"A Reasonable Thing to Ask For": Towards a Unified Voice in Privacy Collective Action

Yuxi Wu, W. Keith Edwards, Sauvik Das
Georgia Institute of Technology
Atlanta, Georgia, USA

ABSTRACT

People feel concerned, angry, and powerless when subjected to surveillance, data breaches and other privacy-violating experiences with institutions (PVEIs). Collective action may empower groups of people affected by a PVEI to jointly demand redress, but a necessary first step is for the collective to agree on demands. We designed a sensitizing prototype to explore how to shepherd a collective to generate a unified set of demands for redress in response to a triggering PVEI. We found that collectives can converge on high-priority concerns and demands for redress, and that many of their demands indicated preferences for broad reform. We then gathered a panel of security and privacy experts to react to the collective's demands. Experts were dismissive, preferring incremental measures that cleanly mapped onto existing legal structures. We argue this misalignment may help uphold the power chasm between data-harvesting institutions and the individuals whose personal data they monetize.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; • **Human-centered computing → Social navigation**.

KEYWORDS

user privacy, collective action

ACM Reference Format:
Yuxi Wu, W. Keith Edwards, Sauvik Das. 2022. "A Reasonable Thing to Ask For": Towards a Unified Voice in Privacy Collective Action. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3491102.3517467

1 INTRODUCTION

While many Internet users are concerned about how large institutions collect and handle their personal data, they may feel powerless to effect change. For example, prior work has shown that users express concern, anger and frustration when they encounter privacy-violating experiences with institutions (PVEIs)—be it through investigative exposés of surveillance, as in the Snowden revelations [2, 5, 48], or through personal exposure to data breaches, like the Equifax breach [4, 58]. Yet, a 2019 Pew study found that over 80% of adults in the U.S. believed that they had little or no control over the data that corporations and the government collected, and that it was impossible to go through daily life without having data about themselves collected [10]. This tension—between workaday people's concerns over PVEIs and their perceived lack of agency to effect change—is indicative of a wider power chasm between data-aggregating institutions and the individual users whose data they collect and monetize.

How might we bridge this power chasm? One strategy that has been effective in other contexts is channeling the frustration of the dis-empowered masses into collective action—i.e., action taken by multiple people in pursuit of the same goal or collective good [38]—to demand redress. For example, in the Industrial Revolution, workers unionized, unilaterally agreeing to withhold labor from employers, tilting the balance of power toward workers and resulting in basic mainstays of modern society like minimum wages, the two-day weekend, and an 8-hour work day [55]. Importantly, prior to these worker victories, legal doctrines reinforced employer property rights over the ability of employees to organize [28]; regulatory efforts to support worker rights only came *after* sustained, collective effort. In short, history suggests that we cannot rely on existing legal structures alone to effect change in favor of people and at the expense of powerful institutions; a sustained, united public pressure must come first.

In the context of privacy, there is some evidence that this sort of collective action can work. For example, a 2017 petition signed by California residents was the origin of today's California Consumer Protection Act (CCPA). However, the CCPA was heavily financed and driven by a small team of three individuals; the collective primarily contributed signatures necessary for a ballot measure rather than substantive policy recommendations [9]. More attempts at privacy collective action have, thus far, fallen short of effecting real change: for example, a Change.org petition responding to the Cambridge Analytica scandal garnered nearly 180,000 signatures [35], but did not result in any material redress. Other vectors for expressing collective frustrations similarly result in little material change, e.g., voicing concerns and sharing information about PVEIs on online forums. This discrepancy begs the question: what causes collective action efforts in privacy to fail, and how can we improve their likelihood of success?

Shaw et al. [50] introduced a five-stage model for computer-supported collective action (CSCA) that can help diagnose why CSCA efforts fail: many such efforts fail because they skip over requisite stages in the model. These stages include: (1) Identifying a problem; (2) Generating, debating and selecting solutions; (3) Coordinating and preparing to take action; (4) Taking action; and, (5) Following up, documenting and assessing action taken. Adapting

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04…$15.00
https://doi.org/10.1145/3491102.3517467

Shaw et al.'s model to the context of online privacy collective action, Das et al. [17] note that existing CSCA efforts for privacy often skip stage (2): after identifying a problem, e.g., the Cambridge-Analytica scandal (stage 1), typically one or a small group of individuals draft a petition and solicit signatures (stage 3). What's missing is a structured gathering, debate and filtering of ideas from the collective that forms around an issue. Consequently, petitions are often not representative of the collective's concerns, nor do they necessarily represent the best ideas of that collective. In this paper, thus, we build upon Das et al.'s vision of privacy collective action — what they call *Privacy for the People* [17] — by focusing on how we might design a process that facilitates this structured gathering of ideas (stage 2). Specifically, we explore the following two research questions:

RQ1 Representation. Viral petitions authored by only a few can demotivate those who might not know or trust the original author(s), and can overshadow other ideas that better represent the collective's demands. *How can we mobilize collectives to move from amorphous discontent and anger toward specific, representative privacy demands?*

RQ2 Stewardship. Existing structures to interpret demands into actionable redress (e.g., filing class-action lawsuits, issuing FTC penalties) often require specialized expertise or access. *How do privacy experts view the privacy demands generated by a collective, and how might they be effective stewards for the collective in translating their demands into actionable recourse?*

First, to explore the *Representation* RQ, we designed a sensitizing concept based on Bernstein's Find-Fix-Verify (FFV) crowd programming pattern [12]. Sensitizing concepts are exemplary artifacts intended to inspire other designers to new possibilities beyond the specific artifact that was created [13], and have been employed in HCI research as probes to explore and evaluate futuristic concepts to synthesize new design knowledge [56]. We implemented our FFV sensitizing concept as a series of questionnaires designed to guide a collective, presented with an emotionally-resonant user account of a PVEI, to (1) find specific privacy concerns demonstrated in the account, (2) propose concrete fixes for these concerns, and (3) verify that the proposed fixes address emergent concerns, and prioritize the most compelling fixes. We found compelling evidence that participants emotionally connected with strangers' accounts of PVEIs and easily converged on concerns and demands; however, they had trouble articulating concrete demands for redress. Instead, the collective proposed and voted for broad, systemic changes that would be difficult to formalize without significant access and expertise—e.g., "data protection laws" and "rethinking the algorithm".

To address the *Stewardship* RQ, we asked a panel of security and privacy (S&P) experts to interpret the collective's concerns and demands. Importantly, our goal here was not to prove or disprove that our sensitizing concept "worked" but to uncover insights into how we might solicit expert stewards to help translate the collective's high-level demands into concrete compensatory or punitive requests for recourse. Unexpectedly, we found a strong tension between what the panel deemed to be appropriate responses and what the collective desired. The panel, while sympathetic to the collective's *frustrations*, tended to dismiss their *demands* altogether. They either preferred highly-specific, one-off penalties unrelated to the collective's demands—e.g., fines and FTC consent decrees—or expressed that the collective's demands were altogether unrealistic. In short, the collective wanted broad, systemic change but did not have the expertise to translate these desires into specific, actionable demands. The panel expressed little desire to steward the collective, and wanted instead to work within existing legal structures to provide one-off relief and/or punishment that was often unrelated to the collective's demands. This disconnect suggests that S&P experts, however well-meaning, may play a role in upholding the power divide between end-users and institutions, and that there is ample room for future work in aligning the desires of non-expert collectives with the knowledge of experts.

To summarize, in this paper we contribute:

(1) A sensitizing exploration, modeled after Bernstein et al.'s Find-Fix-Verify [12], of how non-expert collectives might generate representative concerns and demands for redress in response to a PVEI.
(2) An assessment of how collective-constructed concerns and demands map onto existing existing mechanisms for redress by a panel of S&P experts spanning industry, academia, government, and law.
(3) A discussion of how existing mechanisms for privacy reform can be misaligned with end-user desires, along with recommendations for designing privacy collective action platforms that help alleviate this misalignment.

2 BACKGROUND AND RELATED WORK

2.1 User reactions to PVEIs

There has been extensive prior work documenting users' reactions to a variety of PVEIs, from discovering their information was a part of a data breach [26, 39], to learning about new regulations in the news, to perceiving output from recommendation algorithms as being too specific or creepy [52]. A study of the aftermath of the 2017 Equifax data breach illustrated that while people were aware of the risks resulting from this breach, they tended not to take protective actions because they did not know enough about the breach or because it was cost-prohibitive to do so [58]. A theme in past work is that despite their worry, fear or anger in response to these PVEIs, users tend not to take further action to protect themselves or react to the institution behind the event. Similarly, people tend to reject security advice or adopting S&P behaviors because of stigmas of doing so as being "overkill" [19, 24], feeling that it was not their job to feel responsible, since they trusted corporations to protect them from outside threats [47]. This prior work does not speak to users' sense of responsibility for protecting themselves from corporations, however. And, even if people do not feel empowered to protect their own S&P, they feel responsible for others' [16, 20].

In summary, people feel angry and frustrated about PVEIs, but feel powerless to effect change. Yet, people do feel a sense of accountability towards protecting others' S&P. In this paper, we explore whether harnessing this sense of accountability on a collective scale can offset users' learned helplessness.

2.2 Pain points of systems supporting (privacy) collective action

2.2.1 ***Existing systems supporting privacy collective action.*** Online petitions, perhaps best exemplified by all-purpose, all-cause websites like Change.org, MoveOn.org and Care2.com, are commonly used for collective action online, but rarely translate to real-world action. Moreover, the types of people who sign these petitions might not be representative of the broader population: less than 5% of users on Change.org accounted for over half of all signatures, and more than 99% of petitions are never marked as "victorious" [31].

In the context of privacy, when people turn to platforms like Change.org to generate petitions to make demands of institutions after PVEIs, there is no guarantee of recourse. For example, at last count, 243,900 people had signed a petition titled "Don't let EQUIFAX escape liability!", addressed to the Federal Trade Commission, demanding that Equifax, in the wake of their 2017 breach [4], be forced to "pay for their greed, even if it drives them into dissolution" [3]. Four years after the event, people are still signing this petition, suggesting that their anger has not abated over time, and that there have still not been adequate amends made toward those affected.

There is also little productivity on discussion forums directly related to privacy. For example, on the r/privacy subreddit, Reddit users share privacy-related news and seek advice on privacy-enhancing behaviors. However, rarely do posts there result in more than a handful of replies, much less users organizing around their privacy grievances toward a particular institution. One promising movement arose in June 2020, where a Reddit user, fed up with being "watched by cops" in the wake of the protests after the murder of George Floyd, started scraping public records to monitor police officers' on-the-job behaviors in retaliation [6, 7]. This user garnered thousands of upvotes and comments of support, launching a new subreddit (r/DataPolice) with 7000 members dedicated to the cause, as well as a Slack workplace with more than 2000 volunteers who wanted to contribute. However, just six months later, r/DataPolice was already bereft of new posts and comments. Those who signed up inquired about progress updates on the cause's work, to little avail.

2.2.2 ***Computer-supported collective action.*** Why do so many existing collective systems and platforms for enhanced privacy protections fail? A helpful framework for answering this question is Shaw et al.'s computer-supported collective action (CSCA) [50]. Shaw describes five key patterns of CSCA that computing systems need to address to successfully support collective action—viz., (1) Identifying a problem, (2) Generating, debating, and selecting solutions, (3) Coordinating for action, (4) Taking action, and (5) Following up and assessing action—and claims that failures in CSCA occur not only within these patterns but also in the transitions *between* them. Das et al. [17] outline a vision for an end-to-end system — *Privacy for the People* (PftP) — that spans Shaw et al.'s CSCA framework for the context of privacy collective action, in particular.

CSCA and PftP can help diagnose why online petitions, specifically those against large data aggregators, often fail. In the Change.org petition against Equifax, for example, after signing a petition and helping bring attention to a problem, signers had no way to collectively decide which of their concerns were most important to present as a united front. Nor could they debate on the exact mechanics of what solutions they wanted from Equifax, much less unilaterally move to a platform that would facilitate this debate or coordinate further action. In other words, the petition failed at the *second stage of CSCA and PftP* — the gathering and deliberation of ideas from the collective. However, neither CSCA nor PftP directly operationalize how such a structured gathering of ideas might successfully be collected, debated and filtered.

Our work builds on Shaw et al.'s CSCA and Das et al.'s PftP by operationalizing and evaluating a specific structured process—that we discuss in detail in Section 4—to gather, debate and filter ideas for redress across a broad collective affected by a PVEI. In so doing, we aim to address the lack of buy-in or representation people have in privacy collective action. We also explore the external resources and scaffolding necessary to make such collective action more realizable.

3 EXPLORATORY INTERVIEW STUDY: IDENTIFYING INCITING INCIDENTS

Our primary goal was to explore how we might design a system that facilitates the second phase of Shaw et al.'s framework for CSCA in the context of privacy collective action —the systematic gathering, refining and selection of compensatory and punitive demands in the wake of an "inciting" PVEI. We leapfrog Phase 1—the proactive identification of a problem and finding others who care—because responding to PVEIs is inherently reactive: collectives, like those who signed the petition demanding Equifax be held accountable for their data breach, naturally form *after*, e.g., the publicizing of a data breach or a media exposé. Nevertheless, a necessary precursor to Phase 2 is to find an emotionally resonant inciting PVEI that might motivate a collective to act. To find candidate "inciting" PVEIs for our sensitizing design probe, we started with an exploratory interview study to identify emotionally-resonant PVEIs, hypothesizing that PVEI accounts where individuals articulated specific emotional impact and concrete demands for redress would be good candidates for collective action.

3.1 Procedure

We ran semi-structured interviews with 10 participants over the BlueJeans video conferencing tool due to the COVID-19 pandemic. Our procedure was approved by an IRB. Participants were: located in the United States; active users of Internet-based services and devices; and aged between 18 to 44 years old. Half were women, and half were men. Seven had a formal computer science education or career.

We first asked participants about experiences where a large institution had handled their personal data in a way that was unexpected or violating. Then, we asked about how the institution could remedy the situation. Many participants struggled to envision themselves making demands of the institutions, so we asked them to imagine themselves in a variety of "power roles" relative to the offending institution: (1) The participant was assigned to design a new competitor institution that had all the features, benefits, and social reach of the initial institution, but with the privacy practices

that the participant wanted; (2) the participant was part of a class-action lawsuit by a third-party law firm and was asked to make a statement to the institution about their experiences and demands; and, (3) the participant wielded enough power to create legislation or regulation that would force the violating institution to comply. Then, to unpack the emotional resonance of these PVEIs, we asked participants to describe how they felt about the PVEIs by asking them to select five emotional adjectives adapted from the expanded Positive and Negative Affect Schedule (PANAS-X) [54].

Interviews lasted 30 to 60 minutes, depending on how many experiences participants felt comfortable sharing. Participants were paid 10 USD in gift cards. We promoted the study on our personal Facebook and Twitter accounts. Participants were notified in consent forms that their responses would be used to inform future design opportunities relating to user agency over personal data.

3.2 Data analysis

One member of the research team transcribed the contents of the interviews. Then, through repeated discussions involving the entire research team, we performed reflexive thematic analysis [14] on the interview contents to categorize the types of PVEIs participants reported and the emotional resonance of those experiences. We also noted patterns in the types of power roles that led participants to come up with specific demands against privacy-violating institutions.

We further evaluated the types of experiences that people reported, as well as the differences in emotional reaction that these experiences elicited. We considered the types of language participants used to talk about themselves in relation to the corporations, as well as what role they felt they could play in the situations. We organized the PANAS-X adjectives they chose to describe their experiences based on the categories outlined in the original PANAS-X manual: fear, hostility, guilt, sadness, joviality, self-assurance, attentiveness, shyness, fatigue, serenity, and surprise [54].

3.3 Findings

Participants reported three broad categories of PVEIs: targeting and personalization, data breaches, and surveillance. *Targeting and personalization* experiences included feeling harmed by perceived reductive profiling, or being "creeped out" by high levels of specificity in targeting. Participants who mentioned *data breaches* had been victims of a wide range of breaches: e.g., Yahoo [43], Equifax [4] and OPM [41] Violated data included personal contact information, passwords, credit card data, and financial history. Participant accounts of *surveillance* included being concerned that Amazon Alexas or Google Homes were listening, or worried that Facebook was surreptitiously using the microphone on their smartphones to record their conversations and target them with ads. We took participants' concerns at face value, and did not attempt to fact check their concerns; our goal, in this phase of our work, was only to derive a sense of which PVEIs could be emotionally-resonant enough to serve as the basis for a collective action effort.

3.3.1 ***Emotional impact of different PVEIs.*** The PVEIs that participants shared with us spanned a wide, primarily negative emotional range. Notably, data breaches incited particularly high negative emotions in participants; participants reporting these incidents frequently chose words corresponding with fear (e.g., "nervous", "scared") and hostility (e.g., "disgusted", "angry"). One participant, a victim of multiple simultaneous breaches involving the same sensitive information about him, could not identify where threats were coming from, and felt scared for his friends and family.

Instances of targeting and personalization that had materially, negatively impacted participants' lives and influenced their Internet usage also elicited strong reactions, e.g., "disgusted" and "frightened". One participant noted that her mother was concerned about getting targeted with inappropriate ads for dating websites even though she was happily married; the participant was at a loss for how to explain the situation to her mother, who was less technically-educated. On the other hand, those who generally disliked the level of data collection needed to enable targeted advertisements and personalization conceded that they reaped small benefits from it, mirroring previous work [52]. They chose words like "amazed" or "surprised" to describe their experiences. Even when they chose negative words, participants felt the consequences of the targeting were not severe enough for them to warrant redress, and blamed themselves for not doing or knowing more. One participant admitted, *"I would like to be more informed about it…I just really haven't been able to do that yet, and I've already given them so much information."*

Similarly, those who mentioned surveillance were concerned that their smart home device or smartphone was recording audio, but also felt that they could simply disable microphone permissions, turn off the devices, or get rid of the devices. Several participants felt simultaneously "afraid" of the surveillance and "amazed" at how pervasive it was. One participant noted possible malicious intent behind Google offering free Google Home devices—to collect as much home audio data as possible—and said she warned her friends not to redeem the free devices.

3.3.2 ***Conflicting senses of agency.*** Regardless of the "power role" we asked participants to imagine themselves in, they struggled to make specific demands of institutions. Participants had deeply-ingrained notions that they were themselves to blame, and were concerned about their lack of alternatives. One participant wondered if they were really allowed to feel violated if they had consented: *"I guess I am giving my consent when I sign up for a Google account. Like it's all in the fine print. So I almost feel like I shouldn't feel violated because I'm consenting to these things by using a phone."* Others felt they should have simply known better and taken better precautions or not consented, but sometimes didn't do so anyway. In response to this phenomenon, one participant remarked, *"That cognitive dissonance makes me sad."*

This is not to say participants felt completely defeated: they often felt responsible for protecting others, and also found solace in sharing their experiences. However, this pressure of social responsibility made them feel both more frustrated and more powerless about the privacy-violating experiences, because they could not help those with less S&P knowledge navigate these experiences. One participant admitted that even though she was not completely knowledgeable about best S&P practices, she still had to take care of her family: *"My family kind of relies on me to keep them safe, so I feel a lot of pressure that way. I know that I'm really not the best at this,*

but I would like to help keep them safe." So, while participants often felt helpless to effect change as *individuals*, their senses of solidarity with and accountability to others could present an opportunity for collective action that is triggered from a personal narrative.

4 THE REPRESENTATION RQ: FIND-FIX-VERIFY

The exploratory interview study helped us learn about the types of PVEIs that might inspire privacy collective action. Given this set of inciting PVEIs, to address the *Representation* RQ—How can we mobilize collectives to move from amorphous discontent and anger toward specific, representative privacy demands?—we next employed methods from concept-driven design in HCI research [51]. Specifically, we designed a collective sense-making process as a "sensitizing concept" that envisions one way privacy collectives might transition from an individual's PVEI to collective-synthesized demands for redress. Sensitizing concepts are exemplary artifacts meant to probe a design space and inspire designers to new possibilities in the space [13]. Importantly, the utility of a sensitizing concept is *not* the artifact itself, but the synthesis of new design knowledge from the creation and evaluation of that artifact [56].

Prior art in shepherding collectives towards meaningful creative output informs our approach. ConsiderIt [37], for example, a platform for supporting public deliberation, surfaces and summarizes pro/con statements from individuals who are broadly for or against an issue up for public debate. However, ConsiderIt is meant to be used in a consultative manner for policy makers and experts, rather than directly represent collectives. Similarly, Lean Privacy Review [34] collects users' privacy concerns, but is also meant for S&P *practitioners* to consult.

In designing WeDo [57]—a prototype participatory, end-to-end collective action system built on top of Twitter designed to help transition collectives through Shaw et al.'s five phases of collective action—Zhang et al. found that to improve chances of a collective action campaign at succeeding, it was critical to identify and mobilize clear leaders; otherwise, the campaign could stall without clear direction on next steps. Salehi et al. [49] similarly identified two challenges—stalling and friction—when designing a collective action platform designed to congregate crowd workers into collectives. Stalling entails a loss of momentum: a collective would form around an issue but, without any tension or clarity in driving towards consensus, would quickly disassemble without acting. Friction entails an impasse in which two or more opposing ideas lead to a break down in civil discourse and progress. To overcome these challenges, the authors recommend design considerations that help structure the collective's labor, e.g., setting clear deadlines for consensus, allowing for decisions to move forward with space for undoing if necessary, encouraging reflection and producing hope. Based on this prior art, we concluded that a collective sense-making process must be carefully scaffolded in order to assure productive forward momentum [49].

Our sensitizing concept provides this scaffolding via three online questionnaires presented to users on Prolific, a platform where people can perform Internet-based tasks for monetary compensation. The questionnaires were modeled after Bernstein et al.'s Find-Fix-Verify (FFV) crowd programming pattern [12], which presents a distributed crowd with a high-level open-ended task (e.g., shortening a block of text), and funnels individual crowdworkers' attention to smaller sub-tasks that, in aggregate, accomplish the high-level task. Here, the high-level open-ended task was to take an emotionally resonant account of a PVEI and have a distributed collective converge on a set of core privacy concerns and demands for redress. To that end, our three surveys presented participants with an emotionally resonant account of an inciting PVEI, and then participants had to: (1) **find** concerns they had with the account, (2) propose concrete **fix**es for these concerns, and (3) **verify** that the proposed fixes addressed emergent concerns, and prioritize the most compelling of the proposed fixes, respectively.

FFV simplifies the complex task of asynchronously distilling a unified set of demands from a distributed collective. The three stages are easily translatable to design requirements, each offering different insights about how to support the collective: whether a collective even cares about others' concerns (**Find**), whether it can understand and provide support for itself (**Fix**), and whether it can unite (**Verify**). While other methods like focus groups provide explanatory insights about consensus-making at a small scale, our goal was to uncover insights that would more directly inform the design of a larger scale system. FFV has been shown to be effective at shepherding groups to produce high-quality outputs for open-ended creative tasks [12].

At the same time, no amount of guided scaffolding can be successful without an unifying motivation. One failure point of privacy petitions previously mentioned is that they are ad-hoc, or only responsive to immediate events like a singular data breach; such actions tap into a collective identity of all being part of the same breach. However, a given user has been affected by multiple breaches, violating feelings from targeted advertising, and experiences of unwanted surveillance, and they connect to and support each other by sharing these experiences with each other [18, 44]. Users experience unique combinations of PVEIs, the overlaps of which create an even bigger base for collective action. Thus, in the case of end-user privacy, we believe that tapping into collective empathy with other users' personal related experiences, via Bennett and Segerberg's connective action [11], is more imperative as a motivation than membership in a single data breach's class of victims.

In this section, we will examine the results from each phase of our FFV concept, which will help address **RQ1**. Specifically, we split the problem into two sub-questions:

- ***RQ1.1:*** *How do people empathize with and relate to others' PVEIs?*
- ***RQ1.2:*** *What external stewardship is necessary to guide collectives toward concrete demands for redress?*

Answering **RQ1.1 (Empathy)** will shed light on whether an emotionally-resonant inciting PVEI can motivate someone to substantively contribute to a collective effort. Answering **RQ1.2 (Scaffolding)** will unpack the potential design requirements of an effective platform for orchestrating collectives into jointly composing privacy concerns and demands in response to an inciting PVEI.

4.1 Recruitment and overall procedure

For our FFV sensitizing concept, we picked three PVEI accounts from our exploratory interviews that had the strongest emotional resonance with our participants, hypothesizing that these accounts would be more likely to elicit empathic reactions from the collective. The accounts we selected reflected reactions to specific violations, rather than general opinions on phenomena like the "creepiness" of audio recording or aggregate data collection. The interview participants who provided these three accounts gave high levels of detail in their answers about what specifically made them uncomfortable, and how they wished institutions had responded. Each scenario was comprised of direct quotes from respective individual participant accounts, edited for brevity.

At each phase, FFV participants were assigned to read one of the three PVEI accounts (henceforth known as either the *Equifax data breach scenario*, the *Instagram profiling scenario*, or *OPM data breach scenario*, respectively). The author of the *Equifax data breach scenario* described his experience of finding out he was affected by the breach [4] by checking Equifax's online tool, relaying his frustration at the one year of credit monitoring and small settlement payment Equifax offered in response. The author of the *Instagram profiling scenario* described seeing recommended posts on Instagram based on perceived profiling of his identity as a gay man, and expressed discomfort with this reductionist targeting. The author of the *OPM data breach scenario* described how he felt confused and alone when he found out he was affected by the breach [1, 41], and how he wished there had been more direct followup from OPM (the U.S. Office of Personnel Management, which manages the employment data of all federal government employees). The full text of the three accounts that we chose can be found in the appendices.

Following the original Find-Fix-Verify design [12], participants were split into three independent groups across the phases. As with the crowd-powered text-processing system, Soylent, for which the FFV design pattern was originally developed, we felt that differing effort levels in participants could yield incomplete coverage of the concerns in the accounts. Thus, recruiting independent groups for each of the three phases allowed us to limit the amount of effort required from any individual contributor. (For example, if Find and Fix were combined, participants might simply choose concerns that they felt were easiest to address, rather than ones they felt were most concerning.) Recruiting three independent groups could also ensure participation from a greater number and diversity of voices from the collective, and the separate Verify participant pool also provides an independent verification of the best fixes.

Each phase consisted of a short online questionnaire, each of which we will detail in the following subsection. A diagram showing the overall flow of the FFV process is found in Figure 1. We recruited three sets of participants (200 for the Find phase, 100 for Fix, and 100 for Verify) on Prolific. Participants were over the age of 18, located in the United States, fluent in English, and active users of Internet-based services like social media, a smartphone, or a smart home device. For each phase, participants took part in a short questionnaire hosted on Qualtrics, taking on average 5 minutes, for which they were compensated 1.50 USD on the Prolific platform (the equivalent of 18 USD per hour). Participants had a mean Prolific score of 99.7. Demographics of the participants across the three phases can be found in Table 1.

Phase	% Women	% Men	% Other	Mean Age	Std.Dev.
Find	47.0	52.5	0.5	29.96	9.99
Fix	61.0	38.0	1.0	29.87	9.97
Verify	48.0	52.0	0.0	30.62	10.06
All Phases	50.8	48.8	0.4	30.10	9.98

Table 1: Demographics of Find-Fix-Verify participants. Three separate, non-overlapping sets of participants were recruited, one for each phase.

We parsed the text responses from each phase manually. To minimize researcher guidance and best mimic the hands-off nature of such a platform in the real world, we did not edit or paraphrase any concern or solution statements. We uncovered emergent patterns in each of the phases through thematic analysis [15].

4.2 Phase procedures

In the **Find** phase, participants were asked to first express their emotional reaction to reading their assigned scenario by selecting two of Ekman's six emotions [22]—afraid, angry, disgusted, sad, happy, surprised—and explaining why they had chosen those emotions. We presented this question as a space for participants to first vent any feelings or biases directed toward the institutions themselves. Afterwards, we asked participants to identify two specific concerns from the passage that they found most concerning, and explain why.

In the **Fix** phase, after reading their assigned scenarios, participants were randomly presented with five concern statements (parsed from the previous stage and respective to their assigned scenario). They were then asked to pick two that they felt should be prioritized. In pilot studies, we found that participants interpreted "prioritize" to mean whatever resonated most with them. Then, for each of the two concerns they chose, we asked participants to pick one entity—out of (a) the offending institution, (b) other people who had been affected by a similar experience, (c) a government agency or regulatory body, or (d) another third party like a law firm or advocacy group—that they felt could take action to address the concern. We then asked them to detail what actions they believed this entity should take. This simplified categorizing participants' responses, and also guided them into thinking about parties outside of only those in the passage they read. Since we also wanted to know about how users viewed their agency in these scenarios, we also asked participants how they felt after completing the survey.

Finally, in the **Verify** phase, we carried forward only concerns from the fix phase that had actions where participants had chosen the three entities with the most votes to take action. To further streamline convergence on a few concerns and recommended actions, we restricted the concerns (and corresponding actions) to only those that had gotten at least two votes. This resulted in five to 10 concerns and 10 to 20 actions per scenario. After reading their assigned scenario, participants were, similar to the fix phase, randomly presented with five concerns and asked to choose the two they felt should be prioritized. For each of the concerns they

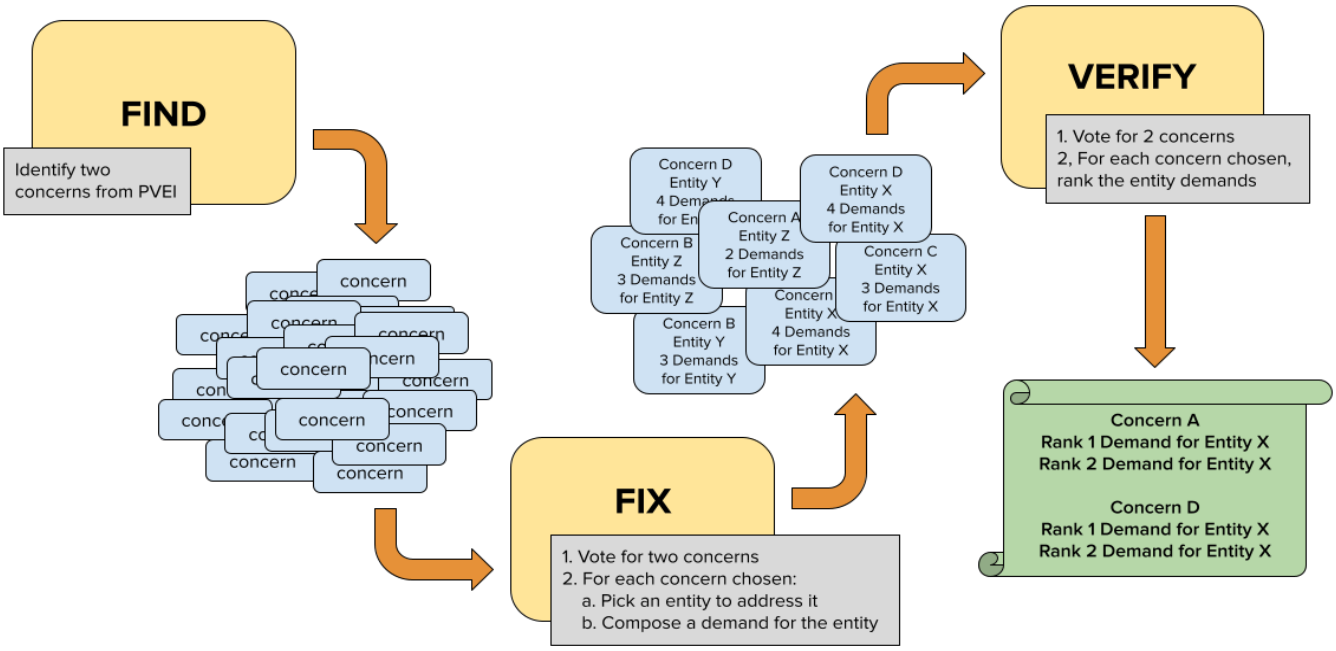

Figure 1: *The Find-Fix-Verify process for an inciting PVEI.*
In the Find phase, a set of 200 participants identified concerns they had with a PVEI. In the Fix phase, another set of 100 participants picked the most pressing concerns and proposed demands to address them. In the Verify phase, a third set of 100 participants picked the most pressing remaining concerns, and ranked the corresponding demands from the previous phase.

picked, we showed them all of the respective actions that fix-phase participants had authored and asked our verify-stage participants to rank-order the proposed fixes. We asked participants to keep in mind three criteria for ranking: (1) specificity, i.e., whether the action included specific tasks or steps for the entity to take; (2) effectiveness, i.e., how well the action addresses the concern; and (3) desirability, i.e., how much the participant personally wanted the action to be implemented.

4.3 Find: Aggregating user concerns

4.3.1 ***Collective output***. Participants indicated negative emotional reactions across the board in reaction to reading the accounts. 69% of Equifax-assigned participants felt angry or disgusted; 56% of Instagram-assigned participants felt sad or disgusted; and 45% of OPM-assigned participants felt angry or afraid.

Equifax data breach concerns. Participants expressed strong disappointment and dismay at the lack of adequate compensation, remediation, and general effort on Equifax's part. Many strongly empathized with the original author's perceptions of being neglected and brushed aside. Participants felt that a year of free credit monitoring offered by Equifax to those affected by the leak was inadequate, as was the class action lump sum payment, and also made value judgments about Equifax's perceived priorities. One participant said, for example: *"Nobody really cared about what happened; [Equifax] couldn't be bothered to actually take the time to properly structure payout and examine the issue. It was just a large chunk of money which, honestly, doesn't even really hurt these large corporations all that much."*

Instagram profiling concerns. Participants expressed confusion about Instagram's recommendation algorithm, as well as a lack of control over the posts they saw. Some tried to guess at the mechanisms of the recommendation algorithm, remarking on their perceived problems with how the algorithm works: *"The user is not putting every post using the hashtag 'gay' or anything related. Yet the recommended posts do not reflect what hashtags the account primarily uses."* This is not to say that participant conceptions of the Instagram recommendation algorithm were accurate, but rather that the perceived outcome drew negative reactions. Outside of algorithmic concerns, participants also worried about the possibility of context collapse—i.e., how different social contexts like the personal the professional blur together in online environments [21]—when accidentally displaying not-safe-for-work photos in a work environment. They noted that this experience could restrict how the original author uses Instagram: *"This limits when the user can use the application because it may show a NSFW post that he doesn't want someone to think he is looking at [in the workplace]."*

OPM data breach concerns. While the OPM and Equifax scenarios were similar in that participants felt the punishment for OPM was insufficient, several participants directly cited OPM's status as a governmental agency, holding OPM to a higher standard of security and transparency: *"You would think that a government agency would be more equipped and transparent about things that could*

compromise safety and livelihood." They also worried that the government could not be held accountable: *"The lack of options given by a government entity always makes me uncomfortable, because ultimately they are unaccountable to anyone and their actions are hardly scrutinized with any consequence."*

4.3.2 ***Findings.*** Concerns raised in this phase were abundant but similar, suggesting that a collective could empathize with an inciting PVEI and rally around common concerns. We found initial answers to both RQ1 sub-questions.

RQ1.1 Empathy. The strong emotional language participants used to detail their concerns, plus their relation of the accounts to their own experiences, suggests that participants could strongly empathize with accounts of inciting PVEIs.

For example, participants assigned the Equifax scenario felt angry for the original author and were reminded of their own anger towards Equifax as a result of the breach. Many strongly empathized with the original author's perceptions of being neglected: *"Just a year? Credit monitoring? This is a company that does not care about people."* Some also worried of becoming habituated to learning about data breaches like the Equifax one. For example, one participant said, *"Honestly, I had almost forgotten about the Equifax thing until I read this, which sort of scares me too. Large institutions are able to get away with near criminal behavior and we as a public just tend to brush it off after a few years."*

Participants similarly related the Instagram scenario to their own lives, e.g., feeling *"frustrated on behalf of a gay friend who uses Instagram".* Several directly mentioned the harmful nature of certain stereotypes about gay men: *"As someone who's well acquainted with multiple members of the LGBT community, I fully recognize the stereotype that all gay people are driven by sexual desires, and that's exactly what Instagram is perpetuating here.... Instagram's algorithm simply labeled him as 'GAY' and shoved pictures of shirtless men at him."*

Those assigned the OPM scenario empathized more broadly with the author's feelings of loneliness and confusion in the middle of interpreting legal documents without help, generalizing the author's experiences to other data breaches. One participant related, *"I've gotten so many notices over the years about my info being stolen from companies, and there's never any follow-up. Literally never. Is my data being sold on the dark web? Did they track down the thief? Did they at least improve their security practices? Who the hell knows."* Participants also opined about the burden of reacting to a data breach, echoing past work [29]: *"Individuals are left in these situations where they are given a kind of impossible task. Sure, you can theoretically protect yourself, if you have hours and hours of your private time to spend reading fine print, and understanding complex legal things, and sitting on hold and getting transferred, and still not really getting answers."*

RQ1.2 Scaffolding. There were hints of an answer to RQ1.2 in this phase. Participants often generalized specific concerns into broader statements about the power that institutions have to come out unscathed after negative events. No additional researcher input was necessary to guide participants into these responses, because the scenarios were emotionally resonant in and of themselves. However, due to the number of concerns brought up—two per participant, 400 total—the next challenge the collective would need to overcome would be converging on a shortlist of actionable priorities.

4.4 Fix: Proposing demands to concerns

4.4.1 ***Collective output.*** Free-text responses from this phase were noticeably less impassioned and detailed than the previous phase. The level of detail in the actions that participants authored were also dependent on both which scenario they were assigned and which entity they chose to take action. We also found the entities that most participants believed should take action for each scenario. 51.5% of participants assigned the Equifax scenario believed a governmental agency or regulatory body should take action to address the concern; 63.2% assigned the Instagram scenario believed Instagram, itself, should do something; and 51.6% of participants assigned the OPM scenario believed OPM, itself, should act.

Equifax data breach scenario. Even though a majority of participants wanted a governmental agency or regulatory body to take action, the level of specificity in the actions they wrote was low. A large number of people who chose a government action came up with general phrases like "Policies, fines", "Data protection laws", or "Anything that would punish Equifax for what was done"; very few described what kind of regulation specifically. On the other hand, participants who chose Equifax to act were very detailed about what they wanted from Equifax. For example, one participant wanted Equifax *"to be responsible for any and all identity thefts for the next 5 years as well as total cooperation and customer service and complete ownership of the problem. oh and any money made from my information goes directly to me as well as a promise that any information sold equals a fine (paid also to the victim) of 50,000 USD."*

Instagram profiling scenario. Since a large majority of participants wanted action from Instagram itself, the specificity of participants' recommended actions varied depending on the concern rather than the entity. Those who prioritized the aforementioned context collapse problem overwhelmingly wanted Instagram to implement an end-user toggle for displaying NSFW photos. Meanwhile, participants concerned with reductive inferences or a confusing algorithm tended to provide less specific responses. Several participants wanted Instagram to "fix/update/reconfigure/revamp their algorithm". A significant minority of participants chose anyone who'd been affected by a similar experience as the entity that should take action, urging those affected to *"petition other parties and the service being used to not be reduced to a gay person, as their combined lived experiences may have more sway than a bunch of individual complaints."*

OPM data breach scenario. We defined OPM itself and the entity of "governmental agencies or regulatory bodies" to be distinct, even though OPM is a governmental agency itself. One participant wrote extensively that they wanted another governmental agency *"To fully investigate the breach, publish the investigation in easily understood prose, and follow up with every individual who had personal information compromised. The follow up should include information...on how the breach occurred and how it's being corrected, as well as very specific information on how the breach could affect the individual and steps to take if it did (such as fraudulent charges, sold social security number, etc) so that the affected individuals have*

a starting place to fix their lives and livelihoods." Broadly, participants kept in mind the long term effects of the OPM breach. One participant mused, *"If they put someone in this position, it's their responsibility to make sure it doesn't have catastrophic effects. The leak may be brief, but people can easily hold onto the info for later use."*

4.4.2 ***Findings.*** **RQ1.1 Empathy.** We uncovered three themes in how participants felt after proposing fixes to emergent concerns: heightened frustration, greater alertness about the concerns raised, and resignation at the chance to voice their demands.

Several participants felt frustrated that their contributions would be fruitless. For example, one participant said they felt *"like nothing is going to change...because the problem is bigger than one company and some data mining. It's difficult to say there should be government oversight when we all know the government is doing the exact same thing and we're most likely vulnerable there, too."* Similarly, another participant said they felt *"more outraged? I feel like, I just realized that they #1 made money off me (they should give it to me), #2 they don't have to help with the fact that they ruined my life (they should take care of me), and they still didn't come clean (if they do it again there should be a fine.)"*

Others felt that their participation reintroduced previous concerns highlighted in the inciting PVEI. For example, one participant said, *"I feel a bit better [about contributing a demand], but the guy that had his information leaked was right. I totally forgot about the equifax thing until I read that [the inciting PVEI] again."* Another noted after completing the fix phase, *"I feel like I got the chance to better organize my opinion on these concerns and have a more solid stance on the issue."* Others felt more empowered: *"I feel that I ought to get more involved in local politics to express my views more freely."* Participants were not completely satisfied, though: *"I feel a little bit better that I got [my opinion] out, but I would prefer to see actions related to this being taken/being held accountable before I let this issue go to rest."*

Even without being asked about the likelihood that their demands would be realized, though, participants felt pessimistic about their prospects. As one participant said, *"I feel like my opinions were valid and easily executable but will not bear any weight on how companies actually treat breaches."* In other words, some participants felt that: (i) powerful institutions that have the ability to effect change will not listen; and, (ii) that they, themselves, have no power against these institutions. This belief, in turn, could have a negative motivational effect on their participation.

RQ1.2 Scaffolding. In a naive reading of the question, our strict rules for advancing concerns and demands to specific entities easily drilled down on numerically fewer concerns and demands. And there were indeed specific entities that participants wanted to take action more than others: for the Equifax data breach, a government agency or regulatory body; for the Instagram profiling scenario, Instagram itself; and for the OPM data breach, OPM itself. Carrying forward only the concerns and demands that (1) involved these entities respectively and (2) had been picked by at least two participants sufficiently reduced the number of choices to a manageable amount for the next stage's participants. A limitation of this approach is that participants in the verify phase would only see a subset of proposed fixes. The best proposed fixes might not always be associated with the most popular entity of whom the collective wishes to make demands. However, without prioritization, the collective's attention would be spread too thin. We elected to prioritize entity popularity so that the process could be, in theory, entirely self-contained, deterministic, and not requiring moderator input.

Content-wise, participants were better at providing detailed actions for Equifax and OPM to take, such as specifying exact amounts for compensation or step-by-step timelines for them to communicate with people affected in the breaches. On the other hand, they struggled to generalize these demands into regulations that would prevent scenarios like the inciting PVEI from recurring in the future, perhaps because average users do not have extensive knowledge of what could go into S&P regulations. In the same vein, participants might be good at identifying themes of concern—take, for example, participants in the Instagram profiling scenario wanting Instagram to "modify their algorithm"—but may require expert stewardship to translate these desires into actionable demands.

4.5 Verify: prioritizing demands

4.5.1 ***Collective output.*** For each scenario, we gathered the two concerns that received the highest share of votes, as well as the two top-ranked actions for those concerns. Complete results are in Table 2.

For the Equifax data breach scenario, participants were most concerned with a lack of existing regulation that could hold Equifax accountable and prevent similar future incidents at other institutions. To address this, participants wanted legislation in place that would set security standards, harsher punishment for Equifax to pay more in reparations to those affected, along with investigations into who was involved with and responsible for the breach. For the Instagram profiling scenario, participants most disliked the lack of transparency around Instagram's recommendation algorithms. Participants wanted Instagram to update their algorithm to better reflect their expectations: specifically, basing recommendations on what a user posts rather than inferences about their identity. They also wanted a formal apology from Instagram. In response to the OPM data breach scenario, participants prioritized clear communication from OPM, and were concerned that the author of the account did not know what specifically had been "messed with." To address these concerns, they wanted explicit disclosures about the nature and extent of the data breach, detailed plans for compensation, and general transparency from OPM.

4.5.2 ***Findings.*** In this phase, we did not solicit answers from participants about their emotional motivation, but rather aimed to converge on the most popular demands, i.e., answering **RQ1.2 (Scaffolding)**.

We started from 400 concerns across the three scenarios. Fix-phase participants assigned accountable entities and demands to these concerns. We first isolated only concerns from the most popular entities, resulting in 110 concerns and demands; we further advanced only concerns that had at least two votes from the fix-phase, for 23 concerns and 49 demands in the verify phase. Verify-phase participants then condensed these further into 6 concerns and 12 demands. The collective effectively synthesized a total of 400 concerns down to six. (Again, a diagram of this FFV process can be found in Figure 1.) Since participants were faced with a limited set

Scenario	Concern	Rank 1 Solution	Rank 2 Solution
Equifax	"How can a company continue operation as normal after such a major security event? How does our legislation let something as serious as its citizens' identities being leaked pass without reform? I feel the entire situation described was a high level case of lunacy, and I feel I'm probably not the only one who feels that way."	"Regulations and legislation addressing the larger issues that allowed the breach and mistreatment of customers to happen in the first place. Coming down hard on Equifax and requiring them to increase security and paying reparations to those they harmed."	"I would want to see an investigation into the persons who perpetrated the act as well as the security measures that should have been taken. I would like to know why the data wasn't so secure."
	"There was no clarity on what has changed to prevent the same thing happening in the future, so this will continue to happen and we will suffer for it."	"I want the government to try to set better standards and regulations to prevent something like this happening again and to minimize the damage if it happens again"	"Laws and/or regulations to prevent this type of data breach from happening again."
Instagram	"It directly opposes the idea of an algorithm that Instagram uses to recommend posts. Logically, if most of his posts are about baking and cooking, that would be what his recommendations fill up with. However, the recommended posts have nothing to do with that."	"Update their supposed algorithms so that recommended posts are related to most of the content posted by the person."	"Work on their algorithm and address why this is happening with a formal apology"
	"I would guess there is an algorithm to blame. But no one should have to deal with that reduction of their identity."	"I would like them to make sure the algorithm is fixed to work better and see if they are responsible or the consumer. Being more transparent about how the algorithm works could also help."	"I would want them to improve their algorithm so that this does not continue to happen to this man, or anyone else."
OPM	"The fact that [OPM] didn't explain what happened is terrible. I would want to know why my info got messed with, what exactly got messed with, what problems I can expect, what I can do to save myself."	"I would want OPM to be thorough and transparent in their communications. It is their responsibility to inform the people affected with all pertinent information"	"The employer should be mandated by law to make specific disclosures about the nature and extent of the data breach and should be required to pay for an independent review of its IT security policy and procedures"
	"After a large data breach like this, I would expect the company to detail out to all users of their service how they have updated their security protocols, and how they plan on making things right and better for me and the pain that I was sent through because of their mistake."	"OPM would be detailing out all of their mistakes and processes to rectify these mistakes. Detailing plans for compensation and timeline for this. Additional regulatory process in place that would catch future issues like this."	"I would want OPM to revise their data security protocols and communicate any changes to all customers. They owe people an apology and a better compensation that the 5 year protection plan that people didn't ask for."

Table 2: The final output of concerns and demands voted on by participants in the Verify phase.

of choices, they could converge on a small set of popular concerns and demands. Both the most popular concerns and most popular demands from the end of this stage were specific and impassioned. While we did not solicit any free-text responses from participants in this phase, we can surmise that participants heeded our instructions and took into consideration the specificity, effectiveness, and desirability of the demands based on the demands they ultimately selected. Indeed, demands containing low-effort text such as "Investigations and policies to prevent" (Equifax data breach scenario), "Improve their software" (Instagram profiling scenario), and "Be upfront" (OPM data breach scenario) did not receive many votes.

Overall, the compensatory demands that participants selected suggested the desire for broad, systemic changes but were low on implementation details. Indeed, participants wanted regulatory reform or algorithmic changes, but, unsurprisingly, could not (or did not) specifically articulate what would would go into these regulations or what changes to make. Note that this lack of specificity could be because of the lack of expert knowledge, but it could also be because we recruited participants to complete a short compensated survey. In practice, self-motivated, self-organized collectives may also be more motivated to be detailed in their responses. Still, to bridge this gap, we might consider enrolling S&P experts to act as stewards for the collective—i.e., to interpret or translate the collective's voice into actionable steps for the real world. We explore this possibility with an expert panel.

5 THE STEWARDSHIP RQ: EXPERT PANEL

Participants who used our FFV prototype, henceforth known as "participants" or "the collective", converged on a few salient concerns and demands for redress. However, to effect real change, these demands must be presented clearly to the institutions accountable for compensatory action (be it a regulatory body or the offending institution itself). Our next research question (**RQ2**), thus, focuses on understanding the role of experts in representing and guiding the collective: *How do privacy experts view the privacy demands generated by a collective, and how might they be effective stewards for the collective in translating their demands into actionable recourse?* To answer this question, we asked a panel of security and privacy (S&P) experts to evaluate the collective's top-ranked concerns and solutions.

5.1 Procedure and recruitment

We recruited eight non-compensated experts in privacy and security whose expertise and experience spanned academia, government, law, and industry, by reaching out to them directly through Twitter, email, and LinkedIn. We reached out to five more experts, but, as might be expected, many experts were oversubscribed and unable to commit. Demographic details of those who participated are found in Table 3. All experts had completed at least a bachelor's degree in computer science, and all were based in the United States.

Three experts participated in a 30-minute interview conducted over BlueJeans, and five filled out a survey of free-text responses

hosted on Qualtrics. We offered all experts the opportunity to participate in the interview, but most preferred the asynchronous questionnaire. Experts were assigned the set of top-ranked demands from Table 2 for the scenario most closely aligned with their expertise and asked to translate those demands into tangible tasks for entities in the real world, as well as assess the impact of these demands. They were also asked if they agreed with the rankings that the verify-phase participants had decided on, and whether they thought there were more appropriate solutions.

Expert	Gender	Age	S&P Experience
E1	Female	45-54	A, I, G, L
E2	Male	35-44	A
E3	Female	45-54	A, I, G
E4	*	*	I
E5	Male	25-34	A
E6	Female	25-34	A, I
E7	Female	25-34	A, I
E8	Male	35-44	I

Table 3: Demographics of experts. A = academia, I = industry, G = government, L = law.
E4 did not wish to be identified.

5.2 Findings

Expert responses can be broken down into two themes: (i) alignment and (ii) misalignment between experts and the collective. First, both experts and the collective recognized the harmful effects of the violations described in the three scenarios: for the most part, experts empathized with the collective's sense of helplessness, even if they were more informed about the technicalities behind data breaches and algorithmic personalization. Second, experts dismissed the punitive demands our participants wanted offending institutions to take. For example, experts felt that quantifying harm and attributing blame in these scenarios would be difficult and unrealistic, and that the collective-generated demands could result in unintended negative consequences.

5.2.1 Expert-collective alignment. The panel agreed that several participant concerns and demands were pressing to address and appropriate to enact, respectively.

For the Equifax scenario, while most of the panel felt that generalized laws and regulations would be too slow to implement, several felt that FTC consent decrees, where an institution would be legally obligated to abide by certain terms and regulations or pay a heavy penalty, could help ensure good behavior from the institution for a set period of time. Some also agreed that setting federal-level legal standards for security best practices and strict punishments for noncompliance would help prevent this from happening in the future. Other experts were less optimistic that these legal standards could be established in a manner that benefits consumers: E7 conceded, *"I think meaningful regulatory reform is unlikely to happen as long as the interest of policymakers and corporate are deeply intertwined."*

The Instagram profiling scenario drew mixed reactions across the panel. While they largely agreed that the experience that the author of the account had was unfortunate, the panel also expressed that it was unlikely to be intentional on Instagram's part and tried to guess at possible explanations that led to the PVEI described in the scenario. E4 surmised that while the author might not search for pictures of half-naked gay men himself, Instagram might infer that his identity is similar on average to other people who do want this behavior. E1 was curious if the author had searched for these pictures once but had simply forgotten.

The OPM data breach also drew mixed reactions. E1, who was also affected in the same breach, suggested that all of the solutions that people were demanding from OPM—transparent communications about who is affected, plans for compensation, strategies for rectifying the mistake—had likely already been implemented. They argued that it was the responsibility of the author of the inciting PVEI to keep up-to-date with the communications that OPM sent out in the aftermath. E2 rebutted: *"The information might exist, but people are not necessarily seeking it out, or it's not directly presented to them in ways that are actually meaningful to them. I'm sure there's like a 50-page report out there about what went wrong, but most people won't see that or look at that."* Expert stewards may be helpful, thus, in not just refining demands but also in pointing collectives towards sources of information that may help address their concerns.

In general, the panel sympathized with the powerlessness that the collective felt with regard to the two data breach scenarios. E2 mentioned that because Equifax did not require consumer consent to collect their data, and it was impossible for federal employees to avoid interacting with OPM, average people could not speak out or demand more transparency from either institution. They added, *"OPM is basically your employer or entity that manages your employee data. So what are you going to do, quit because of this breach? It's not like they have a heightened interest in being more transparent or forthright."* E7 suggested that users could file complaints with the FTC, but admitted that this was only for the *"highly motivated... I know that's a lot of burden on consumers when they already have limited time and emotional distress to deal with, but unfortunately, that's the reality we need to work with."*

5.2.2 Expert-collective misalignment: Unknown harms and unintended consequences. While experts were sympathetic to the collective's anger and frustration, they also dismissed the collective-generated demands as infeasible or having the potential to cause unintended negative effects. For example, one peripheral demand for both the Equifax and OPM breaches was providing compensation for victims. Experts felt that calculating a specific amount to pay in damages would be difficult: from a legal standpoint, compensation must be commensurate with tangible, proven harm, but the extent of the harm caused by both breaches is both unknown and ongoing. Experts also felt it would be too difficult to attribute all harm that victims endured directly to Equifax or OPM because the breach happened due to negligence and not malicious intent. Similarly, in the Instagram scenario, experts noted that because there was no evidence Instagram directly intended to make the author of the account feel targeted or marginalized, there was little recourse to be had.

The panel also noted that collective-requested solutions may have undesirable and unintended consequences. For example, in the *Instagram profiling scenario*, FFV participants wanted a "formal

apology" from Instagram to the author of the account. The panel felt that there were a few things that could inhibit Instagram from doing so: (1) There would have to be a specific line of communication between Instagram and the author; (2) Instagram would have to issue equivalent apologies every time something like this happened. E4 offered a worst case version of the formal apology solution: to keep up with all the feedback and adverse effects of algorithmic profiling, Instagram might even resort to algorithmically predicting ahead of time if users will negatively react to a targeted post.

The collective also wanted Instagram to modify their algorithm to recommend posts only based on what users post, rather than based on Instagram's inferences of user identities. E4 felt that this solution could have negative effects: *"What people like to read and what people like to post are very, very different. Doing this [solution] means I am limited to seeing the things I can talk about. I think this can be a pretty dangerous thing. But on a more innocuous level, I like to read recipes, but I don't like to post them because nobody wants to eat my food."* E8 added that even if such changes could work, their effects would not be permanent: *"Realistically, those algorithms are tuned for engagement and if proposed changes would result in a drop in that metric I'd expect that, over time, the same issue would resurface again."* E5 said bluntly, *"I am not quite sure how willing a platform designer will be to so drastically modify their system."*.

5.2.3 Summary. Our findings for **RQ2**—i.e., understanding the role of experts in guiding the collective—were multi-faceted. The expert panel empathized with the collective's frustration and desire for broad change, but only dismissed their demands as unrealistic rather than conceive of alternative approaches that might still capture the spirit of participants' demands. We hypothesize that this dismissal was partially due to the panel's depth of knowledge about the existing legal and technical structures that could be utilized to effect change: the panel discussed how realizing collective demands would be difficult to implement (e.g., quantifying harm for reparations) or could have negative consequences (e.g., facilitating filter bubbles). Instead, the panel tended to favor incremental reform or punitive measures compatible with existing legal structures or even inaction, in spite of the emotionally resonant frustration underlying collective concerns with the inciting PVEIs. Indeed, we observed the panel defending the offending institution and/or absolving it of responsibility owing to a presumption of good intentions. This misalignment between people and experts could contribute to people's impression that they are unable to effect change, despite their privacy concerns [10].

6 DISCUSSION

Today, there is a wide power chasm between individuals and the data harvesting institutions who collect, process and monetize their personal data. With our FFV sensitizing concept, we envisioned a future in which people can come together with one unifying voice to demand change when these institutions commit egregious privacy violations. Such a future is not necessarily far-fetched: as we found in our evaluation of our concept, a collective can empathize and advocate for strangers and rapidly converge on a small set of concerns and compensatory action; however, they require expert stewardship to translate their desires for broad, systemic change into actionable steps. On the other hand, S&P experts, while sympathetic to the sentiment of the collective, were generally pessimistic of the collective's desire for systemic change. They preferred, instead, working within the system for incremental reform.

6.1 Towards a platform that facilitates grassroots privacy collective action

Prior work by Shaw has unpacked models of online collective action and proposed stages of computer-supported collective action (CSCA) that align with our findings. Our artifact focuses primarily on the second stage—*Generate and debate ideas*—of Shaw's model, but also speaks to the first stage—*Identifying a problem*. However, there are still three other phases in the model: coordinating and preparing to take action, actually taking the action, and reflection after the action is taken. Das et al. scoped out a vision for future work spanning *all* of the CSCA phases in the context of end-user privacy [17], and Vincent et al. proposed a framework for some of the types of actions that users can take as leverage against privacy-violating institutions [53]. Some tools for facilitating subversive privacy collective action already exist, but are not yet directly integrated into broader, coordinated efforts: e.g., AdNauseum [30] aims to protect users from tracking advertisers by silently clicking on blocked ads to send noisy data back to advertisers; similarly, TrackMeNot sends "ghost queries" to search engines to obfuscate users' actual searches [42]. We thus envision a rich future design landscape that includes systems or processes that help people coordinate in a more sophisticated manner than a series of surveys; that allow people to effectively take leveraging action against PVEIs; and that clearly communicate the progress that they have made.

An open question for future work is how to move from our sensitizing FFV to a self-contained system through which collectives can effectively act in the real world. From our sensitizing concept, we saw the utility of canvassing collectives to take an inciting PVEI and giving them a platform to collectively compose demands for redress. Participants felt clearer about their own stances on PVEIs after being asked to extract concerns from them, more alert about the PVEIs in their own lives, and more incensed to take action of their own. We also witnessed a shared sense of social responsibility that people had for injustices faced by strangers.

Work by Abebe [8] has also examined broader trends of the role of computing in social change, which can be used to understand the potential for future online platforms for collective action. More specifically, our work fits several roles of computing in social change categorized by Abebe [8]. Using Abebe's terms, as a *diagnostic*, a future platform that allows users to voice their concerns about institutional privacy violations would help us measure and understand what the public wants. As a *formalizer*, such a platform can concretize these concerns via collective-powered sensemaking, be it through voting, external governance, or sophisticated topic modelling. As a *rebuttal*, it highlights the growing gap between individual users and institutional priorities. And as *synecdoche*, it exposes glaring tensions of reform versus revolution, with security experts who have a stake in upholding existing institutions on one side, and users on the other, respectively.

6.2 Reformist vs. non-reformist reform

The philosopher Andre Gorz made a distinction between reformist and non-reformist reforms [27]. Reformist reform is the incremental updating of existing structures and is pursued with no intention of ultimately modifying the structure of society and institutions, and instead aims to keep a calm status quo. Many of the solutions raised by experts, which included FTC consent decrees, heavier fines, and federal best-practice standards, fall into the broad category of reformist reform. Such solutions bolster the punitive power of existing regulatory institutions (e.g., the FTC) or encourage institutions that are responsible for PVEIs to develop methods to circumvent fines (e.g., Equifax), rather than tip the power imbalance in favor of the people.

Non-reformist reform, in contrast, challenges entrenched power structures. It originates "not in terms of what is possible within the framework of a given system and administration, but in view of what should be made possible in terms of human needs and demands" [27]. As an example, some participants (and even one expert) were deeply unhappy with the lack of consent to financial surveillance by Equifax, and worried that lack of regulation meant that other corporations could also misbehave with little recourse. In response, they wished for reparations bequeathed directly to those who were affected, rather than fines collected by a government entity. In short, even if they personally held grander desires for systemic change in privacy, experts' assessments of collective demands suggests that while the people want non-reformist reform, experts view only reformist reform as tenable.

6.3 The role of experts

Perhaps owing to this disconnect, some experts explicitly said they did not want to get involved with stewarding collectives or interpreting their desires owing to the perceived lack of knowledge non-experts had about "how the world works". Others had trouble seeing outside of the context of existing frameworks of heavy fines or legal settlements. Our findings illustrated a misalignment between non-expert end-users and S&P experts in their demands for how institutions can collect and manage personal data. Many S&P experts are themselves embedded in institutions that are responsible for PVEIs, even if their goal is to effect change from within. Others are experts precisely because of their in-depth knowledge of existing systems. Perhaps due to their immersion in these institutions, we found that the experts we interviewed tended to be more dismissive of general demands for sweeping action or large changes.

As Rahwan argues, however, it is impossible for any one person to be fully informed on all aspects of some policy question: public opinion, which shapes social norms and morals, should be used as a check on the "sovereign force" of experts, and influence the metrics by which expert performance is evaluated [45]. Extending calls from prior work on the privilege that researchers hold in designing for vulnerable populations [23, 40], we implore S&P experts who work on improving user privacy protections to consider the role they play in bolstering the power chasm between institutions and the individuals whose personal data they exploit.

Are we working towards reform or revolution—and how does that orientation align with the objectives of those for whom we advocate or design? We, the authors of this paper, recognize our own role in upholding this power chasm as "S&P experts" ourselves. One avenue future work might explore is developing a scaffolded process—much like the one we explored for collective demand generation here—that opens a line of communication between expert stewards and the collective to facilitate collaborative refinement of demands. This line needs to be a constant dialogue with devotion to repair and maintenance [32], rather than a one-off panel of experts. At the same time, in the same flavor as Irani and Silberman [33], being able to synthesize and funnel end-user privacy concerns into existing regulatory frameworks will not make us (and other experts) design saviors of user privacy; the experiences of end-users themselves, and the work they contribute to collective movements, must remain the driving force of action.

Feminist ethicist Carol Gilligan also distinguishes an "Ethics of Justice" (EoJ) from an "Ethics of Care" (EoC) [25]. Dominant groups tend to prefer an EoJ, which focuses on generalizable standards, impartiality, and a respect for Western democratic ideals. In contrast, an EoC system emphasizes benevolence and the importance of a response to the individual. The panel—in their emphasis on fitting collective demands within existing legal and technical structures—demonstrated alignment with a dominant EoJ. But perhaps what people affected by PVEIs need is for S&P experts to adopt an EoC: people know that what they want is unrealistic, yet they want to be heard and they want change.

6.4 Limitations

Our expert panel, though varied in background and industry, was comprised of only eight experts, all of whom were based in the United States. We juxtapose the diversity of their experiences against their near unilateral preference for working within existing institutional structures and against more sweeping action. However, we acknowledge that cultural norms around privacy regulations differ around the world; future work could explore differences in how experts respond to populist calls for systemic changes based on the regulatory contexts in which they operate.

Secondly, we ran only three scenarios through our FFV artifact, and these scenarios do not represent all the ways participants could have identified concerns or proposed demands. However, the emotionally-charged responses we did get from these scenarios support the argument that users lack representation as collectives working against institutions.

Finally, the use of Prolific itself could present limitations. For one, since our participants were paid, they do not necessarily reflect how a grassroots collective would act in the real world. And, while there have not been studies specifically comparing Prolific users' security attitudes with "average" users, prior work on the representativeness of users on Amazon Mechanical Turk (MTurk), a similar crowd work platform, has shown mixed results. For example, Kang et al. [36] found that MTurk users have higher privacy concerns and were better-educated about S&P than the larger U.S. public. In contrast, Redmiles et al. [46] found that MTurk users were fairly representative of the U.S. population in S&P experiences and education.

7 CONCLUSION

In this paper, we explore how to design a system that facilitates privacy collective action by helping collectives affected by PVEIs generate a unified set of demands for redress. Specifically, we employed a three-stage set of online questionnaires, inspired by the Find-Fix-Verify crowd programming pattern [12], as a sensitizing concept to explore how non-expert collectives can generate concerns and compensatory demands in response to a triggering PVEI. We then presented the results of this artifact to a panel of S&P experts, whose responses helped us not only assess the collective's demands, but also uncover insights into how experts might better steward collectives towards effecting enduring change in privacy practices.Finally, we discussed how our results fit into existing paradigms of computing for social change, and how even well-meaning experts might serve as hurdles to further institutional privacy change. People are frustrated with how their personal data is collected, processed and monetized, but may not have the knowledge to effect meaningful change. Experts have that knowledge, but can be dismissive of those for whom they should advocate. A synergy between expert stewards and the crowds of non-experts fed-up with existing privacy protections could be the foundation for broader change that helps shift power over personal data to the people.

ACKNOWLEDGMENTS

This work was generously supported, in part, by NSF Grant #1755625. Conversations with Peter Swire and DeBrae Kennedy-Mayo helped shape some of our framing of this work. We thank our expert panelists, who agreed to provide their perspectives without compensation. We also thank our anonymous reviewers for being generous with their time and helping us improve the paper.

REFERENCES

[1] [n. d.]. Cybersecurity Resource Center: Cybersecurity Incidents. *U.S. Office of Personnel Management* ([n. d.]). https://www.opm.gov/cybersecurity/cybersecurity-incidents/
[2] [n. d.]. Stop Watching Us. *StopWatching.Us* ([n. d.]). https://optin.stopwatching.us/
[3] 2017. Don't let EQUIFAX escape liability! *Change.org* (2017). https://www.change.org/p/don-t-let-equifax-escape-liability
[4] 2017. Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes. *Equifax* (Sep 2017). https://investor.equifax.com/news-and-events/press-releases/2017/09-15-2017-224018832
[5] 2020. Restore the Fourth - Opposing unconstitutional mass government surveillance. *Restorethe4th.com* (2020). https://restorethe4th.com/
[6] 2020. r/privacy - I think I accidentally started a movement - Policing the Police by scraping court data. https://www.reddit.com/r/privacy/comments/gr11aw/i_think_i_accidentally_started_a_movement/
[7] 2020. r/privacy - If cops can watch us, we should watch them. I scraped court records to find dirty cops. https://www.reddit.com/r/privacy/comments/gm8xfq/if_cops_can_watch_us_we_should_watch_them_i/
[8] Rediet Abebe, Solon Barocas, Jon Kleinberg, Karen Levy, Manish Raghavan, and David G Robinson. 2020. Roles for computing in social change. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. 252–260.
[9] Ben Adler. 2018. California Passes Strict Internet Privacy Law With Implications For The Country. *NPR* (Jun 2018). https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country
[10] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. *Pew Research Center* (Nov 2019).
[11] W Lance Bennett and Alexandra Segerberg. 2012. The logic of connective action: Digital media and the personalization of contentious politics. *Information, communication & society* 15, 5 (2012), 739–768.
[12] Michael S Bernstein, Greg Little, Robert C Miller, Björn Hartmann, Mark S Ackerman, David R Karger, David Crowell, and Katrina Panovich. 2010. Soylent: a word processor with a crowd inside. In *Proceedings of the 23nd annual ACM symposium on User interface software and technology*. 313–322.
[13] Glenn A Bowen. 2006. Grounded theory and sensitizing concepts. *International journal of qualitative methods* 5, 3 (2006), 12–23.
[14] Virginia Braun and Victoria Clarke. 2019. Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health* 11, 4 (2019), 589–597.
[15] Victoria Clarke, Virginia Braun, and Nikki Hayfield. 2015. Thematic analysis. *Qualitative psychology: A practical guide to research methods* (2015), 222–248.
[16] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A typology of perceived triggers for end-user security and privacy behaviors. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*.
[17] Sauvik Das, W Keith Edwards, DeBrae Kennedy-Mayo, Peter Swire, and Yuxi Wu. 2021. Privacy for the People? Exploring Collective Action as a Mechanism to Shift Power to Consumers in End-User Privacy. *IEEE Security & Privacy* 19, 5 (2021), 66–70.
[18] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 143–157.
[19] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. 2015. The role of social influence in security feature adoption. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. 1416–1426.
[20] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.
[21] Jenny L Davis and Nathan Jurgenson. 2014. Context collapse: Theorizing context collusions and collisions. *Information, communication & society* 17, 4 (2014), 476–485.
[22] Paul Ekman. [n. d.]. Basic emotions. *Handbook of cognition and emotion* 98, 45-60 ([n. d.]), 16.
[23] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. " Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.
[24] Shirley Gaw and Edward W Felten. 2006. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security*. 44–55.
[25] Carol Gilligan. 1993. *In a different voice: Psychological theory and women's development*. Harvard University Press.
[26] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. 2018. "What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 1549–1566.
[27] A. Gorz, M. Nicolaus, V. Ortiz, V.O. González, and Beacon Press (Boston). 1967. *Strategy for Labor: A Radical Proposal*. Beacon Press. https://books.google.com/books?id=IPtAAAAAIAAJ
[28] Joseph L Greenslade. 1988. Labor unions and the Sherman Act: rethinking labor's nonstatutory exemption. *Loy. LAL Rev.* 22 (1988), 151.
[29] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*. 133–144.
[30] Daniel C Howe and Helen Nissenbaum. 2017. Engineering Privacy and Protest: A Case Study of AdNauseam.. In *IWPE@ SP*. 57–64.
[31] Shih-Wen Huang, Minhyang Suh, Benjamin Mako Hill, and Gary Hsieh. 2015. How activists are both born and made: An analysis of users on Change.org. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 211–220.
[32] Lilly Irani and M Six Silberman. 2014. From critical design to critical infrastructure: lessons from turkopticon. *Interactions* 21, 4 (2014), 32–35.
[33] Lilly C Irani and M Six Silberman. 2016. Stories We Tell About Labor: Turkopticon and the Trouble with" Design". In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 4573–4586.
[34] Haojian Jin, Hong Shen, Mayank Jain, Swarun Kumar, and Jason I. Hong. 2021. Lean Privacy Review: Collecting Users' Privacy Concerns of Data Practices at a Low Cost. *ACM Trans. Comput.-Hum. Interact.* 28, 5, Article 34 (aug 2021), 55 pages. https://doi.org/10.1145/3463910
[35] Brittany Kaiser. 2017. Tell Facebook: Our Data is our Property #OwnYourData. *Change.org* (2017). https://www.change.org/p/tell-facebook-our-data-is-our-property-ownyourdata
[36] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy attitudes of mechanical turk workers and the us public. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 37–49.
[37] Travis Kriplean, Jonathan Morgan, Deen Freelon, Alan Borning, and Lance Bennett. 2012. Supporting reflective public thought with considerit. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*. 265–274.
[38] Gerald Marwell and Pamela Oliver. 1993. . Cambridge University Press, i–iv.

[39] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J Aviv. 2021. " Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *30th {USENIX} Security Symposium ({USENIX} Security 21)*.
[40] Nora McDonald, Karla Badillo-Urquiola, Morgan G Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J Wisniewski. 2020. Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–8.
[41] Ellen Nakashima. 2019. Hacks of OPM databases compromised 22.1 million people, federal authorities say. *The Washington Post* (Apr 2019). https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/
[42] Helen Nissenbaum and Howe Daniel. 2009. TrackMeNot: Resisting surveillance in web search. (2009).
[43] Nicole Perlroth. 2016. Yahoo Says Hackers Stole Data on 500 Million Users in 2014. *The New York Times* (Sep 2016). https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html
[44] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. 1–17.
[45] Iyad Rahwan. 2018. Society-in-the-loop: programming the algorithmic social contract. *Ethics and Information Technology* 20, 1 (2018), 5–14.
[46] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1326–1343.
[47] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 272–288.
[48] Alan Rusbridger and Ewen MacAskill. 2014. Edward Snowden interview: the edited transcript. *The Guardian* (Jul 2014). https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript
[49] Niloufar Salehi, Lilly C Irani, Michael S Bernstein, Ali Alkhatib, Eva Ogbe, and Kristy Milland. 2015. We are dynamo: Overcoming stalling and friction in collective action for crowd workers. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 1621–1630.
[50] Aaron Shaw, Haoqi Zhang, Andrés Monroy-Hernández, Sean Munson, Benjamin Mako Hill, Elizabeth Gerber, Peter Kinnaird, and Patrick Minder. 2014. Computer supported collective action. *Interactions* 21, 2 (2014), 74–77.
[51] Erik Stolterman and Mikael Wiberg. 2010. Concept-driven interaction design research. *Human–Computer Interaction* 25, 2 (2010), 95–118.
[52] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *proceedings of the eighth symposium on usable privacy and security*. 1–15.
[53] Nicholas Vincent, Hanlin Li, Nicole Tilly, Stevie Chancellor, and Brent Hecht. 2021. Data Leverage: A Framework for Empowering the Public in its Relationship with Technology Companies. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. 215–227.
[54] David Watson and Lee Anna Clark. 1999. The PANAS-X: Manual for the positive and negative affect schedule, expanded form. (1999).
[55] Sidney Webb and Beatrice Webb. 1920. *The history of trade unionism*. Longmans, Green.
[56] Qian Yang, Nikola Banovic, and John Zimmerman. 2018. Mapping machine learning advances from hci research to reveal starting places for design innovation. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–11.
[57] Haoqi Zhang, Andrés Monroy-Hernández, Aaron Shaw, Sean Munson, Elizabeth Gerber, Benjamin Hill, Peter Kinnaird, Shelly Farnham, and Patrick Minder. 2014. WeDo: end-to-end computer supported collective action. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 8.
[58] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. 2018. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 197–216.

A INCITING PVEIS

A.1 Equifax data breach scenario

"In 2017, a large chunk of my personal info was leaked by Equifax. That included my name, date of birth, Social Security number, address, and other small things that I might not even know about.

First I heard in the news that millions and millions of people, many of whom didn't even know Equifax had this info about them, had their data leaked. I had to find out through this online tool that I was one of those people.

Equifax kind of just said, 'This happened', and then offered a year of credit monitoring. That doesn't cover the damage or the surprise that my info was being collected in the first place, much less mishandled. They didn't really address the mishandling. I thought, "If millions of people have had their information leaked, they've gotta fix something – regulation, laws, whatever. You can't just work like that." So I didn't do anything about it.

I guess if you participate in the modern world – buying a car, a house, anything – you end up consenting to being tracked. Instead there was a year of credit monitoring and a settlement. The total payout wasn't based on all the millions of people who were actually hurt; it was just some big capped chunk of money. It wasn't about fixing things for the people who were affected but about dealing the maximum punishment to Equifax. Nothing was made better for us."

A.2 Instagram profiling scenario

"Whenever I go to search for someone on Instagram, it gives you recommended Instagram posts. In their recommendations I'm accosted by, like, 98% pictures of buff, half-naked men.

I'm a gay man. I'm married to a gay man. So, sure, I get it. But most of my posts about baking and cooking and I primarily even use hashtags related to those things in my posts. Maybe a couple posts with '#husband' or whatever, but... I mean, why? It's kind of offensive, as if Instagram's only idea of me is that I'm a gay man so I should like these pictures of half-naked dudes.

Sometimes, when I'm at work and want to show pictures of my nephews and nieces to my coworkers, I'll open up Instagram and go the the search page, and then I'm bombarded with all these images that are inappropriate for work and that I didn't even ask for. It's embarrassing!

When I open up the search page, I wonder, 'Why was I reduced to this?' It's a terrible thing to interact with. Me being gay is not my defining category. I love to cook; I love science; I love playing board games. I wonder, if I look into their algorithm, next to my name it just says 'GAY' in big rainbow letters."

A.3 OPM data breach scenario

"When OPM (Office of Personnel Management of the United States Government) lost a ton of people's personal info, I was affected. I was younger when it happened so I didn't realize the gravity of the situation, and they didn't really explain it well either—they were just like, 'Hey, this little slip-up happened, so we're gonna provide identity theft protection for you for the next 5 years.' At the time, I thought, 'Oh, how nice of them.' I didn't realize how much it could impact me, and thankfully nothing major happened, but I was stupid. I was just by myself, trying to interpret federal bureaucracy.

My identity does get a lot of pokes and prods because I work for the government, but any time I get a new alert from that ID theft protection service it's still heart-pounding. One time I didn't sleep for two nights in a row because I couldn't figure out why there was a new alert. I was terrified every time I got a new email from them. While their service keeps track of your stuff it doesn't give

you much detail on what's actually happening to you. They also just signed me up for it automatically; I didn't get a choice.

It's been a long time since that breach, but I'm always looking over my shoulder because of it. I've never gotten any follow-up from OPM since them either. They've never told me how they've changed. They've never really told me, 'Hey, we've improved. You can trust us again.' And I don't."

B FIND-FIX-VERIFY QUESTIONNAIRES

B.1 Find Phase Questionnaire

(1) The following passage contains an actual American adult's account of their experiences. Please read it carefully. {Randomly display one of three PVEIs}
(2) Please select two words that describe your emotional reaction to {institution's} actions in this account.
- happy
- sad
- afraid
- disgusted
- angry
- surprised

(3) Why did you choose these words?
(4) Please list out two things {institution} did in this account that made you uncomfortable. Use direct quotes from the passage and explain why.

B.2 Fix Phase Questionnaire

(1) The following passage contains an actual American adult's account of their experiences. Please read it carefully. {Randomly display one of three PVEIs}
(2) In response to this account, XX% of people previously surveyed felt {emotion 1} or {emotion 2}.
(3) Some previously surveyed people also brought up the following concerns about {institution} in the above account. Please select two that you believe should be prioritized the most.
- Random find-phase concern A
- Random find-phase concern B
- Random find-phase concern C
- Random find-phase concern D
- Random find-phase concern E

(4) Which of the concerns that you chose would you prioritize most?
- Chosen concern A
- Chosen concern B

(5) You selected the following concern to prioritize the most: {Chosen concern A}. Please choose one party that you would want to be involved in taking action to address this concern:
- {institution}
- Everyone affected by {PVEI}
- Governmental agencies, regulatory bodies
- Other third parties: {free text}

(6) What actions would you want the party you selected to take in order to address this concern?
(7) You selected the following concern to prioritize second: {Chosen concern B}. Please choose one party that you would want to be involved in taking action to address this concern:
- {institution}
- Everyone affected by {PVEI}
- Governmental agencies, regulatory bodies
- Other third parties: {free text}

(8) What actions would you want the party you selected to take in order to address this concern?
(9) How do you feel after expressing your opinion on these concerns?

B.3 Verify Phase Questionnaire

(1) The following passage contains an actual American adult's account of their experiences. Please read it carefully. {Randomly display one of three PVEIs}
(2) In response to the account that you just read, some previously surveyed people highlighted the parts of the account that they found most concerning. Please select two that you believe should be prioritized the most.
- Random fix-phase concern A
- Random fix-phase concern B
- Random fix-phase concern C
- Random fix-phase concern D
- Random fix-phase concern E

(3) In response to the concerns that you just saw, some other previously surveyed people prescribed actions that they believed OPM could take to address them. You'll be asked to evaluate some of these actions. Keep in mind the following criteria to evaluate the prescribed actions:
   (a) **Specificity**. Does the action include specific tasks or steps for OPM to take?
   (b) **Effectiveness**. How well does the action address the concern?
   (c) **Desirability**. How much would you like this action to be implemented?

(4) You selected the following concern to prioritize the most: {Chosen concern A}.
(5) Please rank the following actions that others have prescribed for {entity} to take to address this concern, with rank 1 being the best. You can do so by moving your cursor over the choices and dragging and dropping them. Please keep in mind the specificity, effectiveness, and desirability of the actions.
- Entity action A for chosen concern A
- Entity action B for chosen concern A
- Entity action C for chosen concern A
- Entity action D for chosen concern A

(6) You selected the following concern to prioritize the most: {Chosen concern B}.
(7) Please rank the following actions that others have prescribed for {entity} to take to address this concern, with rank 1 being the best. You can do so by moving your cursor over the choices and dragging and dropping them. Please keep in mind the specificity, effectiveness, and desirability of the actions.
- Entity action A for chosen concern B
- Entity action B for chosen concern B
- Entity action C for chosen concern B

- Entity action D for chosen concern B