Contextual Intent: Activists' Privacy Considerations for Collaborative Technology in U.S. Social Movement Groups

Alexandria LeClerc
Oregon State University
alexandria.leclerc@gmail.com

Glencora Borradaile
Oregon State University
glencora@oregonstate.edu

Kelsy Kretschmer
Oregon State University
kelsy.kretschmer@oregonstate.edu

Abstract

Activists engage in highly public and collaborative work, and their social movement groups have long been targeted by the surveillance state. Many consider the adoption of secure and privacy-enhancing technologies to be the antidote. However, activists operate with limited resources and elevated risk, making the adoption of these technologies difficult and imperfect. We investigate how groups navigate organizing using digital communication, and specifically how groups make intentional (even if insecure) decisions around privacy protections in their organizing.

We interviewed 40 activists belonging to 33 U.S.-based social movement groups ranging in size, structure, and tactics. Responses were analyzed qualitatively to uncover factors influencing digital security decisions for organizing work. We find that low-risk hierarchical groups with a lack of training and little concern for surveillance tended to not consider privacy as they navigate digital technologies and horizontally-organized groups engaging in risky activities took intentional strides to enhance their digital privacy within the context of their activism. The availability and influence of a technically-minded group member or advisor plays a strong role in the adoption of PETs. A groups' lack of knowledge in PET use or concern with surveillance is a barrier to PET adoption and highlights the importance of education. Finally, we find that feature availability and learnability is still an important factor in PET adoption.

This work illustrates the nuanced factors and responses that users aware of the threat of surveillance are taking into consideration, including but not restricted to, the adoption of E2EE communication technology and the digital security culture necessary to operationalize it.

Keywords

privacy, surveillance, usability, social movements

1 Introduction

It is no secret that social movement work is subject to surveillance-enabled interference [21, 25]. Post-9/11 U.S. laws designed to address terrorism have been applied to environmental, animal-rights, and Black Lives Matter activists despite formal protections through the First and Fourth Amendment that should protect dissent and public engagement through activism [49, 51]. With a shifting landscape of political acceptability of protest and groups operating as non-profits that challenge the government at risk of losing legal status [4], compromised information can decrease safety and increase ramifications of social movement activity. In the current U.S. political climate, these consequences are made explicit, such as the labeling of anti-fascist ideology, often shortened to Antifa, as a domestic terrorist organization [72]. In recent years, the U.S. government has sought private data on those engaged in dissent: web traffic data on protesters of the 2017 presidential inauguration [39], Facebook data on anti-fossil fuel protesters [20], private data of student journalists covering protests [13], and social media data on anti-ICE protesters [29], to name just a few examples.

Surveillance can be a repressive tactic unto itself, where the threat of surveillance can deter dissent or otherwise chill behavior. As theorized by Foucault, surveillance can induce populations to conform to the social norms desired by those in power [28]. Disengaging from dissenting behavior and this chilling effect can more greatly impact those who seek to challenge the entities that perpetuate mass surveillance, namely governments and large corporations [50, 68]. One hope of privacy-enhancing technologies (PETs) is to counter the chilling effect by protecting communications from suspicionless surveillance. We investigate whether activists respond to surveillance with protective behaviors such as the adoption of PETs and sought to explore what factors influence robust digital privacy in social movements.

Groups engaging in social movement work provide a rich context for exploring privacy. The breadth of social movement organizing structures provides rich heterogeneity to uncover and explore themes related to technology use. Social movement work requires working with others, often in overlapping groups and groups working in coalition with each other that engage different tactics to meet their goals. These collaborative aspects of social movement work often requires coordination between different individuals, institutions, and sectors with varying technological capabilities and practices. Activists must also balance the need to exist in the public sphere against concerns of being targeted by surveillance infrastructure and online harassment [2]. Despite awareness within activist communities of the presence of the surveillance state, activists do not always uptake privacy-enhancing technologies in their organizing [8] and may engage in non-technological solutions or a mix of technical and non-technical solutions to achieve privacy [3, 12, 19, 40].

We hypothesized that adoption (or not) of PETs by activists would be more nuanced than any single factor (such as learnability or stigma) and so we sought to uncover influencing factors

Proceedings on Privacy Enhancing Technologies 2026(3), 484–504

https://doi.org/10.56553/popets-2026-0092

through semi-structured interviews with members of social movement groups. Initially, we sought to understand those factors that correlate with the adoption of privacy-enhancing technologies. However, once we began interviewing activists it became clear that privacy decisions were more involved than simply choosing whether to adopt an end-to-end encrypted (E2EE) tool. Activists who were using PETs were doing so to different extents and groups with the knowledge, motivation, and resources needed to adopt PETs were still sometimes eschewing tool adoption, but doing so with intentionality and incorporating the use of less private platforms with security-culture-based, non-technical practices. So we broaden our research question to:

> What factors influence intentional decision-making regarding digital privacy in social movement groups?

We interviewed 40 activists belonging to 33 U.S.-based social movement groups that are left-of-center to far-left on the political spectrum. These groups ranged from small to large, from horizontally organized to bureaucratically led. The groups engaged in differing levels of risk entailed by their activism, ranging from low-risk reformist work to work that could mean loss of employment or legal consequences for members. The groups we interviewed used a combination of strategies to adapt both privacy-enhancing and mainstream technologies into their organizing efforts and complimented this with manual practices and protocols as part of establishing a security culture to increase group privacy. Using inductive thematic coding, we identified factors across these groups that related to their navigation of technology choices and decisions around privacy. We used qualitative comparative analysis to structure our findings and tease out themes that explain the presence and absence of intentional privacy decisions.

We find that group structure, activism risk-level, particular social movement context, access to technical help, and establishing a security culture all influence how, and whether, a group considers privacy in their technology choices and that intentionality is an important step toward PET adoption. Participants were able to demonstrate a basic understanding of the concept of encryption and general digital security practices, and some were even trained specifically in the use of PETs for social movement work. However, awareness and knowledge alone were not sufficient in explaining why a group was or was not using privacy-enhancing communication technology or doing so intentionally. Social movement groups were weighing privacy against multiple factors such as usability, functionality, and public perceptions. Hierarchical groups with a lack of security training, little concern for surveillance, and a low level of risk tended to choose technologies without considering privacy implications. Conversely, horizontally organized groups with a high degree of concern or risk were intentional about their technology choices and considering privacy in their technology choices with feature limitations, difficulty of use, and stigma arising as barriers to adoption.

2 Related work

Research more generally on social movement use of digital technology has evolved from early skepticism about the Internet's ability to sustain meaningful activism to a rich, interdisciplinary field examining how Internet technologies shape every stage of movement activity [24]. As communication technology has evolved from paper, to telephone, to digital, activists have adapted to make use of these tools to their advantage [14]. However, members of social movements are often also members of groups who are marginalized by modern technology. Mainstream digital technology already fails to meet all the needs of users of historically marginalized groups, and this holds true for activists as well [65]. We see this general technology gap extend to activists in recent research. We compare our findings to the recent work in this area in Section 6.

2.1 Barriers to adoption of PETs

Early research into the uptake of PETs focuses on the general public and has largely examined the usability and learnability of these technologies. PETs use has historically been difficult for average computer users to navigate in even a controlled setting [27]. Studies seeking to understand the barriers to adopting PETs have largely focused on difficult-to-adopt tools, focusing explanations on usability and learnability, and generic populations or convenience samples, and unfortunately not addressing the heterogeneity of privacy needs that would echo that found in privacy risk assessments [52].

The first usability studies of PETs examined E2EE email using the PGP protocol. PGP email requires some degree of manual set up and management of encryption keys, PGP provides robust E2EE and was the first PET available to the general public, notably developed with the use-case of anti-nuclear activism in mind [75]. These initial studies, starting in 1999, focused on usability in a controlled lab environment with first-time users and have repeatedly found the technology difficulty to learn. Whitten and Tygar were the first in several examinations of PGP email interfaces, seeking to understand what about the interface design impedes users from being able to successfully send and receive PGP email [74]. E2EE email has evolved since this initial evaluation, and while similar analyses through 2015 have found some improvement, the tools are ultimately still difficult for users to learn how to use [30, 64, 67].

There has been less research into the practical adoption of PETs by communities of users in the wild, though a few factors beyond usability have been identified as playing a role, including network effects [22] stigma of use [31]. and contextual privacy [43]. In recent years we have seen more usable PETs such as Signal and Proton come to market, changing how users install and use E2EE and privacy enhancing communication tools.

2.2 Building PETs for high-need users

Development of more usable PETs followed studies identifying learnability challenges with PGP and considered the needs of users with higher privacy needs. In 2017, Lerner, Zeng, and Roesner created an E2EE email platform 'Confidante' and evaluated its use amongst journalists and lawyers [42]. Participants were more successful with Confidante than with previously evaluated PGP tools, but even within the scope of this more specific population of users, their varied needs proved difficult to meet with a one-size-fits-all solution. In the same year, McGregor et al. retrospectively studied the team responsible for the Panama Papers reporting [46]. The Panama Papers investigative journalists were supported by a few

technical experts who provided ongoing support for E2EE communication and file sharing, including customizing tools to suit the needs of the various contributors.

Both studies highlight the challenges arising from specific users' needs but the solution presented is to tailor technology for a specific action. Many high-needs individuals, and in particular, activists, do not have the resources to develop and support bespoke tools. Most users must adapt to the technology available in an ever-changing landscape of available privacy information and advice.

2.3 Activist response to surveillance and privacy

There are notable studies over the last half decade that have examined the use of PETs by activists. In this era, we see activists motivated to utilize privacy-enhancing technology but falling back on manual privacy strategies over non-private communication channels when the technology is inaccessible or onerous. Borradaile et al. found that in order to adopt privacy enhancing communication channels, members of social movements groups must make a collective decision to do so, usually encouraged by a few motivated individual members willing to support the groups' adoption [9]. Dafalla et al. found that among activists in Sudan, when the private communication channel of choice was made unavailable, activists were forced to rely on low-tech and manual defense strategies over non-private channels [19]. Albrecht et al. found that activists in Hong Kong tried to maintain pseudo-anonymity and secrecy by carefully isolating communication across different channels and devices [3]. During the George Floyd protests of 2020 Rosenbloom et al. found that novice protestors relied heavily on personal networks to find information, used PETs to feel safer in participating in protests, relied on word of mouth for guidance, and showed concern for the reliability of information available online [63]. Even when a PET would be preferred, activists cannot always rely solely on technology and have adapted manual and analog alternatives.

Activists must balance the material realities of implementing PET adoption with the social dynamics and perceptions of private communication practice. In 2006, Gaw et al. published a study of an activism-focused organization to understand how users were interacting with private and secure communication [31]. Some participants felt the need to use secure channels for most organizational needs, but expressed an aversion to do so for fear of seeming paranoid by their colleagues; other participants expressed doubt their communication would warrant targeted surveillance at all. In 2022, Kapoor et al. show that labor organizers balance the practical realities of organizing under employer surveillance and the need to choose familiar communication channels. Participants described privacy as both an individual and a collective operation, framing the two as interlinked concepts in achieving protections from workplace surveillance [40]. Brough, Jensen and Albrecht observe that UK climate activists' adoption and perception of PETs are deeply shaped by the social, organizational, and moral dynamics of their movement [12]. All three studies find that activists grapple with the tensions between recruitment and protection, with the adoption of PETs posing as a barrier to participation.

There is an abundance of advice aimed at activists about privacy, but said advice is often difficult for users to sift through. There is little guidance from, or even consensus among, security and privacy experts on how users should prioritize the actions they can take to protect themselves [58]. Even when activists understand what the advice is telling them to do, they are not sure why they are being told to do it [11]. Activists have differing goals and mental models from the security and privacy professionals disseminating information, resulting in a divide between how experts recommend priorities and what privacy-conscious users end up prioritizing [37]. While the available privacy and security advice for activists is not necessarily inaccurate, the number of actions suggested are numerous and overwhelmingly wide-ranging.

3 Methods

We conducted 40 semi-structured interviews with participants belonging to 33 social movement groups between December 2019 and January 2022. See Table 1 for a timeline of interviews. Interview questions focused on group, rather than individual, activities and perceptions. Likewise, analysis is performed at the level of groups rather than individuals, resulting in 33 cases to analyze. Some groups are local chapters of national groups, but we consider each chapter a separate case.

All interviewees were "key informants" within their groups [5]. For hierarchical groups, this might be an elected position or an administrative position. For non-hierarchical groups, this was usually a person referred to colloquially as a "core" organizer, a member that did not have formal authority but was still considered an essential coordinator for the group.

Interviewing started prior to the COVID-19 pandemic, with 3 interviews being conducted in person prior to April 2020 and the remainder conducted remotely via Signal (E2EE) call, phone call, or Zoom to comply with social distancing guidelines. The semi-structured format of the interview allowed participants to set the pace resulting in interviews varying in length from 23 to 91 minutes and averaging 51 minutes. Semi-structured interviews are useful for adjusting expectations as data is collected, allowing new information and directions to emerge [5].

3.1 Recruitment

We recruited social movement groups across the spectrum of organizing structures and tactics. We recruited direct-action groups initially through convenience sampling of our pre-established good standing in activist trust networks and snowballed from these an approximately equal number of additional participants. This stage of recruitment included many typically difficult-to reach direct-action groups and was limited to politically left-of-center groups in the United States. We then expanded our recruitment to include cold-emailing additional public-facing and largely bureaucratic groups to intentionally diversify our sample across modes of organizing. We limited this phase of recruitment to left-of-center organizing to avoid potentially introducing a conflating factor of political stance and artificially biasing our findings. Likewise, we limited the expanded recruitment to the United States for similar reasons. Our recruitment practices follow the diverse case selection practices described by Seawright and Gerring [66].

The groups recruited (described in Table 2) varied in the scope of their work. In order to preserve their anonymity we categorize them under the following general missions:

Table 1: Interview timeline

Numbers were assigned to groups in the order that the group was recruited. Chapters that share a parent organization are denoted with the same number for the shared parent, and individual chapters with a letter (e.g. groups 1a and 1b). Note that groups without a letter may still be chapters of a parent organization in cases where we did not interview another chapter.

2019	2020										2021								2022
Dec	...	*Mar*	*Apr*	*May*	*Jun*	*Jul*	*Aug*	*Sep*	*Oct*	*Nov*	...	*Apr*	*May*	...	*Sep*	*Oct*	*Nov*	...	*Jan*
4		3	1a	2	6	9	10	13	14a	15a		1b	18		16b	16c	14b		19-22
5					7		11	8		16a							15b-e		
										17							16d-f		

Community Groups revolved around providing resources to a specific local community. These groups may host informational events, distribute resources, or connect local residents in their area to services and resources. This is distinct from Direct Action as it focuses on fostering local relationships and services.

Direct Action Groups focused on demonstrations for specific political and social movements. This is distinct from Community groups as these groups were more interested in participating in wider social movements, and not solely on providing local services.

Labor Groups involved in worker rights and union organizing. This may be workers unionizing their workplace, or larger umbrella groups providing resources for workers who were looking to, or had already, organized their workplace.

Legal Groups focused on legal services and resources. Often these groups provided counsel to other groups or to individual activists, but this could also include organizations whose practice was focused on aspects of the law relevant to various social movements.

Policy Groups organized around a specific policy issue. These groups often employ a number of different methods, and may have the same goals or scope as direct action, but operate in more 'official' channels towards influencing policy.

The scope of work for groups we interviewed were usually covering one part of a broader social movement, and the categorization is meant to reflect these general roles without leaking identifying information. The above categories are not exclusionary. A group may engage in activities that could be considered under more than one category, but we attempt here to best reflect the primary scope of their activism.

Table 2: Attributes of Groups Interviewed

GROUP	MISSION	STRUCTURE	# of Members
1a	Direct Action	Elected	<100
1b	Direct Action	Elected	<100
2	Direct Action	Non-Hierarchical	<100
3	Labor	Non-Hierarchical	>1000
4	Legal	Elected	<100
5	Labor	Elected	>1000
6	Legal	Elected	100–1000
7	Legal	Elected	<100
8	Community	Non-Hierarchical	<100
9	Direct Action	Non-Hierarchical	<100
10	Direct Action	Non-Hierarchical	<100
11	Community	Non-Hierarchical	<100
12	Direct Action	Non-Hierarchical	<100
13	Labor	Elected	>1000
14a	Policy	Elected	100–1000
14b	Policy	Elected	>1000
15a	Policy	Elected	>1000
15b	Policy	Elected	>1000
15c	Policy	Elected	>1000
15d	Policy	Elected	>1000
15e	Policy	Elected	>1000
16a	Policy	Elected	100–1000
16b	Policy	Elected	>1000
16c	Policy	Elected	100–1000
16d	Policy	Elected	100–1000
16e	Policy	Elected	>1000
16f	Policy	Elected	100–1000
17	Policy	Elected	100–1000
18	Policy	Elected	<100
19	Direct Action	Non-Hierarchical	<100
20	Direct Action	Non-Hierarchical	<100
21	Direct Action	Non-Hierarchical	<100
22	Legal	Non-Hierarchical	<100

3.2 Ethical principles

The research protocols were approved by our Institutional Review Board under study number 8537. Informed consent was obtained at the start of interviews and additional data protections were taken in order to meet the privacy needs of our population. Participants were informed of how their data would be used and that they could opt-out of participation at any point, including retroactively.

Interviews were recorded on an offline memo voice recorder, and stored offline on a designated computer with an encrypted hard drive. Audio was transcribed manually by one member of the research team. All of the audio files were deleted after they had been transcribed and anonymized. Participants were informed prior to being recorded that they could request audio recording be stopped at any point. One participant requested not to be audio recorded at all, and their interview was conducted with the interviewer taking notes while conducting the interview, and then filling in with

more details immediately after the interview had concluded, as is best practice. Research communication and all data containing identifiers including contact data for recruitment, transcripts, individual and group demographic data, were relayed via E2EE chat and file transfer. Participants were informed of data practices prior to recording for all interviews.

After March 2020, to enable social distancing, the research protocol was adapted in order to conduct interviews remotely. Participants were given their choice of telecommunication: Signal [15] app for E2EE voice call, normal phone call, or Zoom call. Signal was strongly recommended to participants in order to preserve their privacy, but interviews were ultimately conducted on the technology that the participant was most comfortable using.

3.3 Thematic coding

Our interview instrument (Appendix C) covers a range of factors we hypothesized would influence privacy decisions. Interviews were semi-structured, with conversation guided by the topics in the script but allowing for open discussion and follow-up questions. The interview transcripts were hand-coded using MAXQDA software by two authors over three rounds, with the third round being applied to all transcripts. An open coding scheme was used to inductively uncover themes. We formalized themes relevant to the technology decisions and privacy choices and encoded these as a set of binary conditions; we describe these conditions in detail in Section 4.2. Some conditions were coded in a straightforward way based on participant responses (e.g., TRAIN) while others were determined via qualitative coding by two authors (e.g., RISK). We coded whether a group was intentional as 0 or 1. This was done qualitatively through two researchers independently coding the groups with this outcome with little disagreement and a reconciling process. We describe the coding of this in detail in Section 4.1.

We thus summarize each group in our sample as a set of binary conditions, one binary outcome, alongside the underlying more nuanced themes from the interviews. For some groups, multiple members were interviewed. While these members may have differed in opinions on interpersonal dynamics of their group, they did not dispute each other on the specific, attribute-related conditions analyzed here.

3.4 Comparative case analysis

We employ qualitative comparative analysis (QCA), a programmatic method that finds associations between characteristics as they relate to an outcome of interest. QCA uses Boolean minimization to identify combinations of Boolean conditions in disjunctive normal form that separate the groups with positive outcomes from those resulting in negative outcomes. We explain the mechanics of QCA in more detail in Appendix A. We chose to use QCA because it allows in-depth cross-case comparisons without losing focus on relevant complexity within observed cases. QCA as a methodology augments traditional qualitative approaches by providing a systematic and reproducible organization of themes [59]. The thematic organization that QCA provides is valuable in its ability to identify the relevance of certain measured conditions in a way that is more structured than evaluation by human researchers alone. We organize our findings using the QCA-identified combinations of conditions in Section 5.

The sample of activist groups for this study share many attributes, but the specific nature of their work is varied and context-dependent, and the interviews conducted were open-ended. This study intentionally focuses on the experiences and opinions of the activists engaged in this work, and the open-ended design was employed to capture to the real experiences of these individuals in the field. A rigid quantitative design would be more restrictive in this sense, and this work aims to account for observations which may lay outside the scope of what statistical hypotheses traditionally consider. QCA allows for richer examination of conditions in context, and considers those conditions in combination, not just individually. Unlike statistical analysis, QCA is more conducive to identifying conditions that may be necessary to result in an outcome, but may not be sufficient to do so in isolation. Necessary conditions may need other supporting conditions to be present in order to produce the measured result.

QCA was developed for understanding richly detailed cases such as the groups in our study [54, 55, 59] and is used to compare and evaluate data sets with the number of cases we have [16, 60]. While QCA is often used to study cases whose characteristics are derived via external measurement (such as economic, trade and census data), it has also been used to explore characteristics derived from interview data following an inductive coding process as we do [26, 57, 61]. QCA is widely used across social movement studies and political sociology to understand how case characteristics and attributes interact to produce outcomes of interest, which was our study's primary goal [7, 10, 18, 38, 44]. More specifically, QCA has been used in similar research that seeks to understand factors related to success in social movement settings [9, 34, 45].

4 Interview data

At the end of the interview each participant was asked to define, in their own words, terms such as encryption and security. Asking for these definitions at the end of the conversation allowed us to understand how participants were thinking about these definitions (which have varying interpretations depending on domain) in the context that was most relevant to them and their organizing work, without being primed to frame the whole conversation around privacy and security.

Most participants were able to describe encryption at an abstract level. This included participants who were not currently and had not previously engaged in risky activism, and participants who were not formally trained on the use of privacy-enhancing technology. For instance, a member of Group 16e (an elected group that was less involved in direct action) explains:

> To me encryption is something that protects the data while it's in transit, understanding that the source of the data and whoever's receiving it at the other end should be able to see it, in it's full form, but while it's in transit somebody else isn't able to access it.
>
> – Group 16e

All groups interviewed maintained at least one digital communication channel within their group, though the number of different tools varied by group (see Table 3). We label Signal, Keybase, Proton

Table 3: Tools Used By Groups

Select tools in use by our interviewed groups. A full table is in Appendix D.

	←——— Privacy-enhancing ———→												
Group	Signal	Keybase	Crypt-pad	Proton	Jitsi	Zoom	Social Media	Database	Email	Excel	Google Drive	Phone	SMS
1a	-	-	-	-	-	-	●	-	●	-	●	●	-
1b	●	-	-	-	-	●	-	-	●	●	●	●	●
2	●	●	-	-	●	●	●	-	-	-	●	-	-
3	-	●	-	-	-	-	●	-	●	-	-	-	-
4	●	●	●	●	-	●	-	-	-	-	-	-	-
5	-	-	-	-	-	-	●	●	●	-	●	●	●
6	●	-	-	-	-	-	-	-	●	-	-	-	●
7	●	-	-	●	-	-	-	●	●	-	-	-	●
8	-	-	-	-	-	●	●	-	●	-	●	-	●
9	●	-	●	-	●	-	-	-	●	-	-	-	-
10	●	●	-	-	●	-	-	-	-	-	-	-	-
11	●	-	●	-	-	●	-	-	●	-	●	-	-
12	-	-	-	-	-	●	●	-	-	-	●	-	-
13	●	-	-	-	-	●	-	-	●	-	●	●	●
14a	-	-	-	-	-	●	-	-	●	-	●	-	●
14b	-	-	-	-	-	●	●	-	●	-	●	●	●
15a	-	-	-	-	-	●	●	-	●	-	●	-	-
15b	-	-	-	-	-	●	●	-	●	-	●	-	-
15c	-	-	-	-	-	●	-	●	●	●	●	-	-
15d	-	-	-	-	-	●	-	-	●	-	●	●	●
15e	-	-	-	-	-	●	-	-	●	●	●	●	-
16a	-	-	-	-	-	●	-	-	-	-	●	-	-
16b	-	-	-	-	-	●	●	-	●	-	●	-	●
16c	-	-	-	-	-	-	●	-	●	-	-	-	-
16d	-	-	-	-	-	●	●	-	●	-	●	-	●
16e	-	-	-	-	-	●	●	-	●	-	●	-	-
16f	-	-	-	-	-	●	●	-	●	-	●	-	-
17	-	-	-	-	-	●	●	-	●	-	-	-	-
18	-	-	-	-	-	●	●	-	●	-	●	-	-
19	●	-	-	-	-	-	●	-	-	-	-	-	-
20	●	-	●	-	-	-	●	-	-	-	-	●	●
21	●	-	-	-	●	-	-	-	-	-	-	-	-
22	●	●	●	●	●	-	●	●	-	-	-	-	-
Count:	13	5	5	3	5	21	19	4	24	3	21	8	12

and Cryptpad as PETs for their use of E2EE. We include Jitsi as a PET, as groups indicating their use also indicated use of the E2EE option within Jitsi or use of the public meet.mayfirst Jitsi instance, described as trusted by multiple interviewees.

> Yeah, we use Jitsi, specifically, meet.mayfirst. There's some times when we use Zoom [...] but [Jitsi] for like internal meetings and things for that. – Group 2

While some groups did not utilize PETs, only 2 groups restricted themselves to PETs exclusively (groups 10 and 21). We note that the interviews of the groups indicating use of both Signal and Zoom (Groups 1b, 2, 4, 11, 13) occurred before the group calling feature was available in Signal.

4.1 Outcome of interest: INTENT

Our research sought to understand how to increase adoption of PETs by social movement groups, such as indicated by the privacy-enhancing columns of Table 3. However, as interviews progressed, it became apparent that adopting PETs is not the only way to achieve a positive outcome where privacy is concerned. Focusing solely on use of technologies with privacy guarantees would flatten the rich, nuanced, and informed decisions made by social movement groups about technology use. Adoption of PETS by our groups varies, with 2 groups solely using PETS for communication, half our groups abstaining from PETS and those groups using PETS doing so to different degrees, and with different threat models. The way that groups detailed how they considered security and privacy, how

much training they had undergone, and their understanding of surveillance was not directly represented by simply adopting a PET. Adopting a PET was one vector of very complex sociotechnical decisions that required many different considerations. What clearly delineates our groups is whether they are making *intentional and informed decisions* about technology with respect to privacy.

Our articulation of using INTENT as an outcome of interest arose from our inductive process of analyzing the interviews. Two authors independently coded for INTENT, based on a holistic consideration of the entirety of the interview script, only disagreeing initially on the code for Group 8 and coming to agreement through discussion. Groups coded with the final measured outcome as INTENT = 1 were those groups that were choosing technologies intentionally and considering privacy as they were making those choices. Groups coded with INTENT=1 are correlated with those groups using PETs as a strategy to protect their data from third parties. However, the groups coded with INTENT=1 also include some groups that forwent PETs, despite being aware of what PETS provide, but did so as a calculated choice, noting that use of PETs would come at a cost to their group's work.

Groups coded with INTENT=0 made choices about communication technologies without reasoning about the privacy or lack of privacy those choices would imply. These groups are highly correlated with the groups that are not using PETs. However, it also includes groups using PETs, such as a group opting for some combination of PETs, non-private technologies, and in-person communication for different operational needs, but making choices between these options without reasoning about the privacy or lack of privacy those choices would imply. It also includes a group who accidentally adopted a PET without knowing it was privacy enhancing.

INTENT is highly correlated with PET adoption. However, the cases in which we don't have perfect correlation allow us to better understand when and why PETs are adopted or not and provide a more consistent top-level organization of the underlying themes regarding privacy behaviors. In Section 5.1 we analyze those groups with INTENT = 1 and in Section 5.2 those with INTENT = 0.

4.2 Conditions influencing intentionality of privacy decisions

Our inductive coding process identified a number of themes and *conditions* that were relevant to how groups were making technology choices. We describe those conditions here and use them to organize our findings in the next section.

ELEC Based on response to the question: "Do you have formal leaders, like elected positions?" Participants were also prompted to discuss if and how the group selected leadership positions. If the process was formalized, such as through, but not limited to, elections, we coded the group as ELEC=1. Some groups had members that acted as leaders on certain projects or on certain topics, but these were not formalized or elected. These groups were coded ELEC=0 as their leadership structure was not formalized.

RISK Coded as 1 if the research team determined that the group engages in activism that could result in repercussions for members. This could include, for instance, job loss or arrest.

Table 4: Conditions and outcomes for all groups

Group 1a had INTENT=0 while groups 1b and 4 had INTENT=1, but these three groups had the same set of conditions.

Conditions					Outcome	Groups
ELEC	TECHIE	RISK	SURV	TRAIN	INTENT	
0	0	0	0	0	0	12
1	0	0	0	0	0	14a, 15a, 16a-d, 16f, 18
1	1	0	0	0	0	8, 12, 14b, 15b-e, 16e
0	0	1	0	0	0	17
1	1	0	1	0	0	6
1	1	0	1	1	conflict	1a-b, 4
0	1	0	1	0	1	7
1	0	1	1	0	1	3
0	1	1	1	0	1	2, 19, 20, 21
0	1	0	0	1	1	11
1	1	0	0	1	1	5
0	1	1	1	1	1	9, 10, 22

TRAIN Coded as 1 if the group's participants noted formal training in response to the question: "Have you sought out information about making your group information and/or communication secure? Can you tell me about that/those efforts?" Such trainings were indicated as offered by legal organizations either through private training or through workshops at community events and conferences.

TECHIE Coded as 1 if the participants noted a specific person in response to the following questions: "If you were uncertain about a technology your group uses, who or what would you ask for help?" and "Does anyone else in your group consistently worry about your group's security?" These groups discussed having direct access to a tech support person. This may be a group member, a community member that acts as IT support for the group, or an IT professional paid by the group.

SURV Coded as 1 if the participant expressed that the group was concerned about surveillance. This was inferred by how the participant framed their answers and approached topics around data privacy, rather than a specific question outright. This was an intentional decision for the interview to avoid the desirability effect. This is a measurement of the concern expressed by the participants, without concluding whether their concern is warranted, as we seek to explore how social movements are defining and responding to their threat models and risks, rather than assessing how viable we believe their actions are.

Other conditions that we interrogated but did not find useful for organizing our results either through manual analysis or through our use of QCA are described in Appendix B. Table 4 itemizes all the groups by the above-described observed conditions, with rows collapsed for those groups with identical combinations of conditions.

5 Results

We organize our findings by the combinations of conditions (*pathways*) that are associated with each outcome, as uncovered by QCA. We first discuss groups with INTENT = 1, by way of three pathways, and next groups with INTENT = 0, by way of two pathways. As groups 1a, 1b and 4 had conflicting outcomes, they are not covered by the pathways of the qualitative comparative analysis. We discuss these cases in subsection 5.3.

5.1 Groups making intentional privacy decisions

QCA identified 3 pathways that correlate with the positive outcome of INTENT = 1:

Pathway 1:	¬ELEC ∧ TECHIE	2, 7, 9-11, 19-22
Pathway 2:	RISK ∧ SURV	2, 3, 9, 10, 19-22
Pathway 3:	TRAIN ∧¬SURV	5, 11

Pathway 1 indicates that the groups coded as ELEC = 0 and TECHIE = 1 will have INTENT coded as 1. These groups are listed to the right of the pathway. We likewise interpret Pathways 2 and 3. All three pathways have perfect consistency, in QCA parlance. That is, *all* groups coded ELEC = 0 and TECHIE = 1 were also coded INTENT = 1.

We note that the pathways overlap. For example, the fact that Group 2 is coded as INTENT = 1 is encompassed by both Pathways 1 and 2. And, had our number of cases been larger, we may have uncovered additional or different pathways to explain Group 2. However, these pathways provide a grouping of our cases to provide focus for interpreting the qualitative data. We examine each of these pathways in turn.

Intentionally encrypting: Able and capable. The groups with conditions ¬ELEC ∧ TECHIE were using privacy-enhancing technologies (albeit not exclusively) for communication and fit more traditional models of expected success in that they have access to someone to help with adopting new technologies (TECHIE = 1). We also find that their structure provides fewer barriers to changing the way the group organizes itself.

These groups were structured without elected leaders (ELEC = 0), were smaller, more localized, and more focused on specific issues or goals in their mission. For instance, a smaller nonhierarchical group may be a few local activists who frequently attend or organize protests on a specific civil rights issue. In contrast, a larger elected group may have a broader focus, with sub-committees that tackle specific issues. The non-hierarchical structure may be flexible in responding to member concerns, if all members have equal say in the decision-making process. Many non-hierarchical groups use consensus (or similar) decision making. Consensus processes can vary, but within our sample it is often described as follows: one member proposes a motion to the group, the other members then take a vote with the following options: approve and participate in the execution, approve, abstain, oppose but open to persuasion, and oppose.

> It's that long discussion, people chat, and air grievances, and state their opinions and go through the whole, typically several-day process. And by the end of it we kind of wrap it up with a vote and the goal is to make sure that people are heard, and that their positions are taken into account. Because we don't wanna steam-roll over people who disagree. So, if there's a disagreement, like even if it's just one person saying one thing, then we try to take that with as much weight as everything else. – Group 21

This reflects a culture where members are free to propose and execute changes to the group so long as there is no strong opposition. This kind of buy-in process requires more work in a larger group, particularly in the presence elected officers and by-laws that may dictate decision-making. In our sample, RISK was correlated strongly (but not perfectly, e.g., Group 3) with ¬ELEC: groups with non-hierarchical structure tend to be aligned with more grassroots actions and organizing methods. Put another way, forgoing an elected leadership may be correlated with work that involves more risk.

This pathway requires that the group has a reliable tech person to act as a resource. Having a trusted technical advisor is pivotal in these groups that often run on limited time, financial, and human resources. In a non-hierarchical structure, such a technical advisor would have equal place at the table to propose the adoption of secure and private technology.

> I can think of a few other people who are very tech savvy and are very interested in helping the whole process to work better, and then if you got something to say then you're given the floor. And frequently they have things to say. – Group 21

If the group has a technically minded member, that member may have more influence in affecting the technology decisions of the group, not only because of consensus decision making but because there would be fewer challenges to overcome in implementing the technology.

Group 10 noted that they had moved away from PGP email to Signal because it was more fit to the type of work they engaged in, and was more approachable to the members of their social movement group:

> To people who don't utilize these technologies very often, Signal is very straight forward. You open it. You find the person that you want to text, or write something to, and you click on them. It's essentially the same as an iMessage app or something. [...] So we kind of look at it like lowest common denominator, what's the thing that provides security with the least amount of skill for people. – Group 10

This group noted having access to a TECHIE who suggested they try Signal for their organizing. Despite the group deciding to adopt Signal it was still not without difficulty:

> We have a number of people who are not in like, big cities with high broadband, or whatever. So y'know, things that take a higher level of connection, especially if I'm trying to talk to someone in the boonies and they just wanna call me on a normal phone because that works. And they're frustrated — and that's

> not necessarily anybody's fault, that's like a broadband issue – but that has been an issue.
> – Group 10

The group was choosing to use Signal despite the challenges, but had to workaround difficulties in order to not be impeded in their work. End-to-end encrypted chat applications like Signal and WhatsApp are not without usability complications [1, 36]. Activists may be able to overcome some of the usability issues identified in these chat applications if these tools can offer them protection they need, but ultimately utilizing private technology is a means to an end. These groups, while having an elevated tolerance for usability in exchange for privacy, if necessary will forgo the secure option and take on risk in exchange for limiting friction in their communication.

Intentionally encrypting: Risk-taking and concerned. The second combination of conditions, RISK ∧ SURV, has a large overlap with the first in terms of the number of groups covered, but provides an alternate understanding for the adoption of PETs. All the groups explained by this pathway were coded INTENT = 1 because they were intentionally using privacy-enhancing technologies. This pathway would likely align with what most privacy advocates would hope: these groups have the motivation to protect their information because they are engaging in risky activism (RISK = 1); they are concerned about surveillance of their data (SURV = 1); and, they are taking actions to protect that information. We also note that, except for Group 3, the groups characterized by this pathway had access to help in adopting PETs (TECHIE = 1).

> I don't think I would have organized with a group if I knew that we were gonna be texting <laughs>. We needed to communicate when we were at protests, and so that was the initial reason [we used Signal]. – Group 9

Intentionally public. The third combination of conditions, TRAIN ∧¬SURV, only explains two groups, but these two groups are of particular interest for having intentionally decided not to protect their information. In each of these groups, the founders and leadership noted having both training and experience using E2EE software and tools. And while only two groups were coded as having TRAIN = 1 and SURV = 0 (groups 5 and 11), the idea of being intentionally public arose among our other INTENT = 1 groups, particularly as they navigate social media and when to use encrypted communications internally versus mainstream applications for external communications. Most of these groups use a mix of privacy-enhancing and non-privacy-enhancing platforms but are intentional about which they use, when, and for what purpose. Even Group 11, for example, noted limited use of some PETs (namely Signal and CryptPad), with primary communication and shared document functions served by more mainstream methods (namely email and Google Docs). When groups, not just 5 and 11, were deciding to use technology and communication channels they knew to not maintain privacy, they did so for multiple reasons that are best illustrated from our interviews with groups 5 and 11. Only Groups 19 and 20 used on PETS except for social media outreach and only Group 21 even abstained from social media for their organizing efforts.

Interviewees for groups 5 and 11 noted having training when affiliated with groups with different risk levels and threat models than their current organizing project. Their current groups were not concerned about being surveilled. While they were aware of the potential risks of using technologies that do not maintain privacy, they had determined a threat model for their current work that did not necessitate the use of privacy-enhancing technologies.

> I think one of our things is we want to be a public organization. A public group that is an opportunity for people, new people, to get involved, and an opportunity for new people to come in and kind of find these spaces [...] The fact that we want to make it easily accessible to more people that want to plug in to this type of work, and that we have people come in and out, we're wanting [to not] have the technology interfere with someone's desire to engage the group.
> –Group 11

Being intentionally public, does not mean disregarding privacy. Several groups, including groups 5 and 11, made mention of security culture, the proactive practices that group members take to keep group activities, communication, and data safe from surveillance.

Digital security culture, the types of security culture related to the use of digital communication technology, can include, but is not limited to, the use of privacy-enhancing technologies. However, other strategies may include avoiding technology, or being selective about what is discussed, and how it is discussed, on digital channels.

> We talk about and stress [the importance of] security culture often. It's part of our introductions throughout. Kind of the way I think about it now; in some ways I think it's better. Because I think because we're using an unencrypted, corporate tool, people know to be more careful on it. [...] It was better to have security culture than an encrypted tool, and [to] have a tool that was useful. – Group 11

Participants expressed a fear that members becoming 'too comfortable' with the assurances of privacy-enhancing technology could leave the group more vulnerable to a leak, either from an infiltrating adversary or from a technical failure (either due to the technology security or user error). Instead, groups relied on self-imposed protocols on communication channels about what was being shared and how to organize in 'public' view.

Careful selections are made about which members have access to specific channels and data. Even if a privacy-enhancing technology is adopted, security culture must still be nurtured in order to ensure the groups' data stays safe.

However, mainstream technologies, even if chosen mindfully with intent, have other benefits. Groups 5 and 11 noted strategically avoiding the introduction of PETs for the reasons above as well as to benefit certain group members who faced barriers in using or adopting the technology:

> That's more of a frustration with people insisting on Cryptpad and like Keybase and things like that. Because a lot of people, like older folks in particular, like, can't access that. I've had a hard time teaching some of my older activists how to use Gmail. And like

> you're basically excluding so many people from these procedures and you just don't care. – Group 5

And that mainstream, non-secure applications have features that are more useful as a tool for organizing:

> We have conversations about, discussions about, what technology to use for communication. There was a tradeoff, or a wane that had to happen between more secure and private which is preference in that sense, but also functionality and having features that we felt necessary for better more efficient communication. – Group 11

5.2 Groups not making intentional privacy decisions

QCA does not assume that pathways to an outcome are symmetric. This means that simply because a set of conditions is associated with an outcome, the negation of those same conditions may not be associated with the opposite outcome. QCA identified two pathways associated with the negative outcome of INTENT = 1:

Pathway 4:	¬TRAIN ∧ ¬SURV 8, 12, 13, 14a-b, 15a-e, 16a-f, 17, 18
Pathway 5:	ELEC ∧ ¬RISK ∧ ¬TRAIN 6, 8, 13, 14a-b, 15a-e, 16a-f, 18

As with pathways 1-3, pathways 4 and 5 have perfect consistency. That is (for example), all the groups coded SURV = 0 and TRAIN = 0 were also coded INTENT = 0, and these groups are listed under the pathway. Also, as with Pathways 1 and 2, many groups fall under both Pathways 4 and 5, but the two pathways provide different ways of understanding why groups may not be thinking about privacy when they are making decisions about digital technologies.

Groups in these pathways did not use PETs in their organizing – with two exceptions. Group 6 used a PET for limited external communications when required by the external partner (and so, without internal consideration of privacy). Group 8 was using an E2EE chat application for internal communications but was unaware of its privacy properties; we discuss this case separately at the end of this section.

Unintentional and unconcerned. The groups with conditions ¬TRAIN ∧ ¬SURV, reported having not received privacy guidance and did not have a concern with surveillance. These two conditions are not as strongly correlated as one may suspect. In our sample of 33 groups, 7 reported concerns with surveillance despite no specific privacy trainings and 2 groups having received privacy trainings but not having concerns with surveillance.

All but one of the groups covered by this pathway engage in low-risk activism, which may correlate with less concern regarding surveillance and not seeking out privacy trainings or guidance. Conversely, it could be that without the knowledge of surveillance risks and privacy knowledge to create threat models and action plans, the groups are not accurately assessing the risks of their actions.

> There is no state secrets on [Google Drive]. There is nothing on there that would be compromising to anyone. It's not... it's pretty much public information already. Well, I mean it would have emails and addresses which is almost public. I'd say that's the most sensitive, but, bylaws, articles, all those things are public. We're a non-profit, there's nothing on there that I wouldn't happily share. I don't think the information is that big of a risk, we don't have passwords on there. – Group 8

Unintentional and unmotivated. The groups in pathway 5, ELEC ∧ ¬RISK ∧ ¬TRAIN, have a formal leadership structure (ELEC = 1). Elected groups are more bureaucratic, which may result in more than one point of friction with the adoption of privacy enhancing practices. With a top-down approach to decision making, it may be that technology enthusiasts have less of a seat in decision making than in non-hierarchical groups. And so we may view this pathway as a converse of pathway 1. There are also additional steps to approve, onboard, and pay for secure technology for a larger group of people. These groups also tend to be older, well-established groups covering a wider geographical area than the smaller, nonelected groups. This may be an obstacle to changing long-entrenched communication practices, requiring coordination across many individual affiliated chapters or groups. The introduction of the ever-changing software landscape required for secure communication is harder for groups to invest in, especially if their risk level does not warrant a high level of concern. In combination, these groups were engaged in low-risk activism, and so would not provide motivation to overcome the bureaucratic hurdles.

Groups covered under this pathway were largely non-profits officially recognized by the U.S. government. These members may feel that there is less threat from an adversary, as they are legally recognized.

> My attitude and our staff's attitude [...] is that we should be certainly thoughtful about who we share information with and how we are sharing information, but I think a lot of what we do is sort of already in the public realm, where it doesn't feel like high-risk to be talking about it through these platforms – because so much of it is already sort of public information. – Group 15c

Group mission and activities were also usually more well aligned with actions protected by free speech than some of the smaller grassroots groups we talked to, so they may have less motivation to adopt secure technology.

Unintentional adoption. We revisit Group 8, the sole group that did not subscribe to a security culture but had opted to use an E2EE app, WhatsApp, for internal communications. This was not motivated by a need for privacy or security, but rather as a functional requirement so members could more easily communicate cross-platform between Android and iOS.

> [WhatsApp] looked like something most people already had, you could really use the naming feature for the groups and the ability to add and take away people was really user friendly, and that you could easily get it on your desktop as well. That if you had to type out a long message, you could get it on your

> computer and not have to type with just your fingers on the phone. – Group 8

This was apparently suggested by a member who already used the application for their other communications and was able to assist others with installation and use. This is a microcosm of the network effect, wherein one person is utilizing their buy-in to an app to recruit others into the communication network. This case also illustrates, to technology designers, that incorporating encryption into widely used and functional apps, can result in great leaps for privacy. In the case of Group 8, we do not consider this as a complete success as participants in this group were not considering privacy in their other technology choices nor marrying the use of WhatsApp with security culture that would make the PET use meaningful.

5.3 Conflicting cases

Three of the 33 groups survey shared common characteristics, but had contradictory outcomes. The qualitative analysis performed here provides a useful tool for organizing observations, but like all methodology, it is not perfect. Interestingly, two of these groups with conflicting outcomes (INTENT and ¬INTENT) are local chapters of the same parent organization (1a and 1b). All other groups that held a parent group in common in our sample shared the same outcome, yet 1a and 1b are the only chapters that differ from each other. Other groups that were affiliated chapters discussed inheriting more infrastructure in the form of processes and procedures from their parent organization. However, we note that compared to the chapters of groups 14, 15, and 16, 1a and 1b hail from a less involved parent organization that provided little more than a common name shared by the two groups. While these two groups share a common name and mission, each group differs in the specifics of approach, actions, and organization around addressing this mission. It is possible that there are similar affiliated groups existing within this space that have differing approaches to digital technology from each other, despite being associated with a parent in common, thus it is still interesting to consider these two groups and the conflicting cases. When asked to elaborate, 1b noted that their group had attempted to implement the use of some limited PETs for a few specific events, but were unable to consistently make the switch for all group communications and did not report continuing to do so.

6 Discussion

In an age of digital saturation and mass surveillance, perfect privacy protections are not possible. So, what can be counted as a privacy success and how do we get there? For technologists, success is often defined as adopting PETs and using them correctly. However, the journal to uptaking a PET can be long, and users can make nuanced and interesting decisions about their data footprint that achieve degrees of privacy short of PET adoption. We see this not only in our own interviews but in related works, which we discuss in more depth below. Adoption of PETs is still important for robust privacy, but understanding the path from intent to adoption can be used to identify barriers and needs of privacy-minded individuals. Likewise, understanding those without privacy-intentions sheds light on those sociotechnical barriers that could be addressed through improved features, usability and learnability.

6.1 Intention and contextual integrity

In this work, we can interpret the technology choices that groups make as influenced by *and* influencing the contextual integrity of the digital flows that groups are navigating. While contextual integrity was developed to evaluate the potential privacy harms of new technologies or practices [35], its application has been suggested for the qualitative analysis of how users reason about privacy [41]. Among our interviewees from groups that are making intentional decisions about privacy, we see a richness in how groups are implicitly evaluating the contextual integrity of their digital organizing. They reason about the key aspects of contextual integrity, namely data types, transmission principles and actors, and making technology decisions based on this. And we see that this intentionality is a starting point for meaningful adoption of PETs.

We see groups deciding to retain use of mainstream technology choices and thus standard transmission principles, but engaging in a security culture that controls the data types and senders in order to maintain a level of privacy that was meaningful to their activities (groups 5 and 11). Success in private communication should not be measured only in terms of tool adoption: security culture as a PET is necessary, whether employed on or off E2EE channels. Groups combined a developed security culture with specific modes of operation for different technologies that they needed to use. Like the activists interviewed in Hong Kong and Sudan our participants' concern with digital surveillance did not restrict them to purely technological fixes [3, 19]. Activists often choose to (or are put in the position where they must) use non-private communication channels and supplement this with specific protocols in how members safely communicate on these channels. For example, labor organizers maintain secrecy from employers through security culture rather than technology choices before making their efforts public [40]. They abstain from PETs so as to not increase the barrier to participation, but are mindful about which platforms (work vs. non-work) activist-employees are using to protect against employer retaliation.

We have also found groups abstaining from most digital technologies (if only in part) for their organizing, or only using PETs and only doing so for internal communications (groups 19-22). This removes non-movement actors as intermediaries entirely or only transmits meta-data. Forgoing digital technologies would be a very conservative choice in terms of contextual integrity. However, some participants in our study noted skepticism in the promises of PETs and thus a tendency toward the most conservative evaluation for some of their communications. While privacy advocates would hope that users would be able to trust their systems, especially when implementing cutting-edge security protocols and features, the security of these platforms are effectively a black box to end users, who must trust a tool can deliver on its privacy promises. Their trust may be broken, either in the event of a security breach or if the tool publisher changes their terms of agreement.

On the other hand, accidental PET use, such as Group 8's adoption of WhatsApp not knowing it's privacy protections does not necessarily imply meaningful privacy, particularly in the absence of a developed security culture. Through the lens of contextual integrity, such groups are not determining whether their group's information flow is appropriate for their work. While Group 8's

use of WhatsApp does provide some level of protection, they have not considered other choices, such as Signal, that would provide greater privacy through better protections of metadata (reducing the amount of information flowing through a change to transmission principles) with similar usability.

6.2 The influence of risk

Borradaile et al.'s study of individual activist's long-term adoption of PGP email encryption focused on several classic barriers to privacy via a single tool, including motivation, the network effect, and ease of use [9]. As in this study, they also considered the risk level of surveyed activists. Unlike this study in which we found that risk is correlated with intentional privacy choices (often including PET adoption), they found that those who were engaging in riskier activism were less likely to adopt PGP email in the long term. However, our study is not limited to measuring the adoption of a specific tool, but rather a wide array of strategies and approaches that groups employ toward securing their digital communication. If we examine the context of the earlier study which studies PET use in the wild, we see that over the course of the study, ending in early 2018, much easier to adopt E2EE communication platforms (including Signal) were released and gained widespread use among activists and may have supplanted the much more difficult to adopt and maintain PGP. We would expect that risk of activists would, in a less flat analysis of privacy, play a role in increasing one's contextual privacy.

Kapoor et al., in their study of labor activists, comment heavily on the risks that activist employees face through potential job loss and other employment retaliation (despite legal protections) and that while participants do not strictly adhere to PETs, they do calibrate their digital privacy behaviors as a protective strategy [40]. Such activists would be evaluated as making intentional privacy decisions. With more usable or widely adopted PETs, they may opt to increase their digital privacy through consistent PET adoption.

6.3 The importance of technical guidance

Help, through access to technical resources and guidance, is noted as influential in our study and previous studies. Embedded "techies" have domain knowledge and rapport with the activists with which they organize and often provide counsel to multiple different groups within their respective organizing circles. Interviews with Hong Kong and Sudan activists also highlighted the importance of having core organizers to influence, operationalize, and maintain group communication practices [3, 19]. Our interviewees were such core organizers, though not necessarily techies themselves, and were able to reflect on any advice they may have received regarding technology choices. In Boyd et al.'s study, respondents were largely novice Black Lives Matter protest attendees and while they were receiving guidance, they were less likely to follow that advice than our interviewees [11]. However, while these BLM protesters were receiving advice, they were not benefiting from the true help that is often available to central organizers who engage in long-term movement planning.

6.4 Sociotechnical factors

Two of our groups intentionally chose not to use PETs in part as a way to signal their groups' missions not needing to protect information. A similar theme is found in the group studied by Gaw et al. [31] and the climate activists observed by Brough et al. [12] where adoption of PETs brought up feelings of paranoia or concerns suspicion that pushed against widespread adoption of PETs. Social identity signals are known to be used by groups to tell a story of that group (such as clothing and stickers) and these signals have been shown to extend to technology choices by Smaldino and others [69, 70]. Identity signals (including technology choices) inform observers about group membership and guide social cooperation or exclusion. They show that certain identity signals may be avoided with groups delaying or suppressing adoption if a technology is perceived as associated with an outgroup. In our setting, we may interpret intentional avoidance of a PET in this light, and certainly this sentiment was made explicit by Group 11. This adds to evidence of the unfortunate stigma often associated with PETs, most notably with Tor and its association with criminal use despite much broader use [17, 32], and commented on by activists in Brough et al.'s study with an arrestee using the lack of Signal on their phone to denote non-affiliation. On the other hand, the activists in Brough et al.'s study also comment on the need to use PETs to "avoid the judgement" of their fellow activists, signaling belonging and Ghoshal and Bruckman, in an ethnographic study of a grassroots organization, find that activists are drawn to technology that reflects the sociotechnical aspects of their groups' ideological values even when members struggled to use the technology [33].

For collaborative technology, obtaining buy-in from the entire group is key to success in private communication. This does not necessarily require buy in from the entire group on the efficacy of a particular PET, but establishing agreement on adoption as well as proper security culture is essential. Several of our participants, similar to those studied by Gaw et al. [31], expressed doubt that they would be targeted by either corporate or government law enforcement and additionally had varying levels of trust in the promises of PETs. This highlights that users are not only interacting with the technical and usability limitations of a piece of technology, but the sociotechnical as well. These sociotechnical obstacles may leave a hole in a group's threat model, leaving them vulnerable to an adversary. How does a user determine which data is sensitive enough to secure? Even if a threat assessment of current adversaries is accurate, in that the group is not currently a target, allowing for insecure practices of some communication and not others can either leave the group open to human error or a misalignment in judgment, and thus a loss of intentionality around their group's privacy in the context of their organizing.

6.5 Limitations

Like all research, this work is not without its limitations. This work is first and foremost, exploratory. We sought to understand how social movement groups frame their technology decisions in regards to security and privacy, and doing so required an open-ended approach. This, by nature of richer qualitative observations, results in an exploration of a number of cases that is deeper than it is

broad. Nonetheless, even within this framing there are constraints worthy of discussion.

As indicated already, our recruitment was limited to groups that are politically left-of-center. Direct-action activism often includes civil disobedience and understandably groups who engage in these activities may be less willing to discuss these activities with untrusted individuals, an additional complication on top of existing challenges to social movement recruitment [48]. Maintaining our trust with social movement groups (which takes time to establish and nurture) is prohibitive to collecting data from "both sides." Most participants agreed to participate based on an existing level of trust and that the research would be of use the social movement community. Our ability to speak to these often unreachable groups is in large part a product of carefully managing our relationships with activists to reassure them that we are engaging in good faith. Including observation or participation from opposing groups may betray this trust, and alienate the existing relationships with our participating groups.

This sample is also restricted to those participating in social movements based in the United States. The United States has specific political dynamics, including discourse specific to the countries' history and certain legal affordances (and restrictions) not necessarily replicable in other countries. It was already difficult with our resources to reach the groups highlighted here. The ability to sample enough groups from a variety of different geographical locations would require time and resources to understand political dynamics, establish trust networks, and legal council to navigate sensitive data collection. This is a common limitation of qualitative work, and thankfully we are seeing some geographical breadth in social movement privacy research with studies in the UK [12], Hong Kong [3], and Sudan [19].

These limitations are common to qualitative research. However, despite the limitations, we believe the themes that we find are relevant to understanding the rich and nuanced ways that social movement activism in similar political climates engage with information and communications technologies with regards to privacy. We took care to intentionally diversify our sample to include bureaucratic and grassroots groups and groups of different scales, missions and tactics. We are most confident in our findings applying to other left-wing social movements, though prior research has found that activists on both sides of the political spectrum have similar attitudes towards privacy and surveillance [2].

QCA, used to organize our findings, can be sensitive to case choice, condition selection, and calibration thresholds for determining whether a condition is 0 or 1. To manage this, we included many cases and intentionally sought variation among them. We also carefully matched our conditions and calibration to the theoretical literatures in both sociology and computer science. However, QCA treats all conditions as static in their relation to the outcome, so there is a reasonable critique that it remains difficult to tease out if there is a temporal order to conditions, where perhaps conditions must come in a specific order to be associated with the outcome. It is possible that some of our conditions have temporal dependency and would be something to consider in future work [47].

7 Conclusion and recommendations

We have identified that *group structures* that support adopting privacy practices, namely an informal organization and access to technical help, and an *environment* that warrant privacy protections, namely engaging in risky activism and having concern about surveillance, both correlate with making intentional privacy decisions. We also find these two situations to be correlated with one another (in that many groups are described by both suitable group structures and environment) and to be correlated strongly with adoption of PETs.

Based on our examined themes, we have several recommendations for the PETs development and deployment community. Feature availability and ease-of-use or learnability is still important for removing barriers to adopting PETs over mainstream applications. Social movement participants adopt information flow practices from school and work where privacy is not necessarily prioritized. Activists adopt technologies that they use elsewhere in life (such as collaborative editing and internet forms) to make their organizing work more efficient. Replicating the features of these tools while ensuring rigorous privacy of information while maintaining ease of use, we expect, will be a constant task for the PETs community.

A technically-minded group member or advisor plays a strong role in the adoption of PETs. This highlights the benefit that privacy advocates could bring to movements by developing and supporting trusted group "techies." Education is important. We find that a lack of training in digital privacy is correlated with not making intentional privacy decisions, and identify this as positive evidence to justify the work of privacy trainers. We view this as complimentary to development of "techies" as it may improve adoption and privacy practices for larger or more hierarchical organizations by reaching their decision-makers.

Groups see the adoption of particular technologies as a signal of their mission. PETs need to be mindful of branding and how their use is viewed by the public. We find that focusing on intention opened the door to understanding privacy practices that users adopt and adapt to, such as their organizational challenges and practicing of security culture which may instruct how they use technology rather than simply what technology they use. From a practical perspective, focusing on intention also allowed us to study the themes arising from a thirteen groups that engaged with PETs along a highly varied spectrum. While we do not diminish the importance of adoption to privacy, focusing on intent helps to open the door to understanding the pathways to privacy before focusing on the barriers of the technology. Further, with current technologies, it is unreasonable to expect even those with privacy intentions to forgo un-encrypted platforms altogether. For social movements in particular, there are certain aspects of organizing that must be done on public platforms, and there should be support for safely and appropriately operating on these platforms. Recommending which precautions should be taken on which communication channels may be more useful to these users than simply suggesting that they abstain from insecure platforms altogether.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1915768.

References

[1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 137–153. https://doi.org/10.1109/SP.2017.65

[2] Sheetal D Agarwal, Michael L Barthel, Caterina Rost, Alan Borning, W. Lance Bennett, and Courtney N Johnson. 2014. Grassroots Organizing in the Digital Age: Considering Values and Technology in Tea Party and Occupy Wall Street. *Information, Communication & Society* 17, 3 (2014), 326–341.

[3] Martin Albrecht, Jorge Blasco, R. Jensen, and Lenka Marekov'a. 2021. Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong. In *Proc. of USENIX Security Symposium*. https://www.semanticscholar.org/paper/Collective-Information-Security-in-Large-Scale-the-Albrecht-Blasco/c8135211f4dd4ce21c832481ec9f96eac26cc8d9

[4] Thalia Beaty and Farnoush Amiri. 2024. House passes bill that would allow Treasury to target nonprofits it deems to support terrorism. *AP News* (Nov. 2024). https://apnews.com/article/nonprofit-bill-terrorism-treasury-trump-aclu-ac88da656ea0d5cf8deb2e7bd045c1a4

[5] Kathleen M. Blee and Verta Taylor. 2002. Semi-Structured Interviewing in Social Movement Research. In *METHODS OF SOCIAL MOVEMENT RESEARCH*. 92–117.

[6] Camilla Borgna. 2016. Multiple Paths to Inequality. How Institutional Contexts Shape the Educational Opportunities of Second-Generation Immigrants in Europe. *European Societies* 18, 2 (March 2016), 180–199. https://doi.org/10.1080/14616696.2015.1134801

[7] Elizabeth Borland. 2008. Social movement organizations and coalitions: Comparisons from the women's movement in Buenos Aires, Argentina. In *Research in Social Movements, Conflicts and Change*, Patrick G. Coy (Ed.). Vol. 28. Emerald Group Publishing Limited, 0. https://doi.org/10.1016/S0163-786X(08)28003-1

[8] Glencora Borradaile and Kelsy Kretschmer. 2017. Training the Motivated: Digital Security for Activists. In *Poster at 13th Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA.

[9] Glencora Borradaile, Kelsy Kretschmer, Michele Gretes, and Alexandria LeClerc. 2021. The Motivated Can Encrypt (Even with PGP). *Proceedings on Privacy Enhancing Technologies* 2021, 3 (July 2021), 49–69. https://doi.org/10.2478/popets-2021-0037

[10] Hilary Boudet, Leanne Giordono, Chad Zanocco, Hannah Satein, and Hannah Whitley. 2020. Event attribution and partisanship shape local discussion of climate change after extreme weather. *Nature Climate Change* 10, 1 (Jan. 2020), 69–76. https://doi.org/10.1038/s41558-019-0641-3

[11] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. 2021. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–18. https://doi.org/10.1145/3411764.3445061

[12] Mikaela Brough, Rikke Bjerg Jensen, and Martin R. Albrecht. 2025. On the Virtues of Information Security in the UK Climate Movement. 5091–5110. https://www.usenix.org/conference/usenixsecurity25/presentation/brough

[13] Alleen Brown and Alice Speri. 2020. Facebook Warrant Targeting Student Journalists in Puerto Rico Prompts Fears of Political Surveillance. https://theintercept.com/2020/01/19/puerto-rico-university-protests-facebook-surveillance/

[14] Victoria Carty and Francisco G. Reynoso Barron. 2019. Social Movements and New Technology: The Dynamics of Cyber Activism in the Digital Age. In *The Palgrave Handbook of Social Movements, Revolution, and Social Transformation*, Berch Berberoglu (Ed.). Springer International Publishing, Cham, 373–397. https://doi.org/10.1007/978-3-319-92354-3_16

[15] Brian X. Chen. 2018. Worried About the Privacy of Your Messages? Download Signal. *The New York Times* (March 2018).

[16] Francesca Colli. 2024. The Old and the Young: Configurational Niches Amongst Dutch Climate Civil Society Organisations. *Voluntas: International Journal of Voluntary and Nonprofit Organizations* 35, 2 (April 2024), 303–314. https://doi.org/10.1007/s11266-023-00594-8

[17] Ben Collier. 2021. Infrastructural Power: Dealing with Abuse, Crime, and Control in the Tor Anonymity Network. In *Cybercrime in Context: The human factor in victimization, offending, and policing*, Marleen Weulen Kranenbarg and Rutger Leukfeldt (Eds.). Springer International Publishing, Cham, 283–301. https://doi.org/10.1007/978-3-030-60527-8_16

[18] Kristine Coulter and David S. Meyer. 2015. High profile rape trials and policy advocacy. *Journal of Public Policy* 35, 1 (2015), 35–61. https://www.jstor.org/stable/43864134

[19] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas. 2021. Defensive Technology Use by Political Activists During the Sudanese Revolution. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 372–390. https://doi.org/10.1109/SP40001.2021.00055

[20] Simon Davis-Cohen. 2018. The Justice Department Helped a County Prosecutor Target the Facebook Records of Anti-Pipeline Activists. https://theintercept.com/2018/01/14/facebook-warrant-pipeline-protest-whatcom-county-justice-department/

[21] Ron Deibert. 2014. *Communities @ Risk: Targeted Digital Threats Against Civil Society*. University of Toronto.

[22] Roger Dingledine and Nick Mathewson. 2006. Anonymity Loves Company: Usability and the Network Effect. *WEIS* (2006), 12.

[23] Adrian Dusa. 2019. *QCA with R: A Comprehensive Resource*. Springer International Publishing. https://doi.org/10.1007/978-3-319-75668-4

[24] Jennifer Earl. 2018. Technology and Social Media. In *The Wiley Blackwell Companion to Social Movements*. John Wiley & Sons, Ltd, 289–305. https://doi.org/10.1002/9781119168577.ch16 Section: 16 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119168577.ch16.

[25] Jennifer Earl, Thomas V. Maher, and Jennifer Pan. 2022. The digital repression of social movements, protest, and activism: A synthetic review. *Science Advances* 8, 10 (March 2022), eabl8198. https://doi.org/10.1126/sciadv.abl8198

[26] Susan Fahey and Pete Simi. 2018. Pathways to violent extremism: a qualitative comparative analysis of the US far-right. *Dynamics of Asymmetric Conflict* 12 (Dec. 2018), 1–25. https://doi.org/10.1080/17467586.2018.1551558

[27] Simone Fischer-Hübner and Farzaneh Karegar. 2024. Overview of Usable Privacy Research: Major Themes and Research Directions. In *The Curious Case of Usable Privacy: Challenges, Solutions, and Prospects*, Simone Fischer-Hübner and Farzaneh Karegar (Eds.). Springer International Publishing, Cham, 43–102. https://doi.org/10.1007/978-3-031-54158-2_3

[28] Michel Foucault. 1977. *Discipline and punish: The birth of the prison* (1st american ed ed.). Pantheon Books, New York. OCLC: 3328401.

[29] Sheera Frenkel and Mike Isaac. 2026. Homeland Security Wants Social Media Sites to Expose Anti-ICE Accounts. *The New York Times* (Feb. 2026). https://www.nytimes.com/2026/02/13/technology/dhs-anti-ice-social-media.html

[30] Simson Garfinkel and Robert Miller. 2005. Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. In *Proceedings of the First Symposium on Usable Privacy and Security*. ACM, 13–24.

[31] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 591–600.

[32] Adam K. Ghazi-Tehrani. 2023. Mapping Real-World Use of the Onion Router. *Journal of Contemporary Criminal Justice* 39, 2 (May 2023), 239–256. https://doi.org/10.1177/10439862231157553

[33] Sucheta Ghoshal and Amy Bruckman. 2019. The Role of Social Computing Technologies in Grassroots Movement Building. *ACM Trans. Comput.-Hum. Interact.* 26, 3 (June 2019), 18:1–18:36. https://doi.org/10.1145/3318140

[34] Marco Giugni and Alessandro Nai. 2013. Paths towards Consensus: Explaining Decision Making within the Swiss Global Justice Movement. *Swiss Political Science Review* 19, 1 (March 2013), 26–40. https://doi.org/10.1111/spsr.12016

[35] Helen Nissenbaum. 2009. *Privacy in Context*. Stanford University Press. https://www.sup.org/books/law/privacy-context

[36] Amir Herzberg and Hemi Leibowitz. 2016. Can Johnny Finally Encrypt?: Evaluating E2E-encryption in Popular IM Applications. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust - STAST '16*. ACM Press, Los Angeles, California, 17–28. https://doi.org/10.1145/3046055.3046059

[37] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 327–346.

[38] Larry W. Isaac, Jonathan S. Coley, Daniel B. Cornfield, and Dennis C. Dickerson. 2020. Pathways to Modes of Movement Participation: Micromobilization in the Nashville Civil Rights Movement. *Social Forces* 99, 1 (2020), 255–280. https://www.jstor.org/stable/26931929

[39] Laura Jarrett. 2017. Judge OKs fed request for Trump protester data. http://www.cnn.com/2017/08/24/politics/dreamhost-disruptj20-search-warrant-granted/index.html

[40] Sayash Kapoor, Matthew Sun, Mona Wang, Klaudia Jazwinska, and Elizabeth Anne Watkins. 2022. Weaving Privacy and Power: On the Privacy Practices of Labor Organizers in the U.S. Technology Industry. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2 (Nov. 2022), 473:1–473:33. https://doi.org/10.1145/3555574

[41] Priya C. Kumar, Michael Zimmer, and Jessica Vitak. 2024. A Roadmap for Applying the Contextual Integrity Framework in Qualitative Privacy Research. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (April 2024), 1–29. https://doi.org/10.1145/3653710

[42] Ada Lerner, Eric Zeng, and Franziska Roesner. 2017. Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists. In *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 385–400. https://doi.org/10.1109/EuroSP.2017.41

[43] Kirsten Martin, , and Katie Shilton. 2016. Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society* 32, 3 (May 2016), 200–216. https://doi.org/10.1080/01972243.2016.1153012 Publisher: Routledge _eprint: https://doi.org/10.1080/01972243.2016.1153012.

[44] Doug McAdam. 2012. *Putting social movements in their place : explaining opposition to energy projects in the United States, 2000-2005*. Cambridge ; New York : Cambridge University Press. http://archive.org/details/puttingsocialmov0000mcad

[45] Doug McAdam, Hilary Schaffer Boudet, Jennifer Davis, Ryan J. Orr, W. Richard Scott, and Raymond E. Levitt. 2010. "Site Fights": Explaining Opposition to Pipeline Projects in the Developing World. *Sociological Forum* 25, 3 (Aug. 2010), 401–427. https://doi.org/10.1111/j.1573-7861.2010.01189.x
[46] Susan E. McGregor, Elizabeth Anne Watkins, Mahdi Nasrullah Al-Ameen, Kelly Caine, and Franziska Roesner. 2017. 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*. 505–522.
[47] Patrick Mello. 2021. *Qualitative Comparative Analysis: An Introduction to Research Design and Application, QCA and Its Critics (Chapter 9)*. 172–187.
[48] Christine Ogan, Giglou , Roya Imani, , and Leen d'Haenens. 2017. Challenges of conducting survey research related to a social protest movement: Lessons learned from a study of Gezi protests involving the Turkish diaspora in three European countries. *The Information Society* 33, 1 (Jan. 2017), 1–12. https://doi.org/10.1080/01972243.2016.1248615 Publisher: Routledge _eprint: https://doi.org/10.1080/01972243.2016.1248615.
[49] Vinay Patel. 2021. Racially Motivated Spying Pretext: Challenging the FBI's New Regime of Racialized Surveillance. *Columbia Journal of Race and Law* 11, 1 (March 2021), 1–31. https://journals.library.columbia.edu/index.php/cjrl/article/view/8045 Number: 1.
[50] Jon Penney. 2021. *Understanding Chilling Effects*. SSRN Scholarly Paper ID 3855619. Social Science Research Network, Rochester, NY. https://papers.ssrn.com/abstract=3855619
[51] Will Potter. 2011. *Green is the new red: An insiders account of a social movement under siege*. City Lights Books, San Francisco.
[52] Charles D. Raab. 1998. The Distribution of Privacy Risks: Who Needs Protection? *The Information Society* 14, 4 (Nov. 1998), 263–274. https://doi.org/10.1080/019722498128719 Publisher: Routledge _eprint: https://doi.org/10.1080/019722498128719.
[53] Charles Ragin and Sean Davey. 2016. Fuzzy-Set/Qualitative Comparative Analysis. Department of Sociology, University of California..
[54] Charles C. Ragin. 2000. *Fuzzy-Set Social Science*. University of Chicago Press.
[55] Charles C. Ragin. 2008. *Redesigning Social Inquiry: Fuzzy Sets and Beyond* (47116th edition ed.). University of Chicago Press, Chicago.
[56] Charles C. Ragin and Peer C. Fiss. 2016. *Intersectional Inequality: Race, Class, Test Scores, and Poverty*. University of Chicago Press.
[57] Kati Rantala and Eeva Hellström. 2001. Qualitative comparative analysis and a hermeneutic approach to interview data. *International Journal of Social Research Methodology: Theory & Practice* 4, 2 (2001), 87–100. https://doi.org/10.1080/136455701750158840
[58] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. 2020. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *29th USENIX Security Symposium (USENIX Security 20)*. 89–108.
[59] Benoît Rihoux and Charles C. Ragin. 2008. *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*. SAGE Publications.
[60] Benoît Rihoux, Priscilla Álamos Concha, Damien Bol, Axel Marx, and Ilona Rezsöhazy. 2013. From Niche to Mainstream Method? A Comprehensive Mapping of QCA Applications in Journal Articles from 1984 to 2011. *Political Research Quarterly* 66, 1 (March 2013), 175–184. https://www.proquest.com/docview/1445173788/abstract/7D45D69CBA7B4D76PQ/1 Num Pages: 10.
[61] Deana A. Rohlinger and Leslie Bunnage. 2017. Did the Tea Party Movement Fuel the Trump-Train? The Role of Social Media in Activist Persistence and Political Change in the 21st Century. *Social Media + Society* 3, 2 (April 2017), 2056305117706786. https://doi.org/10.1177/2056305117706786
[62] Norat Roig-Tierno, Tomas F. Gonzalez-Cruz, and Jordi Llopis-Martinez. 2017. An Overview of Qualitative Comparative Analysis: A Bibliometric Analysis. *Journal of Innovation & Knowledge* 2, 1 (Jan. 2017), 15–23. https://doi.org/10.1016/j.jik.2016.12.002
[63] Leah Namisa Rosenbloom. 2022. Activists Want Better, Safer Technology. https://doi.org/10.48550/arXiv.2209.01273 arXiv:2209.01273 [cs].
[64] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. 2015. Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client. *arXiv preprint arXiv:1510.08555* (2015). arXiv:1510.08555
[65] Jen Schradie. 2018. The Digital Activism Gap: How Class and Costs Shape Online Collective Action. *Social Problems* 65, 1 (Feb. 2018), 51–74. https://doi.org/10.1093/socpro/spx042
[66] Jason Seawright and John Gerring. 2008. Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options. *Political Research Quarterly* 61, 2 (June 2008), 294–308. https://doi.org/10.1177/1065912907313077
[67] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J. Hyland. 2006. Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software. In *Symposium On Usable Privacy and Security (SOUPS)*. 3–4.
[68] Siena Anstis and Ronald J. Deibert. 2025. Silenced by Surveillance: The Impacts of Digital Transnational Repression on Journalists, Human Rights Defenders, and Dissidents in Exile. (Feb. 2025). https://perma.cc/23RN-UX6V
[69] Paul E. Smaldino. 2022. Models of Identity Signaling. *Current Directions in Psychological Science* 31, 3 (June 2022), 231–237. https://doi.org/10.1177/09637214221075609
[70] Paul E. Smaldino, Marco A. Janssen, Vicken Hillis, and Jenna Bednar. 2017. Adoption as a social marker: Innovation diffusion with outgroup aversion. *The Journal of Mathematical Sociology* 41, 1 (Jan. 2017), 26–45. https://doi.org/10.1080/0022250X.2016.1250083 _eprint: https://doi.org/10.1080/0022250X.2016.1250083.
[71] Alrik Thiem and Adrian Duşa. 2013. Boolean Minimization in Social Science Research: A Review of Current Software for Qualitative Comparative Analysis (QCA). *Social Science Computer Review* (March 2013). https://doi.org/10.1177/0894439313478999
[72] Donald Trump. 2025. Designating Antifa as a Domestic Terrorist Organization. Executive Order No. 2025-18709, 90 Fed. Reg. 46317. https://www.federalregister.gov/d/2025-18709.
[73] J. Warren, J. Wistow, and C. Bambra. 2013. 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 (May 2013), 126–133. https://doi.org/10.1093/pubmed/fdt047
[74] Alma Whitten and J.D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *8th USENIX Security Symposium*.
[75] Phil Zimmerman. 1999. Why I Wrote PGP. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

A Qualitative Comparative Analysis

Interview data was interpreted using Qualitative Comparative Analysis (QCA). As the name implies, QCA is a qualitative method to organize themes identified in observed cases, not a statistical method. Qualitative Comparative Analysis provides a structure to qualitative observations that allows for better reproducibility and a way to organize data interpretations. QCA as a method was developed to infer causal factors linked to a targeted outcome. This methodology was designed to be implemented on smaller sample sizes, with individual observed cases being very detailed [55]. When attempting to correlate factors related to a hypothesized outcome, qualitative analysis, such as QCA, allows for a more nuanced and holistic interpretation of the many factors that may interplay with each other. The method was originally developed to analyze nation states and their various attributes, but has since been generalized to a number of different contexts [6, 56, 62, 73], including similar research on social movements [9, 34, 45].

A.1 Crisp-Set and Fuzzy-Set QCA

QCA uses boolean minimization over observed cases to determine which combinations of conditions correlate with an identified outcome. A specific set of conditions is referred to as a *combination*, with a *pathway* referring to specific combinations correlated with an outcome. In this research, each social movement group is one *case*. In Crisp-Set QCA, conditions are binarized and correlated with a binary outcome. The minimization algorithm (Quine-McCluskey as used here, or an equivalent [23]) can shed light on combinations of factors that appear in correlation with a defined outcome for each case observed. The end result being a disjunctive Boolean formula of minimum size that correlates combinations of conditions to the outcome, based upon the observed cases that were input. Alternative forms, such as "Fuzzy-Set" QCA, defines values on a spectrum between 0 and 1 [53]. This allows capture of conditions that do not fit well into a strict binary category. For the analysis of the data collected here, crisp-set QCA has been able to describe the conditions identified without the need for the ambiguity granted by Fuzzy-Set QCA.

A.2 Pathways

QCA outputs formula(s) that combine observed conditions to determine which correlate with the positive outcome. Pathways are not necessarily an exclusive explanation toward an outcome. The resulting pathways provide a grouping of the cases: cases that satisfy a given pathway all share a particular combination of conditions. This provides more structured organization of recurring themes in the recorded data. A case may possess more than one combination of conditions that result in a pathway to the defined outcome. This reflects traditional qualitative analysis, and leaves room for multiple possible interpretations for an observed phenomena.

Causality vs Correlation. The original QCA methodology frames the connection between the input factors and the outcome variable as "causal", we chose to represent this relationship as "correlational" for a few reasons. First, we leave the interpretation of the QCA pathways somewhat open-ended and leave room for multiple explanations, making it difficult to truly narrow down "causality" in a strict sense. We also thought correlational to be more accurate a term for an audience familiar with quantitative methods in which causality is usually an extremely strong claim, and the nuanced use of causality may not translate as well for this audience. Instead, we refer to the output as correlational pathways between conditions and outcome.

Pathways are considered asymmetric between the positive and negative outcome. Meaning it cannot be assumed that negating the conditions in a pathway to the positive outcome will automatically lead to the negative outcome. Instead, QCA must be run once to determine the combination of conditions that infer the positive outcome, and then repeat analysis on the negation of the outcome to determine the unique pathways to the negative outcome [59]. Identical analysis is performed but with the binary outcome flipped.

A.2.1 Solution Types. There are different approaches in how QCA determines a formula. As the method uses a binary truth table, the total number of permutations in the table is 2^k, where k is the number of conditions being measured. For a table with more than a small number of conditions, it becomes impractical and sometimes impossible to find a case that fits every possible combination of conditions. Not only because of the resources needed for such a large sample, but also due to the fact that some combinations of conditions may not logically occur in real life.

When viewing a complete 2^k truth table of QCA cases, any combination of conditions that is not represented by an observed case is referred to as a *remainder*. Remainders are treated as unknowns, lacking a recorded case for an observation. Any cases in which identical combinations of conditions result in opposite outcomes (one observation resulting in an outcome of 0/False and a different observation resulting in a 1/True) are referred to as *contradicting* cases. For instance, this study has measured a combination resulting a conflicting case, as shown in row 9 of Table 4. A conflicting outcome can be treated as either positive or negative if at least 70% of the cases are positive. Depending on the selected method of arriving at a QCA solution, remainders and conflicting cases may be treated in three different ways [71]. The following solution descriptions refer to inferring the positive outcome, but identical processes are performed for the negative outcome.

Conservative The conservative solution is the most strict: it restricts itself to utilizing only cases which have been observed in the data. Any remainders, as well as cases with a negative outcome and conflicting cases are treated as though they were negative (set to 0). This solution does not make any assumptions about cases that have not been measured, and thus the output is often complex and utilizes many very specific combinations of conditions.

Parsimonious The parsimonious solution creates formula that are based on the observed cases, but is flexible with the remainder cases. All of the combinations with negative outcomes, as well as the conflicting outcomes, are treated as negative but all remainders are allowed to be set to either true or false during the minimization. The flexibility allows the creation simpler solutions that are not bound to the exact conditions sampled. Rather than restricting combinations of conditions to only those in observed cases, we can infer which conditions are most relevant. In practice, these formulas allow for more intuitive interpretations because they must not satisfy an explanation for all present conditions: we can extend our qualitative analysis onto currently unobserved, but easily imaginable, combinations of conditions.

Intermediate The intermediate solution allows the researcher to assign weight to conditions, and pick and choose which remainders to include in the analysis [55]. It is considered to be a compromise between the conservative and parsimonious solution, and relies heavily on the discretion of the researcher.

This work uses the parsimonious solution. The conservative solution can become too restrictive with a small number of cases with many conditions, resulting in long and complex formulas. The intermediate solution trades the aforementioned robustness in favor of the researchers interpretations. We find the parsimonious solution is the easiest to explain mathematically and lends more to the reproducibility in the combinations of conditions.

A.3 Consistency & Coverage

Consistency and coverage are metrics that convey the fit of the pathways to the cases observed in the sample. The fraction of the total cases that satisfy a logical formula with a positive outcome is referred to as the *consistency*. Pathways inferring a positive outcome can be relaxed to include some small fraction of negative outcomes. In this case, the consistency metric is used to convey how much a pathway has been relaxed. Usually, consistency scores which meet a threshold of 0.8 or higher are desired for analysis [55]. We achieved perfect consistency (1.0) for the pathways returned in this analysis. In simpler terms, all of the cases that are covered by pathway found by QCA are consistent with the combination of conditions necessary for the outcome.

The fraction of cases with a positive outcome whose conditions satisfy the formula is referred to as the *coverage*. Unlike consistency, there is not a widely used threshold for coverage scores. In general, a logical formula with a higher coverage score is considered more relevant to explaining the occurrence of an outcome. The pathways for both positive and negative outcome coverage of 0.85 and 0.95, respectively.

B Full set of examined conditions

In addition to the conditions examined in Section 4.2, we included two additional conditions, CHAP and HARM, for QCA to potentially use.

CHAP Coded as 1 if the group is a chapter that has an affiliated parent that has authority over the local chapter. This was usually discussed by the participant in response to the ELEC question. Some of the groups interviewed were large national groups and it was easy to confirm from publicly available information if they were a chapter of a larger group. Groups sometimes affiliate or even adopt the same name, but do not report directly to a parent. For example, groups 1a and 1b in our sample operate as independent entities and thus CHAP = 0. They share an affiliation but do not report to a higher organizing authority.

HARM Coded as 1 if the research team determined that the group engages in activism that could directly result in bodily harm to themselves. This could be from confrontations with law enforcement or opposing groups.

QCA did not use these conditions in the pathways for explaining INTENT. Essentially, these conditions were not useful for organizing the themes we explore. We interrogated other factors, such as group size, but these were found to be non-correlative to the outcome. A full table of these values is provided in Table 5.

Table 5: Truth Table of Observed Conditions

Conditions							Outcome	Groups
ELEC	CHAP	RISK	HARM	TRAIN	TECHIE	SURV	INTENT	
0	0	1	1	0	1	1	1	2,19,20
0	0	1	1	1	1	1	1	9,10
0	0	0	0	0	1	1	1	7
0	0	0	0	1	1	0	1	11
0	0	1	0	0	1	1	1	21
0	0	1	0	1	1	1	1	22
1	1	0	0	1	1	0	1	5
1	1	1	0	0	0	1	1	3
1	0	0	0	1	1	1	conflict	1a,1b,4
1	1	0	0	0	1	0	0	13,14b,15b,15c,15d,15e,16e
1	1	0	0	0	0	0	0	14a,15a,16a,16b,16c,16d,16f,18
0	0	0	0	0	0	0	0	12
0	1	1	1	0	0	0	0	17
1	0	0	0	0	1	0	0	8
1	0	0	0	0	1	1	0	6

C Instrument

The following script was used for all interviews conducted. The questions were used as starting points, with clarifying questions asked at the discretion of both the interviewer and interviewee. Questions were skipped (as indicated by instructions in [square brackets]) based on responses from the interviewee. The analysis reported above examines a subset of the questions outlined below.

Thank you for agreeing to be interviewed. We are interested in how social movement groups understand and make decisions about their technology and security needs. We will ask questions about how your group is structured, how you decide which technologies to use, and your concerns, if any, about digital security. The data collected will be used to inform best practices for security training for community groups. Your participation is completely voluntary and you may skip any questions or stop at any time. Your personal identity and your group's identity will be kept confidential in any presentation or publication of our findings. In order to be in this study you must be of legal age to consent, which is 18 in most states.

Before we proceed with the interview, we need you to confirm:

(1) Are you at least 18 years old, or of legal age to consent? YES NO
(If you are not yet 18 years, or of legal age to consent old, we will stop the interview here and delete any information collected up to this point)
(2) Do you agree to have the interview audio recorded? YES NO
(If no, we will continue with the interview with a study staff member taking notes)

We are going to start with some basic information about you and [Primary Group].

(3) Other than [Primary Group], how many groups are you a part of?
(4) About how many people would you say are a part of [Primary Group]?
(5) How do new members join the group? [Just start showing up? Need to know someone? Other rules for joining?]
(6) Do you have formal leaders, like elected positions?
  (a) If yes, what are the positions you elect?
  (b) What is the process for selecting them? [Regular elections? Terms?]
(7) Do you have informal leaders, like people who regularly take the initiative in the group?
  (a) If yes, why do you think they fill that role? [personal characteristics; specialized skills; founder; other reasons?]
(8) We'd like to know how work is divided up in your group. Is there one person or set of people who do most of the planning and coordinating, or are the jobs all divided equally?
(9) How does your group make decisions? [If people disagreed about something, how would your group decide what to do?]
(10) How would you describe the demographics of your group's leaders? [gender, race, age, education, other important characteristics?]
(11) How would you describe the membership's demographics? [gender, race, age, education, other important characteristics?]
(12) Do you spend time together with people in your group socially, outside of movement work?

Now we are going to ask about the kinds of technology your group uses.

(13) Would you say you are comfortable or uncomfortable talking about the technology that your group uses?
  (a) [If uncomfortable] Are you uncomfortable because of privacy, because of lack of expertise, or because of something else?
(14) Do you meet in person? How often?
(15) Are your meetings ever held remotely or online, like video conferencing or conference calls?
(16) [If yes to meeting remotely] How often do you meet remotely?
(17) What technologies are your members of your group currently using for the following functions? It's ok to answer "I don't know".
  (a) Plan the group's events _____
  (b) Collaboratively edit group documents _____
  (c) Schedule group meetings _____
  (d) Communicate between meetings among group members _____
  (e) Communicate or plan with other groups/public _____
  (f) Store group information or documents _____
  (g) Run programs or apps (Operating system) [e.g. Android, iPhone, Mac, Windows] _____
  [If more than one in a category] Of those, which is the one you use the most frequently? [Circle the one they use most frequently from the list above]

Now we're going to go through the technologies that your group uses the most, and I will ask you some questions about these technologies.

TECH: _____

(18) Why did your group started using _____ ?
  [easy for me to use, easy for others to use, free to use, secure, use at work, everyone uses it, no other choice, new functionality, replacing, interacting with a new group]
(19) Who in the group initially introduced the idea of _____ ?
(20) Did your group need help in getting started using _____ ?
(21) Did you consider any other alternatives to _____? (Other tech that has the same functionality?)
  [have them name what they can remember]
  [If yes] Why did you decided against those other possibilities?
(22) Do you or do you know of anyone in your group who makes sure these technologies are up to date? Or are they set to auto-update?
(23) Now we are going to ask you how secure you consider these technologies to be.
  [Provide the list again to them]

(a) _____	Very Secure	Medium Secure	Not Secure	Don't Know
[Why?]				
(b) _____	Very Secure	Medium Secure	Not Secure	Don't Know
[Why?]				
(c) _____	Very Secure	Medium Secure	Not Secure	Don't Know
[Why?]				
(d) _____	Very Secure	Medium Secure	Not Secure	Don't Know
[Why?]				
(e) _____	Very Secure	Medium Secure	Not Secure	Don't Know
[Why?]				
(f) _____	Very Secure	Medium Secure	Not Secure	Don't Know
[Why?]				
(g) _____	Very Secure	Medium Secure	Not Secure	Don't Know
[Why?]				

(24) Have you sought out information about making your group information and/or communication secure?
  Can you tell me about that/those efforts?
  [Prompts: Formal, informal, Internet, self-guided; May be multiple efforts, list as many as come up]
(25) [If formal training is mentioned]:
  (a) Can you tell me what topics or technologies it covered?
  (b) When did you get this training [dates/categories like this year, last year, etc.]
  (c) During the training, how comfortable were you with the information?
  (d) After the training, did you implement the information in your personal use?
  (e) Did the group implement the information from the training?
    [If yes, go to 'f'.]
    [If no, go to 28.]
  (f) What changes did the group make?

(g) What are some things you think helped the group embrace it?
[prompts: leaders/ key members insisted; everyone liked it]
(h) How did the people in the group respond to the new secure communication technology? Was it positively received, negatively received? Why do you think this?
(i) Have any challenges with the technology/ies come up?
(j) Do you personally still use the technology? If not, why?
(k) Does your group still use it? If not, why?
(l) When did you stop?

(26) [If they did not implement the new technology:]
Why do you think your group decided against using it?
(27) Have you sought out any different secure technologies since you first received training on secure practices?
(28) If you were to increase your group's digital security, do you think it would change any of the ways you currently organize?
[If yes] How?

Motivations for Technology Decisions

(29) On a scale of 1 to 5, with 1 being not at all worried and five being very worried, how worried are you about the security of your group?
(30) Does anyone else in your group consistently worry about your group's security? If so, could you describe their demographic characteristics? [gender, race, age, education, other characteristics they consider important]
(31) Can you think of an example or examples of how this concern affected your group's decision-making?

Now we are going to ask about some basic information and definitions:

(32) In terms of the technology you use, how would you define security?
(33) How would you define encryption?
(34) Do you think of some kinds of encryption as better than others? Or all the same?
(35) When you think about a new technology, how do you decide if it is secure enough to feel safe using it?
(36) If you were uncertain about a technology your group uses, who or what would you ask for help?

We are going to close out the interview with some basic demographic information about you.

(37) What is your gender identity?
(38) What is your racial/ethnic identity?
(39) How old are you?

D Technologies in use

Tools listed below are those in use by at least 3 groups.

	⟵ Privacy-enhancing ⟶																
Group	Signal	Keybase	Cryptpad	Protonmail	Jitsi	Zoom	Twitter	Facebook	Instagram	Database	Email	Excel	Google Docs	Google Drive	Phone	Text Messaging
1a	-	-	-	-	-	-	-	●	-	-	●	-	●	-	●	-
1b	●	-	-	-	-	●	-	-	-	-	●	●	●	●	●	●
2	●	●	-	-	●	●	-	●	-	-	-	-	-	●	-	-
3	-	●	-	-	-	-	-	●	●	-	●	-	-	-	-	-
4	●	●	●	●	-	●	-	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	●	-	●	●	-	-	●	●	●
6	●	-	-	-	-	-	-	-	-	-	●	-	-	-	-	●
7	●	-	-	●	-	-	-	-	-	●	●	-	-	-	-	●
8	-	-	-	-	-	●	-	●	●	-	●	-	-	●	-	●
9	●	-	●	-	●	-	-	-	-	-	●	-	-	-	-	-
10	●	●	-	-	●	-	-	-	-	-	-	-	-	-	-	-
11	●	-	●	-	-	●	-	-	-	-	●	-	-	●	-	-
12	-	-	-	-	-	●	●	●	-	-	-	-	●	-	-	-
13	●	-	-	-	-	●	-	-	-	-	●	-	●	-	●	●
14a	-	-	-	-	-	●	-	-	-	-	●	-	-	●	-	●
14b	-	-	-	-	-	●	-	●	-	-	●	-	-	●	●	●
15a	-	-	-	-	-	●	-	●	-	-	●	-	-	●	-	-
15b	-	-	-	-	-	●	-	●	●	-	●	-	-	●	-	-
15c	-	-	-	-	-	●	-	-	-	●	●	●	-	●	-	-
15d	-	-	-	-	-	●	-	-	-	-	●	-	-	●	●	●
15e	-	-	-	-	-	●	-	-	-	-	●	●	-	●	●	-
16a	-	-	-	-	-	●	-	-	-	-	-	-	-	●	-	-
16b	-	-	-	-	-	●	-	●	-	-	●	-	-	●	-	●
16c	-	-	-	-	-	-	-	●	-	-	●	-	-	-	-	-
16d	-	-	-	-	-	●	●	●	●	-	●	-	-	●	-	●
16e	-	-	-	-	-	●	●	●	●	-	●	-	-	●	-	-
16f	-	-	-	-	-	●	●	●	-	-	●	-	-	●	-	-
17	-	-	-	-	-	●	-	●	-	-	●	-	-	-	-	-
18	-	-	-	-	-	●	●	●	●	-	●	-	-	●	-	-
19	●	-	-	-	-	-	●	●	-	-	-	-	-	-	-	-
20	●	-	●	-	-	-	●	●	-	-	-	-	-	-	●	●
21	●	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-
22	●	●	●	●	●	-	●	-	●	●	-	-	-	-	-	-
Count:	13	5	5	3	5	21	8	18	7	4	24	3	4	18	8	12