    – Thunderbird
    – Outlook
    – Apple Mail
    – iPhone/iPad
    – Android device
    – web interface (e.g. via gmail.com or mail.riseup.net)
    – other: (text box)
16. Imagine you are starting to use a new program (or app) on your laptop or desktop. For each of the following, indicate whether your level of confidence in being able to use the new program. ("I couldn't do it" plus a 10 point Likert from "Not at all confident" through "Moderately confident" to "Totally confident", as a table)
    I could use this new program ...
    (a) if there was someone giving me step-by-step instructions.
    (b) if there was no one around to tell me what to do as I go.
    (c) if I had never used a program like it before.
    (d) if I had only the program manuals for reference.
    (e) if I had seen someone else using it before trying it myself.
    (f) if I could call someone for help if I got stuck.
    (g) if someone else had helped me get started.
    (h) if I had a lot of time to use the program.
    (i) if I just had access to built-in help in the program.
    (j) if someone showed me how to do it first.
    (k) if I had used similar programs before this one.
17. What is your gender identity? (text box)
18. What is your ethnic identity? (text box)
19. How would you describe your political orientation? (text box)
20. What is your age bracket (select one):
    ≤ 19 20-29 30-39 40-49 50-59 60-69 70+

CLDC Digital Security for Activists:
GPG/PGP Email Encryption & Signing

(GNU/Linux)

PART I – download, install, & configure OpenPGP

☐ **1.** Using your GNU/Linux package manager, install gnupg2.
From the terminal: `sudo apt-get install gnupg2`

☐ **2.** Likewise, install Thunderbird (called Icedove in Debian Linux):
`sudo apt-get install thunderbird`

☐ **3.** Likewise, install enigmail:
`sudo apt-get install enigmail`

☐ **4.** Launch Thunderbird — email account setup starts automatically, or start it from the menu: ☰ *File → New > Existing Mail Account*

☐ a) select "*Skip this and use my existing email*"

☐ b) Enter your name as others will see it, your Email address & Password
** If you don't see "Configuration found at email provider" - please ask for help!*

☐ c) Select *IMAP (remote folders)*, click *Done*

☐ d) Sync your email: ☰ *File → Get New Messages for > All Accounts*

PART II – make a PGP key pair

☐ **5.** ☰ *Enigmail → Setup Wizard* starts automatically to generate a key pair your private ("secret") key and your public key ("public lock").
Select "*Start setup now*", then "*I prefer a standard configuration*"
In the future you can make new key pairs from the menu:
☰ *Enigmail → Key Management; Generate → New Key Pair*

☐ **6.** Enter the name and email address you entered in Thunderbird.

☐ **7.** Enter a **strong passphrase** – use Diceware or a reliable password manager: world.std.com/~reinhold/dicewarewordlist.pdf

☐ **8. Write down** this passphrase & keep it safe, away from your computer.

☐ **9.** Generate a revocation certificate & save it to a folder on your computer—you should copy it to a USB stick or backup drive, since you'll need this if you ever forget your passphrase or lose your key. You'll be prompted for your passphrase. Click *next* then *Done/Finish*

☐ **10. Back up your key pair** to a **safe & secure** location (ideally, an encrypted USB stick, **never** email it or sync it to a cloud server):
☰ *Enigmail → Key Management*; right-click on your key, select "*Export Keys to File*", choose "*Export Secret Keys*"

PART III – exchange, verify and sign public keys

☐ **11.** Compose a new email message (*ctrl-N*) to a comrade. In the Enigmail toolbar in the compose window above the "From" field select "*Attach My Public Key*". In red it will read "**This message will be unsigned and unencrypted**" – that is OK. Send the email, and ask your comrade to also follow this step and send you their public key.

☐ **12.** Open each other's email messages. Right-click the attached file (0x#######.asc) and select "*Import OpenPGP key*"

☐ **13.** Verify that you have your comrade's authentic public key. Each of you will reveal the key's fingerprint: ☰ *Enigmail → Key Management*, right-click the comrade's key and choose "*Key Properties*". If the imported key isn't listed, in this window menu: *File → Reload Key Cache*

☐ **14.** Read the entire fingerprint aloud and ask your comrade to confirm that it matches theirs — if exchanging keys remotely, read fingerprints over the phone. **Do not skip this step:** otherwise, an adversary could substitute a counterfeit public key to read or modify your emails!

☐ **15.** If the fingerprints match: in the "*Select action ...*" or "*Certify*" drop-down menu, choose "*Sign Key*" (in the pop-up window, "*Key for Signing*" is your own key). Select "*I have done very careful checking*"

☐ **16.** Ask your comrade to verify your public key (following steps 15-17)

☐ **17.** Write a new email message to your comrade. When the lock icon is selected/highlighted & in the locked position, it will be encrypted.

PART IV – ensure email authenticity

☐ **18.** Email messages can easily be falsified. PGP can be used to verify the author and contents of an email. You should sign your encrypted emails by default: ☰ *Preferences → Account Settings* — at left, under your email account, click "*OpenPGP Security*" — under "*After application of defaults and rules*" tick the box beside "*sign encrypted messages*"

☐ **19.** Signed emails in Thunderbird/enigmail are indicated in the header:
* **[green] Good signature from ...** – everything checks out.
* **[cyan] UNTRUSTED Good signature from ...** – looks good, but you will need to verify/fingerprint (and sign) your contact's public key.
* **[red] Bad signature ...** – something is horribly wrong. Get in touch by a channel other than email to discuss this and check their key.

☐ **20.** This is especially useful for sharing public keys that you have verified/fingerprinted. Compose an email to a comrade who has verified your public key. In the compose window menu: *Enigmail → Attach Public Key...* select relevant keys. When receiving an email with the header "Good signature from ..." any attached keys can be trusted.

Fig. 2. PGP worksheet for Linux. Similar worksheets were provided for Windows and Mac.