"WTH..!?!" Experiences, reactions, and expectations related to online privacy panic situations *

Julio Angulo
Karlstad University
Karlstad, Sweden
julio.angulo.r@gmail.com

Martin Ortlieb
Google
Zürich, Switzerland
mortlieb@google.com

ABSTRACT

There are moments in which users might find themselves experiencing feelings of panic with the realization that their privacy or personal information on the Internet might be at risk. We present an exploratory study on common experiences of online privacy-related panic and on users' reactions to frequently occurring privacy incidents. By using the metaphor of a *privacy panic button*, we also gather users' expectations on the type of help that they would like to obtain in such situations. Through user interviews ($n = 16$) and a survey ($n = 549$), we identify 18 scenarios of privacy panic situations. We ranked these scenarios according to their frequency of occurrence and to the concerns of users to become victims of these incidents. We explore users' underlying worries of falling pray for these incidents and other contextual factors common to privacy panic experiences. Based on our findings we present implications for the design of a help system for users experiencing privacy panic situations.

1. INTRODUCTION

With so many of our daily activities spent interacting with information technologies and so much of our personal data being stored and handled online, the chances that an unexpected, unwelcome privacy-related incident occurs at some point in our lives are not very unlikely. New privacy- or security-related incidents are regularly reported through various channels, like news, blogs and collaboratively maintained databases. A report from security company Symantec [58] in 2014 described a worrisome increase of attacks on online services over earlier years, which have resulted on breaches to their customers' data records. However, there are other kinds of privacy-related incidents which can affect individual users directly and emotionally during their daily interactions with online services. We are talking about incidents that, if they occur, might lead users to experience physical symptoms similar to a person in distress (i.e., momentary shortness of breath, accelerated heart rate, rushed adrenaline, tensing of the muscles, etc.). We refer to these cases as *online privacy panic* situations. Such situations might lead users to worry about the possible concequences of the breach to their privacy, which may include losing one's job, being financially defrauded, or even endure physical harm or damage to one's property.

Previous research has studied isolated privacy incidents (e.g., [49], [55], [65] and others), however, as far as we know, no one has tried to capture users' previous experiences of a range of common incidents. Our intention in this paper is to unveil and understand common online privacy panic situations. We investigate some of the contextual factors that characterize such situations, as well as strategies that people take to deal with them. Moreover, we use the metaphor of a *panic button* to investigate users' expectations and mental models of suitable help mechanisms that could lead these users towards a solution, calming their distress, and preventing similar episodes from happening in the future.

To this end, we report on a study consisting of semi-structured interviews ($n = 16$) and a survey ($n = 549$). From the obtained data we identified 18 different cases of online privacy panic. Victims' topmost worries included possible harm to their finances or fear of embarrassment, as well as third-parties knowing things that might not be of their business. Among the most memorable self-reported panic stories were cases of account hijacking and 'leakage' of personal data, while incidents involving regrets when sharing content online were found to be experienced most frequently. However, scenarios related to the loss of online data, the loss of a mobile device, or falling pray of identity theft also were at the top of users' concerns. Our findings also indicate that, in the case a service provider were to offer a hypothetical *privacy panic button*, users would expect that the help provided is immediate, uncomplicated, actionable, and in-place. From the results of our study, we present implications for the design of a help system for users experiencing online privacy panic situations.

The rest of this paper is structured as follows. First, we present related work on Internet users' privacy concerns in Section 2.1, as well as research studies which look at different aspects of common privacy incidents in Section 2.2. We then introduce in Section 3 the methodologies used to study users' experienced privacy incidents, including the recruitment of study participants and report on the results obtained. From our findings we present in Section 4 implications for the

*(Produces the permission block, and copyright information). For use with SIG-ALTERNATE.CLS. Supported by ACM.

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

design of a possible help system for privacy panic situations. We end with concluding remarks in Section 5.

2. RELATED WORK

In this section we present work related to the study of people's privacy concerns on the Internet and on known privacy incidents that might cause people to experience feelings similar to panic, fear or distress while acting online.

2.1 Users' privacy concerns

Plenty of studies have tried to measure users' privacy concerns on the Internet. For instance, just over a decade ago Earp et al. [16] developed an instrument which indicated that people's primary privacy concerns had to do with the way their personal information was transfered, stored and accessed on the Internet. A follow-up study in 2010 revealed that the types of privacy concerns have not varied much over the years but the levels of these concerns have increased considerably [4]. In 2004, Malhotra et al. [36] introduced the Internet Users' Information Privacy Concerns scale, which tries to capture users levels of concerns with regards to the amount of data collection, the control users have over their data and the awareness they have about service providers' privacy practices. Buchanan et al. [7] developed scales based on the Westin index [27] to understand people's level of technical protection and general caution on the Internet, as well as their level of privacy concerns. Alan Westin himself developed the Privacy Segmentation Index [27], which categorizes individuals' responses into privacy fundamentalist, pragmatist and unconcerned. However, other studies have shown that Westin's categories may be inaccurate predictors of people's real privacy attitudes and behaviours [66].

Despite the efforts of trying to find appropriate measurements of privacy concerns, a survey done in 2002 [21] asked open-ended questions related to people's use of the Internet and found that people's concerns with the Internet had less to do with notions of privacy and more with worries about falling victim to crimes like credit card theft [39]. Another study also found that individuals tend to exhibit optimism biases with relation to online privacy risks, believing that they are less vulnerable to these risks than others [10].

Our study departs from previous studies by focusing on exploring users' actual past experiences with privacy related incidents online. We started our investigation by asking the question '*what are common privacy incidents that are likely to trigger feelings of fear or extreme concern on Internet users with regards to their privacy or personal data?*'

It has been noted that having been a victim of a privacy incident can be closely intertwined with a person's reported levels of privacy concerns [14]. It can be argued that it is the multidimensional [13, 23], dynamic [40] and temporal processes of privacy which can create a change in people's privacy concerns as a result of negative past experiences. All of these, may encourage people to modify their behaviour and become more alert about their future actions online. At the same time, experiencing some kind of privacy incident (or hearing rumors about an incident from someone else) might motivate people to take preventive measures, thereby reducing their privacy concerns for the future, paradoxically making them more vulnerable for incidents later on (e.g., believing that setting up a firewall at one point in time will protect their computer from all future viruses).

In 2009, Paul Buta [8] observed that many of people's privacy-related fears are often induced by reports from alarmist media. He suggests steps to diffuse the panic by taking measures to protect one's privacy. However, some of these might be outdated in today's online environments, like the PrivacyBird tool [12]. Buta's work does not explore people's actual lived experiences of privacy-related panic situations. Our investigations attempt to fill this gap.

2.2 Potential panic evoking privacy incidents

Scenarios related to regretting sharing something on online social networks have been studied by Wang et al. [63], who examined some of the causes for regretting sharing posts on Facebook and reported on the repercussions that certain posts can have on people's lives. Simiarly, Sleeper et al. [55] explored users' sharing regrets while using Twitter as opposed to regrets during in-person conversations. They found that most people regretted sending messages on Twitter if the message revealed too much information or if it expressed criticism towards the recipient, and that most of regretted messages were posted at a time when users were in a highly emotional negative state. Other studies have looked at the concerns of sharing something with unintended audiences and its consequences to the users' reputation [6, 29, 57, 61].

Losing control of one's reputation online due to the content posted by others is also a potential trigger for sudden feelings of fear. Appropriately managing one's reputation is a serious challenge not only because content, once posted on the Internet, becomes very hard to remove, but also because harm to one's reputation online can translate into irreversible real-world problems, such as limiting job opportunities or damaging social relationships. Woodruff [65] has looked at the strategies people take when realizing that content about them has appeared online. Participants in her study expressed feelings of disempowerment when trying to remedy their damaged reputation, also stating that managing one's online reputation is a burdensome and unpleasant task, yet it is necessary. Madden & Smith [34] also explore how people have adapted their behaviours to control privacy settings in social networks and manage their online identities as measures to protect their reputation.

Lampinen et al. [29] also recognize the difficulty of managing the divide between privacy and publicness. The authors report on the issue that arise when third-parties turn one's private content public, thereby revealing too much of others' lives, for example, uploading someone else's picture into a social network site and the feelings of powerlessness this can create. These are actions that, although they might not carry long term consequences to the first-party's reputation, can cause embarrassment and shame. When looking at third-party sharing at a bigger scale, Rader [43] has studied people's concerns with regards to behavioural tracking commonly performed by online services, suggesting that (even) people who are aware of so-called *first party* behavioural tracking are less aware of third-party aggregation of their data and hence are more prone to be concerned about unwanted access. Similarly, Sipior et al. [54] summarized users' concerns with regards to web tracking technologies, and found that users are unaware of web tracking and that they feel exposed and traspassed when they find out about it. Moreover, a report on transparency-enhancing tools also stated that emotions of astonishment, surprise and distress were evoked in non-savvy users by the realization that online

companies collect information and analyze data about them which is more than what they have explicitly consented to disclose [3].

Data being handled, shared and aggregated at different services may lead to higher probabilities for the occurrence of identity theft, profiling and other attacks. Identity theft is a major cause of concern due to the long term repercussions that can linger in the victims' lives [5], as well as to the costs to society and to the individual. A 2009 survey reported that people in the U.S. worry much more about being victims of identity theft than home burglary, getting their car stolen or terrorism [45]. Anderson [2] has examined the likelihood of becoming a victim of identity theft based on the person's demographic characteristics, concluding that people with higher incomes, women, adults living alone in the household have higher risks of getting their identity stolen. As a way to combat identity theft, Lai and Hsieh [28] propose a framework for studying the factors that influence people in adopting identity protection strategies.

Many cases of identity theft occur after an intruder successfully infiltrates or takes control of the accounts of an individual at one or many online services. Thus, the event of having an account hacked or hijacked can be another important trigger of users' panic. Shay et al. [49] surveyed to understand users' attitudes and experiences with account hijacking. The researchers found that around 30% of their survey participants had been victims of some form of account hijacking. Compromised accounts were usually valuable, and the incident had a deep emotional impact on the victims. Beyond academic studies, narrations from people who got their account hijacked and the consequences of their misfortune are not hard to find in blogs, news and social media. One famous story was told by technology journalist Matt Honan [22] who narrated his moment of panic when he realized that access to his iPhone and iCloud accounts were being blocked. Security flaws on Amazon and AppleID systems allowed a hacker to get access to his Twitter account, with the purpose of controlling Mat's convenient Twitter user name (*@mat*). Matt's documents, family photos, emails were deleted in the process.

Matt's story is connected to the findings reported by Ion et al. [24] which indicate that people are still sceptical about moving their personal data into the cloud for fear that their files would be leaked, compromised or inaccessible, and because of their uncertainty on how their files are being accessed and used by other parties. Similarly, Clark et al. [11] showed the mismatch between users expectations about what they are sharing in the cloud and the real disclosures they make.

Losing valuable data located on the cloud because of its inaccessibility or malfunction of the service provider can also be a source of annoyance and/or fear, similar to losing one's laptop or mobile device. Surveys reveal that around 30% of people in Canada, the US and the U.K., have experienced the theft or loss of a mobile device, and owners of lost devices often do not have a locking mechanism on their device [17, 58]. Even with recent apps that help users locate their missing smartphones, such as 'Find my iPhone', 'Android Lost' or 'Android Device Manager', large number of devices are reported lost or stolen. Tu Z. & Yuan Y. [60] suggest a behavioural study on the risks and users' coping measures in the event of losing their mobile devices or getting them stolen. They claim that adopting concepts from Protection Motivation Theory can help understand the users' active or passive reactions in case of falling victims to this event.

Some privacy-related news as portrayed by the media can also be a source of panic. Security incidents reported in recent years, such as the Heartbleed bug [15] or Shellshock [19], created a state of momentary fear and concern specially among users who might not understand all the consequences to their privacy and who might get alarmed by the way the media portrays the incident. The revelations made by Edward Snowden starting in 2013 about the governments' surveillance initiatives, were a reason for making people worried about their government spying on them [32].

News about corporations being victims of hacking attacks are also frequently being reported by the media. Each attack can carry risks of leaking the services' customer personal data to the public, such as home addresses, credit card information, personal habits and more. As an example, the attack in 2014 to the messaging service Snapchat and to Apple's cloud service iCloud, leaked a great amount of sensitive personal images on the Internet [38]. The increasing number of attacks to corporations are documented and advertised in online databases, such as `http://datalossdb.org/`, `http://osvdb.org/` and `http://www.privacyrights.org/data-breach`, which tend to be collaboratively maintained by groups of privacy and security advocates.

Surely, many other types of incidents exist than the ones summarized in this section. Taking some of this related work as the base of our study, our intention is to unveil incidents – and the context of these incidents – that are commonly experienced by Internet users and which potentially evoke sudden feelings related to panic and fear.

3. METHODOLOGY

In this paper we report on the results from two data collection activities. First, we carried out a series of user interviews with 16 participants with the purpose of collecting stories of privacy-related incidents, as well as their concerns to become victims to other similar incidents. Then, we validated and complemented the findings from the interviews by analyzing the submissions of 549 respondents to a survey. The following subsections describe the goals, design and administration of these activities.

3.1 Interviews

We started our investigations by laying out a list of common scenarios that can potentially trigger privacy-related panic. These scenarios were identified though a combination of our own experience working with various privacy challenges, discussions with colleagues experts in the field of privacy, common incidents reported by the media, and the available research literature, some of which was presented in Section 2.2. Table 1 presents descriptions of these 12 initially identified scenarios, which ranged from misfortunes such of identity theft, online stalking or threatening, or losing one's mobile device, to more common cases of sharing something online with the wrong audiences or regret sharing it, as well as others. Complete descriptions of these 12 cases can be seen in Appendix B.1.

3.1.1 Screener

Based on the identified scenarios and other questions about users' concerns and previous studies on privacy incidents, we designed a set of questions with the purpose of screening for

Table 1: Twelve initially identified triggers of privacy panic

Code	Panic scenario	Description
CSC	Changes in my social context	Realizing that someone who I used to be closed with, but whom I no longer trust (e.g., ex-partner, previous employer, old friend) still has access to my accounts or my personal information
DLK	My data was leaked online	Finding out that my personal data has being leaked or obtained by someone who I do not approve of
DLO	I deleted my data or I am not able to access it	Deleting or not being able to access my online data or data in an account that is valuable to me, such as documents, pictures, or other online files
HIJ	My account was hijacked or hacked	Finding out that someone has hacked my account(s) or accessed it without my permission or knowledge
IDT	My identity was stolen or misused	Finding out that someone else is using my identity and personal information to pretend to be me on the Internet
LMD	My mobile device was lost or stolen	Losing a mobile device (like a smartphone or tablet) or getting it stolen
MED	I saw an alert on the news or media	Finding out through the news and media that my privacy or personal data can be at risk
MSR	I regret having shared something online	Sharing something on the Internet and regret sharing it once it's too late
MSV	I shared content with the wrong people	Sharing something on the Internet and realizing that it can be seen by the wrong person or group of people
REP	My reputation was damaged	Someone else posting things or spreading rumours about me on the Internet which may damage my reputation privately or professionally
STK	I was being stalked, threatened or bullied	Feeling uncomfortable because someone seems to be stalking me, threatening, bullying or bothering me on the Internet
TPS	Third-parties shared data about me	Finding out that another person or a company has shared my personal information with others or posted information about me on the Internet without consulting me first

participants that could be invited for a one-on-one interview. After asking interested respondents for demographic information, the screener used 5-point Likert-scale statements to measure respondent's general privacy concerns and their concerns to fall victims for the initially identified panic scenarios.

The screener was distributed to a pool of about 600 people from approximately 15 different country locations who are registered on a platform that was built by the company where one of the authors works. The platform allows for people to voluntarily sign-up to participate in user studies. In the period of one week, we received a total of 128 responses. From these, 29 were female (1 didn't state gender), 78 had some form of employment, 35 were students, and 15 were not employed or retired. The majority (79) were between the ages of 24 and 40 years old.

Respondents to the screener also were encouraged to share similar stories of privacy-related panic that they had experienced. This allowed us to corroborate some of our initially identified scenarios. For instance, one respondent told how his reputation was at risk when "*someone was defaming my wife and me anonymously to my employer and friends*" (TP073), which can be seen as damage to his reputation (REP). Another respondent wrote that "*While I was in a relation with a previous partner, she had access to all my information and accounts as we had trust within each other. Eventually when the relationship ended I didn't feel it was appropriate to ask her to forget that information or delete it, as I thought it was common sense. Weeks later I noticed that someone besides myself was logging in to my accounts, changing information, reading my messages and so on*" (TP034), which is an example of the previously identified scenario of the person changing his social circumstances (CSC).

Table 2: Interview participants demographics

ID	G	Age	Location	Nationality	Profession	Privacy
TP008	M	18-23	Switzerland	Mexico	Engineering student	3.83
TP026	F	24-30	Germany	Poland	Sales representative	3.83
TP027	M	24-30	Slovakia	Slovakia	Financial advisor	2.33
TP030	F	24-30	UK	Malaysia	Medical doctor	4.00
TP053	F	31-40	Switzerland	USA	Business consultant	1.17
TP065	F	31-40	Switzerland	Switzerland	Secretary	1.67
TP069	M	31-40	Germany	Pakistan	Media enterpreneur	4.00
TP076	F	41-50	Portugal	Portugal	Web content creator	4.33
TP082	M	41-50	Switzerland	Switzerland	Security officer	1.83
TP085	F	41-50	UK	Caribbean	eCommerce director	4.00
TP089	M	51-60	Canada	Canada	Law enforcement	2.33
TP091	M	51-60	Switzerland	Switzerland	Civil engineer	3.00
TP093	M	51-60	Switzerland	Switzerland	Airport host	2.00
TP096	M	60+	Switzerland	Switzerland	Software support	3.17
TP097	M	24-30	Switzerland	India	Neuroscience student	4.17
TP105	M	24-30	UK	Italy	Retail store manager	5.00
TP056	M	31-40	Switzerland	India	Store assistant	2.67

3.1.2 Participants

We analyzed all responses of the screener trying to identify a group of about 15 to 20 participants for an additional one-on-one interview. We wanted to select a balanced group of ages, genders, location, familiarity with technology, and in particular people who we thought had a privacy panic story to tell. At the end, 17 out of the 128 respondents to the screener were invited to participate in an interview. The demographics of the selected participants along with their privacy concern score are shown in Table 2. Eight of the interviews were conducted remotely using a video conferencing system with screen-sharing capabilities. To 9 participants who were in reasonable distance to our location in Switzerland we extended invitations for a face-to-face interview. With one no-show (TP056), we had a total of 16 interviews.

Each interview session lasted around one hour and participants were compensated with the equivalent of a 50€ gift card for their time. In order to make use of the time more effectively, and as a way to refresh their memory with a privacy panic incident that they had recently experienced, each selected participant was asked to answer a short pre-questionnaire one or two days before the interview session took place. Questions asked about the context of their reported panic situation, the details of which were expanded upon during the interview.

An interview protocol (Appendix A.1) was prepared to maintain consistency across all sessions. The sessions were audio recorded after obtaining consent from participants, and recordings where later transcribed. To analyze the collected data, we used an inductive approach [59], which allows for simple and quick analysis of raw text data in order to extract relevant themes from the transcribed responses. Each test session was divided into two parts; the first part focused on participant's narrations of privacy incidents that they had experienced, and in the second part they gave their opinion about initial metaphors for a plausible "privacy panic button" that could help them in similar panic situations. Details of these are presented in the following sections.

3.1.3 Part 1 - Narrations of privacy incidents

In the first part, after building rapport with participants and introducing them to the study, they were asked to narrate any privacy incident that came to their mind which had caused them to experience feelings of discomfort. In particular, we started by asking the open question "*Have you ever been in a situation where you have felt a sudden feeling of panic, anxiety or distress for something related to your personal information or privacy on the Internet?*"

Participants reported different incidents and concerns that they either experienced in the past or that constantly preoccupied them in their daily Internet activities. Their responses broadly confirmed the panic scenarios that we had identified in the beginning. This was not surprising since we had primed them with similar situations. However, the collected responses helped us to understand each of the scenarios better, and provided a more complete angle to our initial views of these identified incidents. For instance, participant (TP065) told us that she took rigorous precautions to control the information that she or her family uploaded to the Internet, and recalled her feeling of panic when she suddenly realized that pictures of her daughter had been uploaded into a popular social network site by her own mother: "*I was shocked, because I am trying so hard not to post anything about her [my daughter], and then I see my mother [posting them]... It is just the feeling that you don't have total control of your data, [or] your family ...*". The participant in this case expressed her concern about the scenario in which family or friends may put her own privacy at risk without her been able to control it (TPS). Initially, we had considered third-parties to be service providers which shared the users' information, but the story from this participant helped us realize that third-parties could also refer to other people, and not only to online services. Table 7 of Appendix C lists the panic scenarios mapped to relevant quotes from interview participants who had experienced them.

We identified at least three important themes from other stories from the participant who we interviewed. For one, when we asked participants about the approaches they took at solving their situation, their stories suggested that many technical solutions to prevent or remedy privacy incidents might already exist and may be offered by service providers. However, there is no systematic and straight-forward way for lay users to find and appropriately utilize such available solutions in their particular situation.

Second, similar stories also suggested that approaches taken to solve the problem are very dependent on the type of incident, the context in which it occurs and the persons' familiarity with technology. For instance, participant TP008, who was tech-savvy, scored medium-high in privacy concern, and who had experienced the scenario of having his mobile device stolen, took a number of steps to protect his privacy afterwards: "*The first thing I did was to block the phone, disconnect from Whatsapp ... I went into the device manager section in Google and took that device from my list of devices. I assumed that the account would be disconnected [from the phone] and no synching would occur*". Additionally he setup a PIN code remotely using the AndroidLost app, and was even able to fetch pictures of the thief and his location using this same app. He went to the police with this information, and he cancelled his credit cards. On the other hand, a less tech-savvy participant (TP082) who scored low on privacy concern and whose email account had been compromised, recounted how he, while in panic, went on to search on the Internet for the symptoms of his problem, decided to buy Norton antivirus, stopped using his email account and opened a new one, and at the end hired – what he called – a 'PC doctor' who, after charging him tons of money talked him into throwing his computer away and buying a new one.

Third, when participants were asked about the root of their concerns that emerged from the incident ("*Why was this a big concern?*"), their responses indicated that the focus of their worries had to do with financial risks – "*The biggest concern are money and bank account access...*" (TP027), "*A lot of the bank stuff comes through your email, [I'm] afraid that money would go missing*" (TP030) – and possible damages to their reputation – "*[I am afraid that] something embarrassing would go out to my friends or my colleagues*" (TP082). In a minor scale, some participants also mentioned the burden of going through unnecessary or unexpected efforts – "*You don't only realize what [mistake] you have done, but also what you need to do after that*" (TP076) – or the consequences for their future – "*to be honest I'm afraid of what is on the Internet when I look for jobs*" (TP027).

Furthermore, a common reaction to a privacy threat was for participants to change their passwords for one or several of their accounts. This was seen as a solution that was easy to perform, understood by all, and had an immediate effect. Although changing an account password might not be a solution that fits all panic scenarios (i.e., if an account got hacked because hardware was compromised with a keylogger), the act of changing the password was perceived as a security-enhancing behaviour, which although it can make the person calmer and might take her out of panic mode, it can also give a false sense of security in some situations.

3.1.4 Part 2 - Metaphors towards a "panic button" help system

In the second part of the interview, participants were presented with the hypothetical scenario of an online service provider offering a feature analogous to a physical "panic button", but which would tender to privacy or security emergencies online. Specifically, we asked interviewees to tell us 1) what would they expect such a panic button to do in their panic situation and 2) where would they expect it to be located.

Table 3 summarizes the coded responses from these two questions (multiple answers were possible). Table 8 of Appendix C presents sample quotes extracted for the first question. Regarding their expectations of what the panic but-

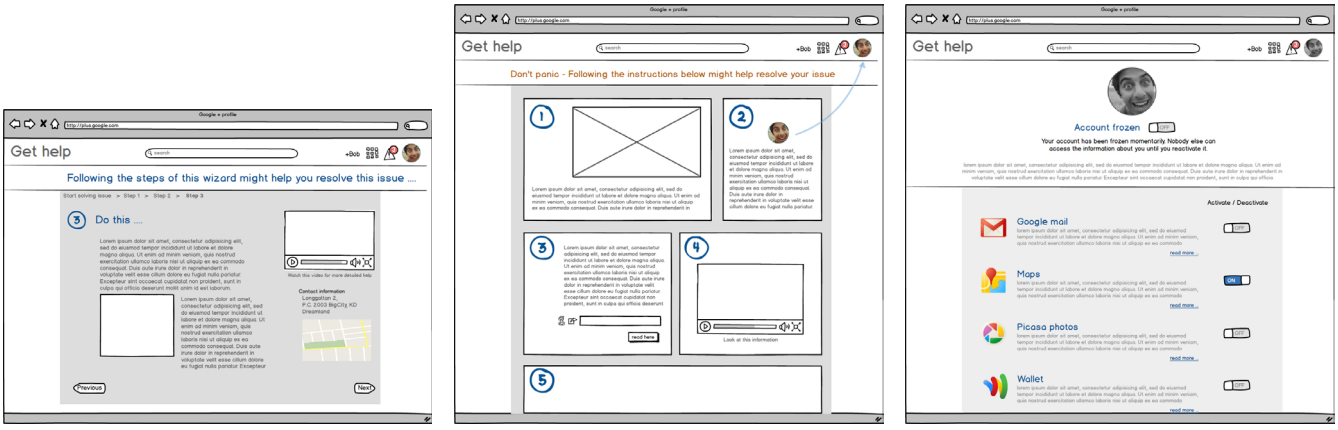
Table 3: Coded results of the expectations of what a panic button should do and how would it be accessed

What would it do?	
Personalized chat / Immediate	6
Give me instructions	3
Freeze or block accounts	3
Lead me through steps	2
Determine my problem	2
Assess the consequences	2
Verify my identity	2
Get me out of panic	1
Educate me (information)	1

(a)

How would you access it?	
Profile	4
Settings	4
Contextual	4
Search	2
Privacy / ToS	1
Mobile device	1

(b)



(a) Wizard (b) Emergency card (c) Account freezing

Figure 1: Three alternative sketches demonstrating possible solutions once the 'panic button' is pressed

ton should do, many participants expressed that, once they have pressed it, they would like to receive some kind of personalized contact with someone, in part because this might provide them an *immediate* response to their problem, but also because it would make them "*feel more safe*" (TP082). Some participants thought of the option of freezing or blocking their accounts, as a *breathing moment* where they could be certain that no more harm can be done to their accounts or their privacy, and others mentioned the possibility of getting instructions or a list of steps that carry them towards a solution.

From their responses to the second question, we learned that many participants expected the button to be located somewhere within their profile pages or under the services' settings. Also, many implied that a help button should be available or connected to the factor that caused the panic in the first place, in other words, it should be contextual. For instance, if the user is notified of an attempt to access her account from another country, then let her launch the help process (i.e., press the panic button) from the notification itself. Although only mentioned by two participants, we believe the possibility to start the help process from the search results as a valuable idea, since many people start looking for help by 'Googling' for their problem (e.g., a search engine could detect that the user might have a privacy issue, and offer actionable help within the search results pages).

Participants were then shown sketched ideas of three metaphors that we had considered during the initial design process. The sketches, shown in Figure 1, were not at all representations of existing or planned designs, but rather just instruments to encourage discussions with the interviewed participants. The three metaphor ideas we used for providing help consisted of 1) a wizard (Figure 1a), showing a series of steps displayed one at the time which leads users towards possible solutions, 2) an emergency card (Figure 1b), similar to the cards found in an airplane's seat, listing the proper measures to take in case of an emergency, and 3) account freezing (Figure 1c), a mechanism to 'freeze' or block an account, so that no further actions are allowed until it becomes unfrozen.

We presented each of these, one at a time but in random order between participants, and asked them whether they thought that the idea was a good approach towards a solution in their case. Their extracted responses from the transcribed scripts are shown in Table 9 of Appendix C. For the wizard approach, participants suggested that it should consist of a series of simple questions and visual elements, it shouldn't contain too many steps and should have a few words at each step, since "*when you are in panic the last thing you want is to read*" (TP030). About the emergency card approach, participants appreciated having a complete overview of the possibles steps they ought to follow to reach a solution, noting also that the instructions given need to be simple, clear and straight forward. Regarding the possibility to freeze the account momentarily, participants recognized that the feature is analogous to the security offered by their banks when, for example, suspicious activity is detected in the account or when a credit card is reported lost. In general, participants found this feature reassuring or comforting, commenting things like "*it would make me feel a little better*" (TP093) and "*it makes me feel safe*" (TP026). Some participants also made observations about the considerations that need to be made before freezing someone's account, such as secure ways to unfreeze it, and the social implications of having their account blocked, "*Imagine that I am waiting for this urgent mail from a client [and I cannot access my email anymore]*" (TP076).

After looking at the three options, participants were asked their opinion on which of the three metaphors would be most suitable for helping people in similar panic situations. Their opinions were not mutually exclusive, and 14 out of the 17 interviewed participants favoured the possibility to freeze their account(s), 5 liked the idea of an emergecy card approach and only 2 said that they would prefer to be led through steps in a wizard-like fashion. Other ideas that came out at this stage of the interview included things like getting help from trustworthy or knowledgeable people, providing chat support, providing information about the scope of the problem, using media (images, videos) to instruct on possible solutions, and letting the user undo certain actions.

After obtaining this feedback from participants and making our own reflections, we concluded that a combination of the different approaches would be suitable for the different stages of the panic help process. For instance, as an

immediate first step, users can be given the choice of momentarily 'freezing' their account, making them feel at ease and experiencing that something has been done to stop further harm. Then, a wizard with few simple multiple choice questions could be used to help determine the problem that the user is experiencing. Lastly, a series of possible tailored solutions or actionable steps could be suggested using an overview layout inspired by in-flight emergency cards.

3.2 Verification survey

The results obtained from the interviews gave us a good initial idea of the reasons and contexts for privacy panic, and the approaches that people take towards trying to solve their problems. In order to confirm and, if necessary, complement those findings we created and launched an electronic survey to collect additional privacy panic experiences from a different cohort of participants. In this section we describe the process of constructing the survey, its distribution and the obtained results.

3.2.1 Survey design and considerations

In the survey we wanted users to provide us with their first memorable experience of privacy panic[1], without us hinting in any of the privacy panic scenarios that we had previously identified, shown in Table 1. Similarly, we didn't want to force all respondents to tell us about a privacy incident if they could not think of any bad experience that had happened to them with regards to their privacy on the Internet. We thus started the survey by asking the same open question as we did at the beginning of the interviews: *Have you ever experienced sudden feelings of concern, anxiety and/or stress about something that happened to you on the Internet, related to your privacy or your personal information?*

If respondents indicated that they had been in such a situation they would proceed to the first section of the survey, where they were first asked to tell their story of the privacy incident and other questions around it (all questions are presented in Appendix B). Then they would continue to the second section of the survey, which asked questions surrounding the different incidents that we identified earlier (Table 1), as well as their concerns to become a victim of each of these incidents and other privacy concerns in general. Respondents who didn't have a privacy panic experience in mind were taken directly to the second section of the survey.

Three of the questions in the first section were open-text questions. In these, participants briefly narrated their story of the privacy incident, the way they found out that something was wrong or out of the ordinary, and the approach they took to try to fix their problem. For these three questions, two independent coders categorized each answer, using the findings from interviews as the bases for the category buckets, but adding additional categories if needed. If there were discrepancies in the category chosen by the two coders, the opinion of a third coder acted as a tie-breaker. The entry was considered a mismatch if there was disagreement between the opinions of all three coders. Cohen's kappa inter-rater reliability for the three questions was calculated, all of them suggested substantial agreement between coders ($kappa = 0.647, \rho < 0.001$, $kappa = 0.782, \rho < 0.001$, $kappa = 0.775, \rho < 0.001$, correspondingly). When categorizing the responses, the coders were instructed to read between the lines to extract the essence of the reason for panic or concern. For instance respondent SP923 narrated the following story: "*I once accidentally clicked on a spam ad that then downloaded spyware on my computer without my knowledge. After running a security sweep a few weeks later the software was detected and deleted however, I am still concerned that my personal information may have been stolen.*" Although the description narrates the infection of the respondent's computer, the underlying concern had to do with the possibility of her data being stolen or leaked.

[1] We avoided using the word *panic* throughout the survey, since the word in itself might sound too alarming. Instead we talked about *concerns* or *incidents*, as can be seen in Appendix B

Table 4: Survey respondents' demographics

		($n = 549$)
Gender	Male	72.1%
	Female	27.0%
	Rather not say	0.9%
Age	18 - 24	38.6%
	25-34	39.0
	35- 45	15.8%
	45-55	1.1%
	55-65	5.1%
	65+	0.4%
Occupation	Employed	41.7%
	Student	26.4%
	Not employed	9.1%
	Self-employed	8.6%
	Retired	0.4%
	Other	13.8%
Industry	Not at all technical	27.0%
	Not too technical	23.0%
	Somewhat technical	13.5%
	Very technical	28.2%
	Missing	8.4%
Crowdsourcing	Microworkers.com	79.8%
	CrowdFlower	15.0%
	ProlificAcademic	5.3%

At the end of the survey we collected some demographics from respondents and information about the crowdsourcing platform that referred them to the survey.

3.2.2 Survey administration and participants

Before launching the survey, two rounds of pilot sessions were carried out where we obtained feedback from a total of 16 participants. The final version of the survey was distributed using three different crowdsourcing platforms: Microworkers.com ($n = 438$), CrowdFlower ($n = 82$) and ProlificAcademic ($n = 29$). We received a total of 830 responses to the survey from these different recruitment platforms, from which 549 of these responses were kept after rigorously disqualifying entries which seemed rushed, incomplete, irrelevant, inappropriate or with very poor language. Responses came from different parts of the world, but the majority of respondents were located in India (31.1%), the United States (11.7%) and the United Kingdom (7.1%). Table 4 shows some additional demographic characteristics of our sample of respondents. For their participation, respondents were paid between $0.50 and $1.90 depending on the crowdsourcing platform they used. The survey took an average of 20 minutes for respondents who narrated a story and 14 for those who didn't.

3.2.3 Privacy panic scenarios

From the 549 valid responses to the survey 313 (57%) indicated that they had experienced sudden feelings of concern, anxiety or stress with regards to their privacy or personal information on the Internet. The responses from 5 partici-

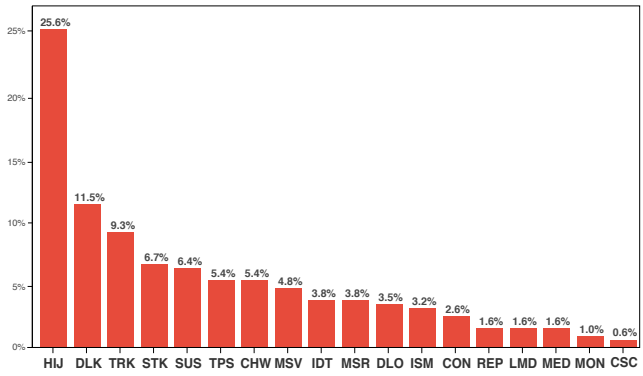


Figure 2: Percentages of self-reported panic stories according to the categorization of survey responses

pants were coded as ambiguous or unclear, and we were left with 308 privacy panic stories. We noted that slightly more than half of the respondents remembered, right on the spot, a personal incident that provoked privacy panic and were willing to tell it. Thus, we considered these as *memorable* cases.

Analysis of the responses from people who indicated to have a privacy incident to tell, yielded for 6 additional scenarios of privacy panic on top of the 12 identified at the beginning. Table 5 shows the newly identified six panic scenarios that resulted from coding the panic stories. These include cases of attempts to be tricked (TRK, e.g., falling for phishing attacks, Nigerian prince emails, buy/sell scams, etc.), realizing that a device has been infected by malware (CHW), realizing that your account is being monitored (MON, e.g., checks on network traffic, someone monitoring the activity in my computer), not having appropriate security measures (ISM, e.g., forgetting to log off from a public computer), getting stressed because of misunderstandings of technology (CON, e.g., confusions with data flows in the cloud and among multiple devices), or becoming aware of suspicious activity in one's account (SUS).

Appendix B.1 lists the characteristics of all 18 identified scenarios. In this list we present the proportion of people who experienced each scenario, their common approaches to solve their issue, their concerns about falling victims for the scenarios, as well as academic literature that has studied related privacy incidents and example quotes extracted from our data.

According to the coding of the self-narrated privacy panic stories, it can be seen that the event of having an account hacked or hijacked was by far one of the most memorable of all cases (HIJ, 25.56%), followed by stories of personal data being leaked (DLK, 11.5%) and attempts to be tricked (TRK, 9.27%). Figure 3.2.3 shows a bar graph of the 18 identified incidents ordered by the frequency of the coded stories of privacy panic. A chi-square analysis comparing stories from Indian and U.S. participants for the three most prominent cases yielded no statistical significant difference between these groups.

Many people who suffered a privacy panic incident indicated that a social network service (48.4%), a payment service (15.8%) and/or a messaging service (15.0%) were involved in the incident. Also, most incidents occurred when using either a desktop (50%), a laptop computer (41.4%)

Table 5: Six added panic scenarios after the classification made from the responses to the survey

Code	Panic scenario	Description
CHW	My device became infected or compromised	My device (mobile, laptop, desktop, web camera, etc.) has been infected with a virus or malware
CON	Managing all my data and connected devices is stressful	Realizing that my identity or private information is at risk because I find it hard to understand and keep track of all the data exchanges between all my connected devices or Internet services
ISM	I didn't take appropriate measures to secure my account	Realizing that I neglected to take appropriate measures to protect my account or my personal data, which resulted in a breach which could have been avoided
MON	Someone else is monitoring my account	Being suspicious or realizing that someone else is monitoring my account or devices, or looking at my Internet activity
SUS	There was some suspicious activity in my account	Being notified that there was an attempt to access my accounts(s) or to obtain my personal information, or that unusual suspicious activity that I do not recognize has been happening in my account(s)
TRK	An attempt to trick me or defraud me was made	Nearly becoming a victim of fraud, someone trying to trick me or making me believe that a service was secure when it really wasn't

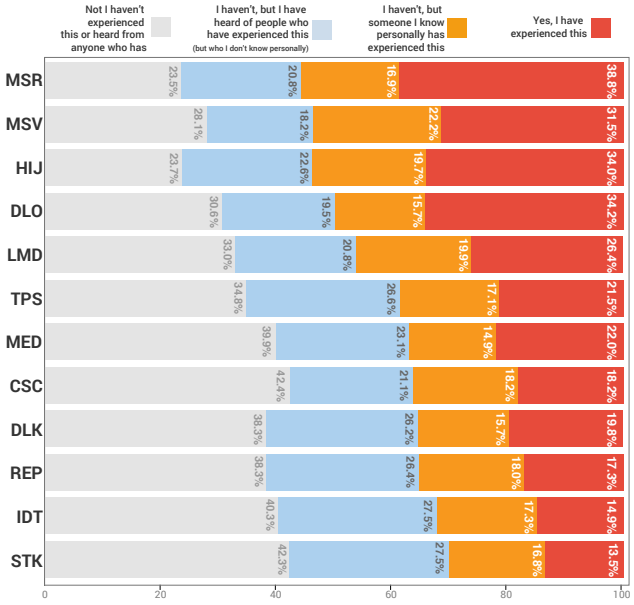
and/or a mobile device (31.2%). Few incidents happened with gaming consoles, wearables or other (5.3%).

Respondents also reflected on how the incident that they experienced might have also indirectly affected their close friends and family. In other words, there might be occasions in which the effects of a privacy incident are not contained within the main victim. One respondent who had his account hacked commented that the event had repercussions on his family, since they couldn't spent time with him due to the extra work hours he had to put to solve the issue.

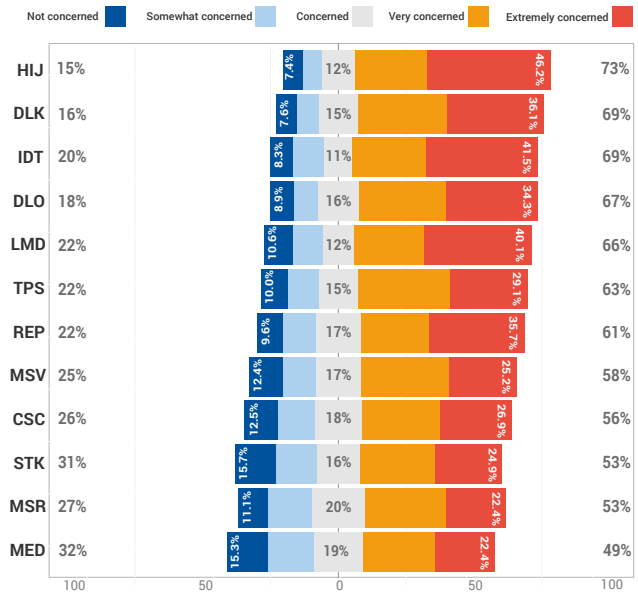
In the next section of the survey all respondents, including those who did not tell their panic stories, got to indicate if they, or someone they know, had experienced one of the twelve panic scenarios identified earlier, described in Table 1. This question was asked to encourage respondents who did not tell a specific story to remember and reflect over possible privacy incidents from the list that they might have experienced. The aim was to get an idea of frequency in which these scenarios are experienced by users. Figure 3a shows that many participants indicated having directly experienced the cases of regretting to share content online (MSR, 38.80%), sharing content by mistake with the wrong person or group of people (MSV, 31.50%) as well as having their accounts hacked or hijacked (HIJ, 34.06%) or losing access to their data (DLO, 34.24%). However, when it comes to *rumors of privacy panic* (i.e., hearing panic stories that happened to others), the cases of stalking or threatening (STK, 27.50%), identity theft (IDT, 27.50%) and third-party sharing (TPS, 26.20%) came at the top.

To test for reliability of our results, we looked back at the answers obtained in the initial screener to the same questions. Except for the case of stalking or threatening, a series of chi-square tests for all the other initially identified panic scenarios revealed no statistically significant differences between the screener and the survey samples with regards to the proportions of respondents who had personally experienced each of the initial privacy panic scenarios ($\rho \geq 0.05, \alpha = 95\%$, for all cases except STK, $\rho = 0.045$). Again, a Mann-Whitney U test between Indian and U.S. revealed no significant differences between the cultures.

3.2.4 Respondents' concerns



(a) Experiences with the identified panic scenarios



(b) Indicated levels of concern about the identified panic scenarios

Figure 3: Results from survey respondents

All respondents in our survey were asked to rate their level of concern about falling victims for each of the identified incidents, as well as their concerns of other privacy statements. We adapted two different instruments to measure privacy concerns as suggested by Anton et al. [4] and Buchanan et al. [7], explained in Section 2.1. From the latter, we took only the top four questions with higher factor loading. Additionally, we included our own set of six questions which we believed to be more relevant for our study and to today's technologies, as seen in Appendix B. Results from a factor analysis revealed that our set of questions fit together with the four selected questions from the scale suggested in [7]. Nine out of ten of these questions correlated at least with a factor of .380, a Kaiser-Meyer-Olkin measure of sampling adequacy was .918, and the Barltlett's test of sphericity was found to be significant ($\chi^2(105) = 2735.117, \rho < 0.001$). Hence an average privacy concern score was calculated from the values of these nine questions ($\mu = 3.26, std = 0.924$). A test of normality of this score revealed that our sample was slightly skewed towards privacy concerned respondents ($Kolmogorov - Smirnov = 0.046, Shapiro - Wilk = 0.978; \rho < 0.001$).

A Mann-Whitney U test of the privacy concerns score between people who told a story of privacy panic and those who stated that they had not experienced any such situation, shows that there was a significant difference in the level of stated privacy concern between these two groups ($U = 28295.0, \rho < 0.001$). One possible reason for this difference is that having been a victim of a privacy incident can have an impact on people's privacy concerns online, possibly modifying their behaviours to become more privacy aware and cautious. This is consistent with the arguments in [14] and also supported by many of the responses from our interview participants, which indicate that they tended to use online services in a different way, stopped using certain services or became more weary about the risks that can be encountered on the Internet. It was also noted from the collected responses that there exists a very small but significantly positive increase in the respondents' privacy concerns depending on the amount of privacy panic scenarios that they had directly experienced ($r = 0.182, \rho < 0.001$). Moreover, a non-parametric Spearman's rank order test revealed that there is a significant positive relationship between the reported level of concerns about the privacy statements and the respondents' concerns of becoming victims of the privacy scenarios presented to them ($\rho_s = 0.681, n = 544, \rho < 0.0001$), meaning that individuals who are more concerned about their privacy in general will tend to be more concerned about experiencing the identified privacy panic scenarios.

From the 12 scenarios presented, respondents in our sample indicated that they were *very* or *extremely concerned* about having their account hacked or hijacked (HIJ, 73%), realizing that their data has been leaked online (DLK, 69%), having their identity stolen (IDT, 69%), or losing their online data (DLO, 67%), while they were least concerned about hearing something from the news or media (MED, 32%), being stalked or threaten (STK, 31%) or regretting sharing something online (MSR, 27%). Curiously, these last case also appeared to be the one that most people mentioned having experienced personally at some point of their lives.

Analyzing the sample from our initial screener ($n = 128$) shows that the cases of MSR and MSV where at the bottom of the participants' concerns, yet they occurred most frequently. One possible reason for this seemingly paradoxical attitude could originate from the individuals' perception on how much control they have to remedy or reverse the situation. In other words, the event of sharing something publicly by mistake or having shared something that they later regret can be something that people perceive as "un-

Table 6: Ultimate concerns or reasons for worrying

Reasons for panic	n	%
People knowing things that are not of their business	81	25.88%
Embarrassment or damage to my reputation	73	23.32%
Money going missing or financial harm	68	21.73%
Emotional harm to me or someone close to me	51	16.29%
Physical harm to me or someone close to me	12	3.83%
Possible loss of physical property or something valuable	11	3.51%
Possible loss of my employment	6	1.92%
Other	11	3.52%

doable" or easily correctable, whereas the misfortune of having their identity stolen, having their information leaked or their account hacked, are cases that are seen outside their reachable control, thus raising their levels of concern about such situations.

Similar to our interviews, we wanted to get an understanding about why people worry when experiencing, or being near experiencing, a breach to their privacy. In other words, what do users see as the consequences of a privacy incident and what is the impact on their lives. To find out, we asked the following question to survey respondents who had a panic story to tell: *In the situation you described, which of the following options best represents your ultimate concern or reason for worrying?* Respondents chose one out of seven options which reflected common concerns identified in the interviews, and the proportions of their responses are presented in Table 6. Consistent with the results from the interviews, financial harm and embarrassment or damage to their reputation were among the top of their worries. Above all, survey respondents' ultimate concern had to do with third parties knowing things about them which are not of these third parties' business.

From the table, it can be noted that around 65.5% of people are concerned by things that are 'softer' types of harm that deal with concepts that are hard to quantify, such as emotional harm, reputation or nosiness of others. On the other hand, 31% expressed concerns related to more concrete and measurable worries, such as losing of money, one's employment or material valuables. This suggests that users in a panic situation could be informed through a user interface about a quantified estimate of the impact of the incident in terms of value, which can motivate them to take steps to resolve the issue and enhance the protection of their privacy.

3.3 Limitations

We are aware that the methods of data collection we employed in our study are only recollections of previous privacy incidents. People might forget other important privacy panic experiences or not recall every instance of what really happened and how they went about solving it. Nevertheless our approach gave us a good starting point for understanding such situations, which can later be studied in-depth with methods that capture users' everyday experiences.

Interview participants were recruited based on a convenience sample of people who voluntarily signed up to participate in user studies. This limitation was one of the reasons that drove us to verify our results with an additional survey. Since due to our location, we were not able to employ the services from Amazon's Mechanical Turk (MTurk), the recruitment of the survey participants was done through three other crowdsourcing platforms: Microworkers, Crowdflower and ProlificAcademic. Although we did not find specific studies about the quality of the workers in the platforms we used, we employed three different ones based on findings from a recent study which indicate that different sample providers might provide differences in their variances with regards to privacy measurements [47]. From our sample Microworkers' participants were slightly older and had higher proportions of Southeast Asians, whereas the proportion of female participants in Crowdflower was slightly higher. However, a Kruskal-Wallis H test showed that there is no statistical significant difference of the levels of privacy concerns among the three platforms $\chi(2) = 2.145, \rho = 0.342$, ($\rho > 0.5$, for all cases).

4. IMPLICATIONS FOR THE DESIGN OF A PRIVACY PANIC HELP SYSTEM

After obtaining a better understanding of possible reasons of privacy panic in users, we can now describe a list of implications for the design of a system of that could try to help users in these situations.

Our findings suggest that some types of panic scenarios that occur most often are not necessarily the same as the ones that concern users the most. However, the case of having one's account hacked or hijacked (HIJ) was one that appeared at the top of users concerns and also was frequently experienced personally, which indicates the need for providing users with more education on how to protect their accounts against this type of attacks, and for prioritizing solutions and remediations for this panic scenario. When presenting users with possible solutions to their privacy panic moment, an intelligent help system could try to detect the type of scenario that the user is experiencing and investigate the users' main concerns. Our investigations showed that many users' concerns have to do with their finances, their reputation or other people knowing things that are not of their business. Thus informing users about the consequences of the incident could help them understand what is at risk, hopefully relieving some of their panic.

From the analysis of the stories told by interview participants, it was observed that people with different levels of familiarity with technology tend to approach a privacy panic problem in different ways. Tech-savvy users are often aware of possible solutions to their particular problem and they just need to have those solutions more accessible, without the need for lengthy instructions or the feeling that they are being patronized. On the other hand, non-tech savvy users could feel lost on where or how to start looking for a solution. An interface for a privacy panic help system should cater for these different users, offering expert users with direct calls for action and convenience on the steps to quickly reach a solution, whereas non-experts could be directed with easy-to-follow steps to solve specific problems, and information about how to protect oneself against similar scenarios in the future. Further studies can help determine the specific needs of different types of users in panic situations.

Regarding the type of help that users expect in a panic situation, users would like to have the possibility to contact someone directly, this is specially the case for non-expert users. Contacting someone could imply that the system facilitates users with communication to their acquaintances, other more expert users, or customer support. Ideas for *crowdsourced* help have been presented in [52]. Many users

also like the idea of freezing their accounts to stop further damage and alleviate the feelings of panic. However, explanations on what does freezing mean and the mechanisms to recover the account have to be explicit and clear. From a technical perspective, a potential feature to 'freeze' or block an account momentarily could be very difficult to achieve with todays technologies, possibly carrying many security implications and potential for abuse. Although technology should try to address these challenges to meet users' expectations, detailed further investigations of such feature are necessary before it should be implemented.

Users expect to find help within the context in which they realized that a problem existed. For instance, changing the visibility properties of a regretted post on a social network should be possible from within the same view that is displaying the post. Nowadays, many users employ search engines as a way to look for their problem, and we value the possibility of displaying help actions directly within the view showing the search results. For instance, Google's Knowledge Graph [53], displays cards on a side panel whenever a concept is identified in the search query, and similar panels could be presented for searches related to privacy panic scenarios. However, further research is required to identify appropriate search keywords. The contributions of Chilana et al. [9], which propose methods for improving the ways users find appropriate help, could also be considered for these type of scenarios.

In general, users experiencing privacy panic expressed their need for a system that provides them with actions, and not complicated instructions that are lengthy and without assurance that a solution will be reached. A help system has to give users the feeling that something is being done to protect their privacy, and that every step has a purpose.

With these considerations in mind, we identify five characteristics of a system that provides help to users in privacy panic situations:

- **Actionable**: Do not redirect users to other pages where they might (or might not) find help. Let them instead perform in-place, situated actions that are perceived as effective steps towards protecting their data and privacy. For instance, if an effective solution for their case is to change their password, the system should allow them to perform that action right where they are, and do not redirect them to another page.

- **Immediate**: Users in panic expect help quickly, not only because the attack or ongoing harm should be stopped as soon as possible, but also because users can perceive that an efficient and trustworthy service provider should be able to provide them with quick and effective help.

- **Adaptive**: A help system should cater to the different type of users (e.g., experts, vs. non-experts), and adapt to the various types of contexts of these users, as well as the different types of panic scenarios that they might be experiencing.

- **Reassuring**: Depending on the situation and the concerns of users, some users might experience more or less panic than the situation calls for. Providing users with possible scope of the consequences to their privacy, as well as with statements of comfort and reassurance might help users understand the problem better and alleviate their panic more effectively.

- **Preventive:** Users that have experienced a privacy incident should understand why it happened and ways to avoid it from happening again in the future. The system should not only try to help users resolve their problem, but also educate them, facilitate steps to secure their account and encourage them to continue adopting secure behaviours.

While more evidence might be needed to determine concrete design suggestions for a possible help system, the results from this study suggest that the help process to aid users experiencing privacy panic should follow the following guidelines: first, let users take as immediate and easily-applicable actions to protect their account(s) as possible, to stop further harm or blocks access to their disclosures; second, try to identify the user's problem or narrow it down by asking a series of straight-forward questions; and third, present users with actionable, in-place solutions that will try to return things to normal, or even improve the protection of the users data and/or privacy, while at the same time educating users on secure behaviours and on ways to prevent similar events in the future.

5. FINAL REMARKS

We presented our exploratory study into moments of online privacy panic. We identified and ranked 18 situations in which users might experience feelings of concern, distress or panic with regards to their privacy or their personal information online. We presented contextual factors around these situations and we also explored, with the use of a panic button metaphor, users' expectations of a possible help system for these kinds of panic situations. At the end, we introduced implications for the design of such a system.

Although our findings unveil 18 panic scenarios that are valid in today's online ecosystem, we see the need to continue investigating and discovering similar situations of privacy panic that may arise with people's evolving privacy attitudes and concerns and with the emergence of newer technologies, such as wearable devices, ubiquitous sensors surrounding the users' environments, intelligent machines, and others.

Acknowledgments

We want to deeply thank Manya Sleeper and Jonathan Aroner for their contributions to ideas and design of the study. Also, Erik Wästlud and Henrik Anderson at Karlstad University for their help with the analysis of the data. Special thanks to the Privacy UX team and other colleagues at Google for their support and feedback.

6. REFERENCES

[1] H. Almuhimedi, A. P. Felt, R. W. Reeder, and S. Consolvo. Your reputation precedes you: History, reputation, and the chrome malware warning. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '14, pages 113–128, Menlo Park, CA, USA,, July 2014. ACM.

[2] K. B. Anderson. Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, 25(2):160–171, 2006.

[3] J. Angulo, S. Fischer-Hübner, J. S. Pettersson, and M. T. Jessica Edbom. D:C-7.3 Report on end-user perceptions of privacy-enhancing transparency and accountability. Project deliverable D:C-7.3, A4Cloud Project, September 2014.

[4] A. I. Antón, J. B. Earp, and J. D. Young. How internet users' privacy concerns have evolved since 2002. *Security & Privacy*, 8(1):21–27, 2010.

[5] H. Berghel. Identity theft, social security numbers, and the web. *Communications of the ACM*, 43(2):17–21, 2000.

[6] A. Besmer and H. Lipford. Tagged photos: Concerns, perceptions, and protections. In *Extended Abstracts on Human Factors in Computing Systems*, CHI '09, pages 4585–4590. ACM, 2009.

[7] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2):157–165, 2007.

[8] P. Buta. *Privacy Panic – How to Avoid Identity Theft, Stop Spam and Take Control of Your Personal Privacy*. Hillcrest Publishing Group, 2009.

[9] P. K. Chilana, A. J. Ko, and J. O. Wobbrock. Lemonaid: Selection-based crowdsourced contextual help for web applicationselection-based crowdsourced contextual help for web applications. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '12, pages 1549–1558. ACM, 2012.

[10] H. Cho, J.-S. Lee, and S. Chung. Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, 26(5):987–995, 2010.

[11] J. W. Clark, P. Snyder, D. McCoy, and C. Kanich. I saw images I didn't even know I had: Understanding user perceptions of cloud storage privacy. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '15, pages 1641–1644. ACM, 2015.

[12] L. F. Cranor, P. Guduru, and M. Arjula. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction*, 13(2):135–178, June 2006.

[13] J. W. DeCew. *In pursuit of privacy: Law, ethics, and the rise of technology*. Cornell University Press, 1997.

[14] T. Donaldson and T. W. Dunfee. Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of management review*, 19(2):252–284, 1994.

[15] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, et al. The matter of heartbleed. In *Proceedings of the Conference on Internet Measurement*, CIM '14, pages 475–488. ACM, 2014.

[16] J. B. Earp, A. I. Antón, L. Aiman-Smith, and W. H. Stufflebeam. Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2):227–237, 2005.

[17] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are you ready to lock? In *Proceedings of the Conference on Computer and Communications Security*, pages 750–761, 2014.

[18] S. Egelman, A. Oates, and S. Krishnamurthi. Oops, I did it again: mitigating repeated access control errors on facebookdid it again: mitigating repeated access control errors on facebook. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '11, pages 2295–2304. ACM, 2011.

[19] T. Fox-Brewster. What is the Shellshock bug? Is it worse than Heartbleed? *The Guardian*, September 25 2014.

[20] T. Halevi, N. Memon, and O. Nov. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Social Science Research Network*, January 2015.

[21] Harris Interactive. First major post-9/11 privacy survey finds consumers demanding companies do more to protect privacy, February 2002.

[22] M. Honan. How Apple and Amazon security flaws led to my epic hacking. *wired.com*, 6, August 2012.

[23] W. Hong and J. Y. Thong. Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly*, 37(1):275–298, 2013.

[24] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun. Home is safer than the cloud! Privacy concerns for consumer cloud storage. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '11, pages 13:1–13:20, Pittsburgh, PA, USA, 2011. ACM.

[25] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall. When I am on wi-fi, I am fearless: Privacy concerns and practices in everyday wi-fi use. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '09, pages 1993–2002. ACM, 2009.

[26] R. M. Kowalski, S. Limber, S. P. Limber, and P. W. Agatston. *Cyberbullying: Bullying in the digital age*. John Wiley & Sons, 2012.

[27] P. Kumaraguru and L. F. Cranor. Privacy indexes: A survey of westin's studies. *Institute for Software Research International*, 2005.

[28] F. Lai, D. Li, and C.-T. Hsieh. Fighting identity theft: The coping perspective. *Decision Support Systems*, 52(2):353–363, 2012.

[29] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen. We're in it together: Interpersonal management of disclosure in social network services. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '11, pages 3217–3226. ACM, 2011.

[30] E. Litt, E. Spottswood, J. Birnholtz, J. T. Hancock, M. E. Smith, and L. Reynolds. Awkward encounters of an "other" kind: Collective self-presentation and face threat on Facebook. In *Proceedings of the Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '14, pages 449–460. ACM, 2014.

[31] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of the Conference on Internet Measurement*, CIM '11, pages 61–70. ACM, 2011.

[32] D. Lyon. Surveillance, Snowden, and big data: capacities, consequences, critique. *Big Data & Society*, 1(2), 2014.

[33] S. Machida, T. Kajiyama, S. Shigeru, and I. Echizen. Analysis of facebook friends using disclosure level. In *Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IIH-MSP '14, pages 471–474. IEEE, 2014.

[34] M. Madden and A. Smith. Reputation management and social media. 2010.

[35] M. Madejski, M. Johnson, and S. M. Bellovin. A study of privacy settings errors in an online social network. In *International Conference on Pervasive Computing and Communications Workshops*, PERCOM '12, pages 340–345. IEEE, 2012.

[36] N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[37] H. Mao, X. Shuai, and A. Kapadia. Loose tweets: an analysis of privacy leaks on twitter. In *Proceedings of the Workshop on Privacy in the Electronic Society*, WPES '11, pages 1–12. ACM, 2011.

[38] L. O'Connor. Celebrity nude photo leak: Just one more reminder that privacy does not exist online and legally, there's not much we can do about it. *Digital Commons: The Legal Scholarship Repository @ Golden Gate University School of Law*, October 2014.

[39] C. Paine, U.-D. Reips, S. Stieger, A. Joinson, and T. Buchanan. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, 65(6):526–536, 2007.

[40] L. Palen and P. Dourish. Unpacking privacy for a networked world. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '03, pages 129–136. ACM, 2003.

[41] F. Parry. True crime online: Shocking stories of scamming, stalking, murder and mayhem. *The Electronic Library*, 32(2):279–280, 2014.

[42] R. M. Peters. So you've been notified, now what? the problem with current data-breach notification laws. *Arizona Law Review*, 56:4, 2014.

[43] E. Rader. Awareness of behavioral tracking and information privacy concern in facebook and google. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '14, Menlo Park, CA, USA, July 2014. ACM.

[44] M. Ryan. Cloud computing privacy concerns on our doorstep. *Communications of the ACM*, 54(1), 2011.

[45] L. Saad. Two in three americans worry about identity theft. *Gallup Poll Briefing*, 1, 2009.

[46] M. B. Schmidt and K. P. Arnett. Spyware: a little knowledge is a wonderful thing. *Communications of the ACM*, 48(8):67–70, 2005.

[47] S. Schnorf, A. Sedley, M. Ortlieb, and A. Woodruff. A comparison of six sample providers regarding online privacy benchmarks. In *Proceedings of the Workshop on Privacy Personas and Segmentation (PPS). Symposium On Usable Privacy and Security*, SOUPS '14, Menlo Park, CA, USA, July 2014. ACM.

[48] U. Shankar and C. Karlof. Doppelganger: Better browser privacy without the bother. In *Proceedings of the Conference on Computer and Communications Security*, CCS '06, pages 154–167. ACM, 2006.

[49] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo. My religious aunt asked why i was trying to sell her viagra: experiences with account hijacking. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '14, pages 2657–2666. ACM, 2014.

[50] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '07, pages 88–99, Pittsburgh, PA, USA, July 2007. ACM.

[51] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '14, pages 2347–2356. ACM, 2014.

[52] V. Singh, M. B. Twidale, and D. Rathi. Open source technical support: A look at peer help-giving. In *Proceedings of the Hawaii International Conference on System Sciences*, volume 6 of *HICSS '06*, pages 118c–118c. IEEE, January 2006.

[53] A. Singhal. Introducing the knowledge graph: things, not strings. *Official Google Blog*, May 2012.

[54] J. C. Sipior, B. T. Ward, and R. A. Mendoza. Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of Internet Commerce*, 10(1):1–16, 2011.

[55] M. Sleeper, J. Cranshaw, P. G. Kelley, B. Ur, A. Acquisti, L. F. Cranor, and N. Sadeh. I read my Twitter the next morning and was astonished: A conversational perspective on twitter regrets. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '13, pages 3277–3286, Paris, France, July 2013. ACM.

[56] D. K. Smetters and N. Good. How users use access control. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '09, pages 1–12, Mountain View, CA, USA, 2009. ACM.

[57] F. Stutzman and J. Kramer-Duffield. Friends only: Examining a privacy-enhancing behavior in Facebook. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '10, pages 1553–1562. ACM, 2010.

[58] Symantec Corporation. Internet security threat report. 19, April 2014.

[59] D. R. Thomas. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2):237–246, 2006.

[60] Z. Tu and Y. Yuan. Understanding user's behaviors in coping with security threat of mobile devices loss and theft. In *Proceedings of the Hawaii International Conference on System Sciences*, HICSS '12, pages 1393–1402. IEEE, 2012.

[61] M. van Der Velden and K. El Emam. "Not all my friends need to know": A qualitative study of teenage patients, privacy, and social media. *Journal of the*

American Medical Informatics Association, 20(1):16–24, 2013.

[62] K. E. Vaniea, E. Rader, and R. Wash. Betrayed by updates: How negative experiences affect future security. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, CHI '14, pages 2671–2674, 2014.

[63] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor. I regretted the minute i pressed share: A qualitative study of regrets on facebook. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '10, Redmon, WA, USA, 2011. ACM.

[64] J. Watson, A. Besmer, and H. R. Lipford. +Your circles: sharing behavior on Google+. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '12, pages 1–9, Washington, DC, USA, July 2012. ACM.

[65] A. Woodruff. Necessary, unpleasant, and disempowering: Reputation management in the internet age. In *Proceedings of the Conference on Human Factors in Computing Systems*, CHI '14, pages 149–158, Toronto, ON, Canada, 2014. ACM.

[66] A. Woodruff, V. Pihur, S. Consolvo, L. Schmidt, L. Brandimarte, and A. Acquisti. Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '14, Menlo Park, CA, USA, July 2014. ACM.

[67] E. Zangerle and G. Specht. Sorry, I was hacked: A classification of compromised twitter accounts. In *Proceedings of the Symposium on Applied Computing*, SAC '14, pages 587–593. ACM, 2014.

APPENDIX

A. INTERVIEWS

A.1 Interview protocol

Introduction to test session

"*Hi, my name is ... The reason we invited you to participate in this study is because users have told us in previous studies that there might be moments in which they find themselves in distressful situations regarding the data about them that is on the Internet. We want to explore the way people react and handle such situations in order to be able to conceive a easy-to-use service that might help them resolve some of those issues. In order to do that in the best way, we would like to hear your stories about previous experiences when you might have felt panic, stress or anxiety about situations involving your personal data.*

When you were invited to participate in this interview, you were asked a series of questions, we might repeat some of those questions now so you can tell us more about those situations.

If it is ok with you we will record this session, mainly to have a record of what is said. There might be other colleagues observing our conversation that will help me take some notes or that are interested on what we have to say. [Start recording at this point].

What will happen is that I will ask you some questions and we will mostly have a conversation revolving those questions. It is important to keep in mind that we are not testing you or your knowledge. There are no right or wrong answers, and we just want you to narrate your stories as accurately and honestly as possible."

A.1.1 Open-ended questions and dialogues

1. **(10 minutes)** Have you ever been in a situation where you have felt a sudden feeling of panic, anxiety or distress for something related to your personal information or data on the Internet?
   (a) How long ago did this happen?
   (b) How did you find out that the issue was going on?
   (c) Do you remember how did you feel at that moment?
   (d) Why was this a big concern?
   (e) What do you think led to the situation in the first place?
   (f) Did you resolve the issue? How?
   (g) Did you try to seek help some how?
2. **(10 minutes)** From your responses to the screener and pre-questionnaire, you mentioned that [AN INCIDENT] happened to you or to someone you know. Can you tell me more about [AN INCIDENT]?
3. **(10–15 minutes)** We are investigating ways to design functionality similar to a so-called "*panic button*", which can help users solve issues similar to the ones you just described.
   □ Imagine that it is you who discover that there's something not normal, where would you click on a service to access such button?
   □ Imagine that a service provider detects that there is something not normal with your account. For instance it can recognize that your account is being access from another part of the world. What would be the best way to notify you?
4. **(5 - 10 minutes)** Imagine that a service provider is offering a panic button and that you are in a situation similar to the one you described earlier. In your opinion, what should happen when you press such a panic button?
5. **(10 - 15 minutes)** We have been thinking of some possible solutions to offer help once you have clicked on the panic button, which of these different options (Figure 1) do you think would be more helpful for you at solving your problem during a panic situation?
6. **(5 min)** Do you think that you would have used it [panic button] in the situation when the incident you described happened?

B. VERIFICATION SURVEY QUESTIONS

(Page 1) Introduction and consent

"*Thank you for your interest in completing this survey.*

The results of this survey will be used for a project at Karlstad University in Sweden. At no time your name or any other information that directly identifies you will be shared with anyone outside the University. Your answers, along with the answers of many other people, will be analysed and might be reported in academic conferences and scientific venues. The results of our research might be used by our research partner to improve their products and provide their users with a better experience. You have the right to contact us and request that your responses will not be considered in scientific publications as long as your request is received before the results are made public.

Please remember that there are no wrong or right answers to the questions in this survey, we just want your honest opinions and answers to the questions asked. We will not collect your name, email address or other specific information that identifies you directly, so that you feel comfortable answering the questions honestly.

In order to start the survey you need to agree to the terms listed here. This survey consists of around 25 - 30 questions and will take approximately 10 - 20 minutes. You can use a computer or a mobile device to complete the survey. At the end of the survey you can give your opinion on things that were not clear or hard to understand."

(Page 2) Your story about a privacy incidents

There are moments when you might have become concerned that your online privacy might be at risk or when you realised that something was not quite right with your online personal information.
We want to know your story about one of those moments!
Please try to remember such a situation as well as you can and answer the following questions in as much detail as possible.

1. **Have you ever experienced sudden feelings of concern, anxiety and/or stress about something that happened to you on the Internet, related to your privacy or your personal information?**
   ○ Yes, I have been in a situation where I experienced such feelings about my privacy or personal information on the Internet
   ○ Probably, but I do not remember any such situation right now
   ○ No, I haven't experienced any such situation

(Page 3) Your story about a privacy incident

2. **Please briefly describe the incident that made you experience feelings of concern, anxiety and/or stress about your privacy or your personal information on the Internet**

   _____

3. **Approximately how long ago did this happen?**
   - ○ Less than a week ago
   - ○ More than a week ago but less than a month ago
   - ○ More than a month ago but less than six month ago
   - ○ More than six months ago but less than a year ago
   - ○ More than a year ago
   - ○ I don't remember

4. **How did you realize that something was wrong or out of the ordinary?**

   _____

5. **Which type of technology device(s) were involved in the incident that you described?**
   □ Laptop computer □ Tablet □ Wearable technology □ Smartphone □ Desktop computer □ Mobile phone (non-smartphone) □ TV or gaming console □ Other

6. **What did you do to try to repair the problem(s) caused by the incident that you described?**

   _____

7. **Were there any Internet services, mobile apps or companies that were involved in the incident?**
   □ Transport □ Messaging □ Photo □ Entertainment □ Dating □ Media streaming □ Government □ Location □ Payment □ Cloud storage □ Social networks □ Online bank □ Travel □ Other

8. **As far as you are aware, was someone else also affected by the incident that you described?**

   _____

9. **In the incident that you described, which of the following best represents your ultimate concern or reason for worrying?**
   - ○ Possible loss of physical property or something valuable
   - ○ Embarrassment
   - ○ Damage of reputation
   - ○ Possible loss of my employment
   - ○ Physical harm to me or someone close to me
   - ○ Emotional harm to me or someone close to me
   - ○ People knowing things about me that are not of their business
   - ○ Money going missing
   - ○ Other

(Page 4) About your story

10. **Does the incident you described in the previous page relate to any of the situations listed below?**
    - ○ Finding out that another person or a company has shared my personal information or posted information about me on the Internet
    - ○ Feeling uncomfortable because someone seems to be stalking me, threatening or bothering me onthe Internet
    - ○ Finding out that someone has hacked my account(s) or accessed it without my permission or knowledge
    - ○ Finding out that my personal data has being leaked or obtained by someone who I do not approve of
    - ○ Finding out that someone else is using my personal information to pretend to be me
    - ○ Finding out through the news and media that my privacy or personal data can be at risk
    - ○ Deleting or not being able to access my online data that is valuable to me, such as documents, pictures, or other files
    - ○ Losing a mobile device or getting it stolen (such as a smartphone or tablet)
    - ○ Someone who I no longer trust (e.g., ex-partner, previous employer, old friend) still has access to my accounts or my personal information
    - ○ Someone posting things about me online which damage my reputation
    - ○ Sharing something in a Social Network by mistake or regret sharing it
    - ○ Sharing something in a Social Network and realizing that it can be seen by the wrong person or group of people
    - ○ Other

11. **If you chose 'Other', how would you describe in ONE sentence the reason for which you experienced feelings of concern, anxiety or stress**

    _____

(Page 5) About your story

12. **Have you ever experienced any of the following situations?**
    Same list of options as previous question presented in randomized order, with the following options for each case:
    - ○ Yes, I have experienced this
    - ○ I haven't, but someone I know personally has experienced this
    - ○ I haven't, but I have heard of people who have experienced this (but who I don't know personally)
    - ○ No, I haven't experienced this or heard from anyone who has

(Page 6) About your concerns

13. **How concerned are you about the following situations happening to you?**
    Same list of options as previous question presented in randomized order, with the following options for each case:
    Not concerned ○—○—○—○—○ Extremely concerned

14. **Rate how much do you agree or disagree with the following statements**
    Based on the instrument on privacy concerns suggested in [4]. Order was randomized.
    Strongly disagree ○—○—○—○—○ Strongly agree
    - ○ I want a web site to tell me how my personal information will be used
    - ○ I am concerned about unauthorized employees getting access to my personal information
    - ○ I mind when a web site monitors my purchasing patters
    - ○ I mind when a website I visit collects information about my browsing patterns
    - ○ I mind when my personal information is shared or sold to third parties

15. **Rate how concerned you are about the following statements**
    Based on the instrument on privacy concerns suggested in [7] plus questions specific to this survey. Order was randomized.
    Not concerned ○—○—○—○—○ Extremely concerned
    - ○ Someone looking at the contents of my mobile device
    - ○ Strangers looking at the things I post on the Internet
    - ○ If you use your credit card to buy something on the internet your credit card number will obtained or intercepted by someone else
    - ○ In general, how concerned are you about your privacy while you are using the Internet?
    - ○ Online services not being who they claim they are
    - ○ People online not being who they say they are
    - ○ Advertisers using information about me to advertise to me
    - ○ Companies sharing my personal information without my permission
    - ○ The level of encryption of my data when I submit it to an Internet service
    - ○ The amount of information on the Internet available about me

(Page 7) About you

16. **Gender**
17. **Age range**
18. **Nationality**
19. **Occupation**
20. **Industry**
21. **How would you rate yourself in this scale**
    I often ask others for help with technology (computer, phones, etc.)
    ○—○—○—○—○—○
    Others often ask me for help with technology (computer, phones, etc.)
22. **From which of the following services did you hear about this survey?**
    ○ Microworkers ○ Crowdflower ○ ProlificAcademic

B.1 Final identified categories of panic

My account was hijacked or hacked — HIJ

Occurrences:	interviews	survey
	3	80
Description:	Finding out that someone has hacked my account(s) or accessed it without my permission or knowledge	
Literature:	[49] [22]	
Sample cases:	SP229	"My e-mail account was hacked and embarrassing e-mails were sent to various people close to me including my employer"
	SP324	"My email account was hacked and I have lost it because the hacker change all measure to change the account password"
	SP508	"When I wasn't able to log into my Facebook account with an error message saying your account was logged in Burkina Faso a West African country"

Account hijacking (HIJ) happened to be the most prevalent reason for panic among survey respondents. From all the coded incidents submitted by survey participants ($n = 313$), 80 of them (25.60%) narrated a scenario related to the hacking or hijacking of one of their accounts. The victims of this incident found out that their accounts had been accessed by someone else mainly because of a warning given by the service provider (22%) or because they were suddenly unable to access their account (26%). For 20% of them it was their own realization or suspicious that led them to discover that their account had been hacked, for instance cases similar to "*I found out that someone accessed my email account outside of my country where I belong to*" (SP337) were often reported. To resolve this issue (50.2%) of the victims changed their password, (24.1%) contacted the corresponding service provider, and other few tried to update their security or privacy settings in some way (6.3%) or took the steps to recover their account (6.3%). The proportion of all respondents from our survey who stated having personally experienced a case of account hijacking ($33.8\%, n = 549$) significantly agrees with the proportion reported in the study of Shay et al. [49] ($30\%, n = 294$) ($z = 2.51, \rho < 0.01$).

My data was leaked online — DLK

Occurrences:	interviews	survey
	2	36
Description:	Finding out that my personal data has being leaked or obtained by someone who I do not approve of	
Literature:	[24] [38] [51]	
Sample cases:	SP717	"Few years ago I joined Internet casino because of the some bonus program. After that my e-mail is on spam attack almost every day"
	SP425	"When Target had a breach of security, credit card numbers were stolen. Mine was among them"

Answers related to the scenario of **data leaked (DLK)** included the user realizing that her personal information has being stolen, finding out that someone else got a hold of the user's personal information by suspicious means, the user finding her personal information on the Internet when using a search engine, and other similar situations. In our sample, 36 (11.5%) out of 313 respondents declared having found out that their data had been leaked on the Internet. Most of them stated that they found out because they noted something on a website or service that awaken their suspicion. For instance, SP861 wrote that he noticed that his phone number had been leaked when he started receiving unsolicited calls. The majority of the victims of this case (12) mentioned that their reason for worrying was the possibility that someone would steal their money. As attempts to resolve their issue, these victims tended to contact the service provider directly or to change their password.

An attempt to trick me or defraud me was made — TRK

Occurrences:	interviews	survey
	n/a	29
Description:	Nearly becoming a victim of fraud, someone trying to trick me or making me believe that a service was secure when it really wasn't	
Literature:	[50] [41] [20]	
Sample cases:	SP246	"I was paying for something from a site. I already put in my credit card details and push submit when I realised that it was a fake site"
	SP79	"I was navigating a website, can't remember what website, when my firewall flashed that someone was trying to gain access to my computer"

Many respondents to our survey reported becoming afraid, stressed and concerned when experiencing an **attempt to be tricked, defrauded or scammed (TRK)**. Even though the attacker or fraudster might not succeed in his attempt, such cases have the power to encourage victims to take action with regards to securing their data and possibly promoting behavioural change. Many of the stories in this category had to do with phishing attempts, specially targeted to financial online services or social networks. The majority of participants in this case stated that they tried to mitigate such attempt by closing abruptly their browser (SP093), turning off their computer at once, not using a particular service, or blocking the website that originated the attempt. For instance, SP697 mentioned that he hastily "*deleted that account*" when he was requested to enter his PayPal details in an unknown service. Most victims of this case (57.1%) mentioned that their biggest worry had to do with money going missing. Attempts to be tricked is the one of the incidents that the participants in our sample experienced most recently, since 17 out of the 29 respondents indicated that it occurred to them in the last 6 months.

I was being stalked, threatened or bullied — STK

Occurrences:	interviews	survey
	1	21
Description:	Feeling uncomfortable because someone seems to be stalking me, threatening, bullying or bothering me on the Internet	
Literature:	[26] [41]	
Sample cases:	SP554	"Few months ago I made a friend from South Africa on Facebook... One day she told me to send her my nude pics and I did it. After that she started blackmailing and demanding money and [threatening] me to post them on Facebook ... I unfriended her and decided to not make any close friend online"
	SP380	"Someone got my info online and was telling me they will find me"
	SP69	"Once I posted an article in the main daily papers and my e-mail address was also posted. After that, I started receiving threats into my inbox and was feeling bad and completely concerned about it"

This category comprises serious cases of **stalking or threatening (STK)** or recurring offenses of cyber-bullying that made users feel very uncomfortable or fearful that some greater, more tangible, harm could be done to them. These are often cases which may trigger many emotional reactions on their victims. One of our interview participants (TP053) who had been stalked by her ex-husband not long ago before the interview, and felt severely emotionally paranoid, was of the opinion that some of the security approaches adopted by many online services were an enabler for her bad experience. In our survey sample there were 21 of these cases of stalking, threatening or bullying online. Most of them tried to resolve the situation by either blocking a contact on their email or a social network or contacting a service provider for help. For instance, SP124 mention how she "*didn't respond to the man who threatened me... I deleted him from my Facebook and blocked his account.*" The majority of these victims indicated that their biggest concerned was that their reputation might be ruined due to blackmailing, or that some sort of emotional harm will be done to them or someone close to them.

There was some suspicious activity in my account — SUS

Occurrences:

interviews	survey
n/a	20

Description: Being notified that there was an attempt to access my accounts(s) or to obtain my personal information, or that unusual suspicious activity that I do not recognize has been happening in my account(s)

Literature: [42]

Sample cases:
- SP539 "I logged in to my Gmail account and there was a message written in red that my account had been accessed from an IP-address most likely located in China"
- SP691 "My email provider informed me of 179 failed login attempts at an email address I had not logged into in over a month"

Suspicious activities (SUS) include, among others, attempts to be hacked which were actually stopped by the service provider. However, the sole fact that a notification was send to the user about an attempt to infiltrate her account can be a trigger of panic and a call for action about improving secure behaviours. Many of the respondents who reported having received a notification did actually changed their passwords or looked at their account history for signs of recurring suspicious activity. At the same time, a recent legal investigation into privacy breaches presented in [42] argues that a more actionable notification scheme should be considered for data breaching events. The responses of 20 people in our survey sample were categorized under this panic scenario, most of them fearing that a stranger would know things about them that were not of their business. Half of them were warned by the service provider or found out by the tools the service offers (e.g., account login history) about suspicious activity in their account.

My device became infected or compromised — CHW

Occurrences:

interviews	survey
n/a	17

Description: My device (mobile, laptop, desktop, web camera, etc.) has been infected with a virus or malware

Literature: [46] [62]

Sample cases:
- SP977 "I browsed some sites for adults and downloaded something - I don't know what. Unexpectedly, my tablet turned off, and I couldn't turn on them again"
- SP164 "Downloaded a file which turned out to be a virus and my information was compromised"
- SP493 "I was watching a video and my webcam took a picture of me and then put up a full page warning that unless I pay an amount of money out before the timer runs out the Police will be called"

Cases of **compromised hardware (CHW)** are an old common reason for panic in desktop computers, although recently other hardware devices are being infected, such as mobile phones. 17 people in our sample reported cases in which their devices got infected usually due to visiting a malicious website or downloading a suspicious file. At least 2 people reported having their mobile device infected, and 2 other people mentioned attacks via their compromised web cameras. Their biggest ultimate concern was that information or pictures about them were going to be used to embarrass them, but also matters related to money or strangers knowing things that are not of their business was a big concern. The majority of victims, tried to resolve their issue by restarting, formatting or scanning their device.

Third-parties shared data about me — TPS

Occurrences:

interviews	survey
3	17

Description: Finding out that another person or a company has shared my personal information with others or posted information about me on the Internet without consulting me first

Literature: [29] [43] [54]

Sample cases:
- SP60 "When people's morphed photos were uploaded in social networking sites ... including mine"

Cases of **third-party sharing (TPS)** are usually predecessors of reputation damage (REP), since people that panic because of someone else sharing data about them online is usually because the things being shared are embarrassing, untruthful or make the first party uncomfortable. In our sample 16 respondents told stories about other people or companies shared their data on their behalf. Six of them said that they tried to contact the third party to get the content taken down. Their concern had to do with they, or someone close to them, being harmed emotionally. One third of respondents for this scenario tried to either contact the third-party to try to resolve the issue directly or contact the service provider where the data was found. Others indicated a change on their behaviour, for instance, one participant explained how he found morphed photos of himself being uploaded to a social network site, and as a consequence he has never uploaded one more photo to a social network again.

I shared content with the wrong people — MSV

Occurrences:

interviews	survey
1	15

Description: Sharing something on the Internet and realizing that it can be seen by the wrong person or group of people

Literature: [11] [18] [33] [35] [56] [64]

Sample cases:
- SP202 "I once saved a sex story in Facebook under notes. Unfortunately, I posted it public instead of selecting the privacy option 'Only me'. I deleted it soon after but few of my friends asked me about that. I said my account got hacked."
- SP450 "I had accidentally posted a personal status update on facebook without realising that the default audience was set to public instead of my usual strict filtering"

Sharing something with the wrong person or group of people (MSV) is one of the panic scenarios that many of our respondents reported having experienced (see Figure 3a), but only 15 of the respondents told the story of such a case. Eight of them claimed that they found out on their own about posting something with the wrong audience, for instance by receiving strange comments from other people. The big majority resolve their issue by changing their privacy settings on the service where they uploaded the content or by taking the content down. One participant reported that he stopped using Facebook groups in order to stop personal information from being revealed to those groups.

My identity was stolen or misused — IDT

Occurrences:

interviews	survey
1	12

Description: Finding out that someone else is using my identity and personal information to pretend to be me on the Internet

Literature: [5] [45] [2] [28]

Sample cases:
- SP313 "Someone copied my details from my social media account, along with some pictures, and posing as me."
- SP59 "I found out that there existed a Facebook profile using my name and my profile picture"
- SP704 "Sometime last year, a few people have told me that they've already accepted my invite through email to a private site, and they asked what it was all about, because there were only a few words in it and it seemed half finished. I've never made such a website and I panicked about someone accessing my account to send the invites to those people I knew."

There were 12 reported stories of **identity theft (IDT)** in our sample, which included attackers creating email accounts under the victims name, filling credit card applications with the use of the victim's information, and finding out that accounts have been created using the victim's pictures and other information. Five of them indicated that they found out that their identity had been stolen or misused because someone else told them about it, and six realized on their own due to weird activity in their accounts on online services or banks. Half of the victims of this case, contacted the service provider to report the abuse of their data or the observed strange activity, and three of them took steps to have fake accounts blocked. Their biggest concern had to do with emotional harm, money going missing or being embarrassed.

I regret having shared something online — MSR

Occurrences: interviews: 3, survey: 12

Description: Sharing something on the Internet and regret sharing it once it's too late

Literature: [55] [63]

Sample cases:
- SP809 "When I was younger I took silly pictures of myself. I had a hard time purging them all from the internet"
- SP1019 "I posted a picture of my cat on my Facebook page. It was only afterwards when I realized that I had left a marijuana pipe on the desk AND my eBay password was visible on a piece of paper in the picture"
- SP1032 "I submitted a photo that had geotagging data on it to an anonymous website"

Out of all panic scenarios, **regretting sharing something online (MSR)** was the scenario that most respondents of our exploratory questionnaire and our survey admitted to had personally experienced (as seen in Figure 3a). However, it is also the case which people were concerned the least about being victims of. Logically, most people who regretted sharing something try to fix their problem by removing the content that was shared. From the 12 reported cases of regret, 7 stated that embarrassment was their biggest worry. One mentioned that he was worried about the lost of physical property, since he posted an item for sale online and was worried that others would get to know his phone, name, address and the valuable item that was at his home. Other cases included people uploading pictures of themselves that they later regretted, making public comments about the government, or people being teased due to the content of their public posts. One participant described the consequences of his regret when, after having uploaded a photo containing embedded location metadata to an anonymous website, other people started ordering pizza to his home address.

I deleted my data or I am not able to access it — DLO

Occurrences: interviews: 2, survey: 11

Description: Deleting or not being able to access my online data or data in an account that is valuable to me, such as documents, pictures, or other online files

Literature: [24]

Sample cases:
- SP435 "My Gmail account was lost and that day I cried... Many personal information was included in that mail"
- SP76 "Sometimes I feel stress when can't find an important information"

Cases of **losing access to data or an account (DLO)** included stories related to accounts being blocked, forgetting PIN codes or passwords, and not being able to find data that they presumably deleted by mistake. Many people with this problem tried to contact the service provider for help, or try to update their settings once they recover access to their account.

I didn't take appropriate measures to secure my account — ISM

Occurrences: interviews: n/a, survey: 10

Description: Realizing that I neglected to take appropriate measures to protect my account or my personal data, which resulted in a breach which could have been avoided

Literature: [62]

Sample cases:
- SP868 "I have logged in a recharging website from another person's computer. After that two days I did not get time to work in computer. I felt afraid that person may hack my password and take my money"
- SP478 "I forgot to log out my Facebook account in a computer laboratory, then someone used my Facebook status to inform me that I forgot to log out"
- SP39 "I made Paypal account and share my paypal address on the Internet and my password was too short and simple"

Failing to take **appropriate security measures (ISM)** can also result in panic. Examples of stories in this category include users forgetting to log off from an account and others taking the opportunity to post things in the users' behalf (i.e., faceraping), or realizing that their password is too weak or that the security in their account too is vulnerable. This category was made different from identity theft (IDT) or stalking, threatening or bullying (STK) in that the stories describe much lesser offenses, often inducted by friends or family who try to tease the victim but don't mean any great harm. Six out of the ten people who experienced this case stated that they changed their password after the incident. The majority mentioned that they worry about money going missing or public embarrassment.

Managing all my data and connected devices is stressful — CON

Occurrences: interviews: n/a, survey: 8

Description: Realizing that my identity or private information is at risk because I find it hard to understand and keep track of all the data exchanges between all my connected devices or Internet services

Literature: [11] [24] [25] [31] [37] [44] [51]

Sample cases:
- SP730 "[I panicked] when I added my personal number on the Internet such as Facebook because they need it to verify your account"
- SP611 "I realized that Google for instance has everything about me connected... Having all of this out there in the hands of databases of companies created some sort of anxiety. I'm more careful being anonymous on the internet nowadays than I was a few years ago."
- SP828 "In Facebook, I've been watching some publicity about my sexual preferences that I'd prefer to keep private. So I don't know how they get that information"

We refer to difficulties of **managing connected devices and services (CON)** to situations when users find themselves doing something to breach their own privacy or experiencing feelings of stress simply because their lack of understanding on how technology works. For instance, respondents in this category reported being scared at the presence of tailored ads or the realization that service providers can infer information about them through big data analysis. When asked how did they find out that something was wrong or out of the ordinary, one respondent wrote that he "*created an account on Google plus using fake info for anonymity purposes, but then received friend requests from people I know from Facebook*" (SP611). He went on to mention that this unclear coupling of personal information across services keeps him concerned about using social network services. The victims of this use case didn't have any consistent approach to calm their panic. Six of them stated that their main concern lied in others knowing things about them that were not of their business and the remaining two were afraid of some physical harm happening to them.

My reputation was damaged — REP

Occurrences: interviews: 2, survey: 5

Description: Someone else posting things or spreading rumours about me on the Internet which may damage my reputation privately or professionally

Literature: [1] [6] [29] [30] [33] [34] [57] [61] [65]

Sample cases:
- SP105 "Inappropriate photos were posted on some my accounts and fake links too"
- SP631 "One of my friends had posted an embarrassing picture that featured me drinking. My family being extremely conservative objected to this vehemently as they did not like the party I was at"

Contrary to the case of third-party sharing, this category represents events where the victims' main concern is not on the fact that data about them has been shared online, but rather that their reputation can be severely damaged. In her study Woodruff [65] recounts the story of a manager who discovered that bad reviews about her were written by her colleague in an online service. Similarly, a participant of our interviews, told us how she panicked when a bad review was made in a popular travel website about an aspect of her business (TP085). Some of the respondents who experienced this panic scenario, try to solve it by contacting the person who uploaded content or trying to take it down themselves. One participant tried to solve his problem by restarting or scanning his computer for malware, since he explained how he was looking for adult content online, when "*in one second some window showed up, and started popping up again and again, saying that I'm sharing my searches with*

people on my Google+ and my Facebook account, where I was logged in... that window was asking for my personal information in order to stop sharing that stuff. I was very wared, and concerned, scared about idea that someone else or specially my friends and relatives, will see stuff that I was looking on the Internet" (SP927).

I saw an alert on the news or media — **MED**

Occurrences:

interviews	survey
3	5

Description: Finding out through the news and media that my privacy or personal data can be at risk

Literature: [15] [32]

Sample cases:
- SP214 "With all these companies being hacked I fear about my information being stolen"
- SP680 "There was a thing going around on the Internet ... It was called the heart bleed virus or something, but I was terrified that all of my personal information was going to be hacked or spread. It was horrible. I stayed off the internet for like a week"

Every now and then **media scandals (MED)** can create a state of panic in their followers. Popular examples include Snowden's revelations about the goverments' surveillance, news about serious bugs, such as Heartbeat and Shellshock, or major data leaks, like the leakage of celebrity pictures through Snapchat or the hacked suffered by Sony in 2014. In our sample only 5 people reported a story dealing with such scandals. Besides finding out through the news, three of these cases indicated that they were warned about the incident by the service provider.

My mobile device was lost or stolen — **LMD**

Occurrences:

interviews	survey
2	5

Description: Losing a mobile device (like a smartphone or tablet) or getting it stolen

Literature: [17] [60]

Sample cases:
- SP42 "I was casual and I never knew that I had lost my phone, later when I found out I was stunned, speechless. I realized that I lost one of my priced possession which I brought out of my pocket money"
- SP860 "I lost my phone which contained personal information like passwords to email accounts, bank details and contacts. Plus, my browsers had saved passwords to various password protected sites"

The **lost of a mobile device (LMD**) has also become a big concern, given that plenty of personal information and data is stored in these devices and that they become a portal to our private information and many of our online accounts, in which we are perpetually logged in. Only very few respondents submitted stories related to the loss of their mobile device. However, this case was one of the cases at the top of the users' concerns. Recent approaches to secure mobile devices offered by the manufacturers and other apps, also have lower the frequency of this type of incident. For instance, Android offers the 'Android Device Manager' service and Apple has the 'Find my phone' feature, which makes it much harder for thieves to target these devices, and easier for the owners to reclaim them.

Someone else is monitoring my account — **MON**

Occurrences:

interviews	survey
n/a	3

Description: Being suspicious or realizing that someone else is monitoring my account or devices, or looking at my Internet activity

Literature: [48]

Sample cases:
- SP22 "Got a feeling that someone is checking my browsing history and all"
- SP342 "I am using my Facebook account for past 5 years .. when I came to know that my father is secretly monitoring my account I was very angry and I thought that I don't have online privacy"

Scenarios of **account monitoring (MON)** refer to cases in which the respondents might feel that the activity in their accounts or their online communications might be monitored by a third party. The four people in our sample who fell into this category told stories about finding out that family members are monitoring their activity, or simply getting the feeling that someone else is intercepting their online actions. Three out of the four people who experienced this case stated that mere suspicion made them find out that something might be going wrong.

Changes in my social context — **CSC**

Occurrences:

interviews	survey
1	2

Description: Realizing that someone who I used to be closed with, but whom I no longer trust (e.g., ex-partner, previous employer, old friend) still has access to my accounts or my personal information

Literature: [67]

Sample cases:
- SP59 "my ex boyfriend published on Facebook some photos of us together while I was in another relationship"
- SP609 "I used to date a girl, she was into games, like I am and she knew about all my usernames/passwords. When we decided to break up, it took a good time to make them all safe and I even got as far as losing some of them to her"

We refer to **changes in social contexts (CSC)** to the cases in which a person's social circumstances have changed and when the person realizes that some personal data or sensitive information was shared with other people who are no longer trustworthy, reliable or close. This can commonly occur when a romantic relation ends, when changing employers, or moving to different cities. In our survey there were only two such stories put under this category, and one interviewee (TP065) also recounted an episode of panic when she realized that her Google calendar was been shared with a person who was no longer her friend.

C. RESULTS FROM INTERVIEWS

Table 7: Identified reasons of privacy panic supported by quotes from interview participants

Code		Sample quotes
CSC	TP065	"Someone else [an exfriend] having access to my calendar that I shared with him. I was a bit shocked that I forgot to remove him... It would be perfect for a stalker"
DLK	TP027	"Even though they assure me it is secure, there could be a little bug, that will leak out my data, and they can get my card number, address, phone and everything..."
	TP105	"I had my data on the Internet. All the details, they got all details, links to bank accounts..."
DLO	TP076	"I deleted my bookmarks on my old computer long. When I changed computers I exported bookmarks, but then I threw them away [deleted them]. I am concerned about deleting something unintentionally. So I safe my stuff in the Cloud. I trust more storing in the cloud"
	TP097	"Once my computer broke and I lost all my data... I was on the verge of freaking out"
HIJ	TP069	"When login from another country you are asked for the recovery of your email... The first time I got this notification, I thought 'eh?, what is happening'... when you are not familiar with something you will get panic. I thought my account is blocked or hijacked. After that I got a notification that we are trying to prevent an unauthorised login to your account...."
	TP082	"Someone sending emails on my behalf [from my email account]... I was really afraid and I didn't know what to do, so I called one of these PC doctors, really expensive. And at the end nobody could really help me."
IDT	TP093	"I was working as a journalist. Someone contacted me asking me if I wanted to be a member of this thing... I got suspicious... later I found out that someone used my information to get a journalist pass... I'm not sure how he found my information, but I think he found what I was writing"
LMD	TP008	"I got my phone stolen in the train ... I fell asleep and in a lapse of 10 minutes someone snatch my phone from my hand..."
	TP105	"I was vacationing in Gand Canaria and I lost my phone... It is a lot of work when something like that happens"
MED	TP093	"When heart bleed came out I changed all my passwords. I was worried mostly about my credit card.... I was very very worried about my amazon account leaked my bank account data.."
	TP065	"[Facebook] makes studies about people without telling them... I don't want them to do anything with my data without me knowing.... it was in the media some time ago"

(Table 7 continued...)

Code	Sample quotes	
MSR	TP027	"Once I posted a picture of a 5 star hotel were I was staying for a business trip and my colleagues got jealous... Rumours spread some weeks later, which affected me"
	TP069	"First day that Google plus is introduced suddenly my photos got uploaded"
MSV	TP085	"There was something that my daughter put on social media, I think she didn't do well on an exam ... I came across the post later and I had to explain to her why you shouldn't do that... because kids tend to have teachers as friends and everybody... I explained the fact that this is public and that the record stays there forever..."
REP	TP093	"Quite long ago my friends got into my account. I had a strong password, but an easy security question. This made me realize that security is important"
	TP085	"Gay couple experienced discrimination in a reservation they did through one of our hotels. They posted bad reviews about the hotel about the company being homophobic ... there was blind panic within the company. What do you do? How do you react to it?"
STK	TP053	"I used to trust my husband, but then we got divorced. He started stalking me Through bank transactions he knew what I was doing and where I was going."
TPS	TP089	"linkage [of my identity] exists and that it is outside my control, I find that worrying... even if you go into the settings and try to stop all that stuff off"
	TP026	"the connection between searching for something and in a couple of minutes receiving something in my mailbox, I was not feeling comfortable with that"

Table 8: Expectations of a privacy panic button

Expectation	Sample quotes	Codes
Personalized chat / Immediate help	"I would like to have an online chat with someone" (TP027) "I need somebody to talk to, it makes me feel more safe" (TP082) "A chat window.. more personal... I hate FAQs" (TP065) "The best case scenario should offer a real time living person telling you what to do..." (TP097) "I would expect some kind of help immediately.... with someone somehow direct,... like a Whatsapp conversation, like a chat" (TP093) "You should find an answer and a phone number to talk to someone in some cases" (TP096)	DLK; DLO; HIJ; CSC; MSR
Give me instructions	"It will give me instructions on how to recover my files" (TP076) "After posting pictures - let me know how to remove it, or adjust the people who can see the picture" (TP027) "I should get a list of reasons why i panic, the list should cover all possible panic situations, it should be a short list" (TP096)	DLO; MSR; DLK
Freeze or block my accounts	"The panic should be link to all my details, so that when i press it, it would block the accounts... only lock that device [that I selected]" (TP105) "Freeze the activity of your account...It should be easy to unfreeze if i need it" (TP082) "Freeze it [my account], then inform me, with an SMS, about it so i can do something" (TP030)	LMD; STK
Ask me questions to determine the problem	"Maybe a couple of questions, and not more, of what kind of problem is it" (TP026) "Give me a general list of options of why i am in panic... Ask me why very general and go to more specific questions" (TP008)	DLK; LMD
Lead me through steps (Wizard)	"Start a dialogue with me... [it would ask me] why are you concerned?" (TP089) "It will give me instruction on how to recover my files" (TP076)	TPS; DLO
Assess the consequences	"Show me some bullet points with information on about why is it a bad idea to post this" (TP027) "There has to be someone who can measure the seriousness of the situation..." (TP085)	MSR; MSV
Verify my identity	"Only allow someone from this current IP address to access my account... There should be a link where i can authenticate myself, and correlate my answers with the information that the service knows about me" (TP030) "Take me to a screen.... ask me some security questions... ask me information about myself, like my cellphone" (TP053)	HIJ; STK
Get me out of panic	"The user might think that there is some kind of superman coming, but that's not the case" (TP069)	HIJ
Educate me (give information)	"Suggestions of how to alter my actions so that i dont have bad consequences. Then I might learn in the future." (TP027)	MSR

Table 9: Participants' opinions on three metaphors that were shown to them

Wizard
"It cannot be too long or too complicated, because I am in panic" (TP093)
"I don't like it. It looks too Microsoft thingy... always gets me confused, because you need to look, push next, previous, check" (TP026)
"I is useful to have written information, but if there is a visual way to accompany the written information then it is better... in my case, I don't like lots of text. If I'm trying to solve a problem, I want things to be synthesised..." (TP076)
"Depends on how the panic situation is... When someone needs help, he is trying to look for someone that helps, not that asks many questions" (TP069)
"Better if there are not too much words, because when you are in panic the last thing you want is to read... better to do it with yes and no questions" (TP030)
"Good... as long as you are doing something you are not panicking any more... or get the feeling that you are getting somewhere" (TP065)
"You are use to them during installations... it cannot be too many words... videos and pictures would be good" (TP085)
Emergency card
"You have an overview of the steps to reach a solution, which is better than the step by step" (TP093)
"The emergency card in the airplane, should be reviewed before the plane takes off... [too late to look at it when the plane has already crashed]" (TP089)
"Here you can find the help stages at a glance. He can see, these five steps are related to my problem or not... "(TP069)
" Instructions must be easy. People who understand a lot they know what to do, but for people who do not understand that much it must be easy" (TP082)
"Too much text is not a good idea because I am panicking and I want to do something... you are not thinking rational when you are panicking so it has to be easy and fast..." (TP065)
Account freezing
"It would make me feel a little better" (TP093)
"The question is how do you continue with this?!... the problem is that 'the account is frozen' and then how are we going to continue?" (TP093)
"I like it, I like it very much...This is good thing. I can lock the account and look for a solution. It doesn't give the solution like the [wizard or the emergency card], but it helps me feel safe..." (TP026)
"This is what I was thinking of!!... like block my account down for 30 minutes or something... But then again my ex-husband knows my password, so he could go in and unfreeze it.... so that's where this 2-factor would be nice" (TP053)
"If the account is about to be frozen, i would think "ok, fine, but I wanna have a world on it" (TP076)
"I think this solution is also very useful for the user..." (TP069)
"This of course is very very good... then I know for the moment I am safe, what happened happened, damage is done, but for the moment no more damage" (TP08)
"I would definitely use it... you can control access... it is quite good actually" (TP030)
"Oh, that's great! ... For a first step where you don't know what to do is great when you know that there's no more damage done.. where you can activate that and [breathe] 'now i can think" (TP065)
"Like when you lose your credit card!! It can be very helpful in the panic cases... like loosing your phone and someone going to your email... Why haven't someone else thought about this already!!" (TP027)
"It needs to happen quietly, without other people realising that there has been a big problem" (TP085)
"If i suspect that somebody else is accessing my account then yes, but if it has to do with a file that is not recoverable then not, probably not... (TP097)
Other ideas or comments
Friends helping / comforting / supporting other friends
Freeze account first, then provide me with chat support
Inform users about the limitations of the attack
Provide information through media (YouTube, Images, etc.)
Let users undo certain actions