Is this a Privacy Incident? Using News Exemplars to Study End User Perceptions of Privacy Incidents

Pradeep K. Murukannaiah
Rochester Institute of Technology
pkmvse@rit.edu

Jessica Staddon
NC State University
jessica.staddon@gmail.com

Heather Richter Lipford
UNC Charlotte
richter@uncc.edu

Bart P. Knijnenburg
Clemson University
bartk@clemson.edu

Abstract—A clear and efficient process for responding to privacy incidents is widely viewed as necessary for a strong privacy program. In addition, analysis of privacy incidents is advocated to understand risk trends. Both incident response and analysis require an actionable definition of privacy incident, which is challenging to derive given that privacy attitudes vary by culture and context, resulting in variation in incident manifestation. We present a first study of end user understanding of the term “privacy incident” with 482 Amazon Mechanical Turk users. Our study uses a variety of news exemplars, many of which concern the privacy-related concepts of data collection, storage, and usage. We find that although participants appear to closely tie sensitive data collection and usage to privacy, they often conflate privacy and security and are more inclined than privacy law to view perceived or anticipated privacy issues as grounds for an incident. Our study suggests that there is some degree of schism between end user conceptions of privacy and the views of industry and government.

I. INTRODUCTION

Teams dedicated to privacy incident response are increasingly advocated as part of an organization’s privacy program (e.g., [16]). Such teams have the responsibilities of identifying privacy incidents and determining the correct response.

In addition to incident response teams, government organizations (e.g., the U.S. Government Accountability Office [62]) and the privacy research community (e.g., [8, 27, 35]) are also interested in privacy incidents and specifically, how the analysis of incidents can inform policy and technology improvements.

For all these efforts, an actionable and accurate definition of privacy incident is required. Formulating this definition is challenging because privacy attitudes vary by culture [19, 21] and context [30]. As a result, there is variation in incident manifestation. Indeed, privacy perceptions likely vary by stakeholder groups of end users, policy makers, legal scholars and product developers.

We present a first study of end user understanding of the term “privacy incident” with Amazon Mechanical Turk users. Our study uses a variety of news exemplars, many of which concern the privacy-related concepts of data collection, storage and usage. We use news exemplars because real-world examples may be easier for participants to evaluate and because efforts to aggregate and analyze privacy incidents rely heavily on news as a source of incident information (e.g., [27]).

The goal of our study is to assess whether participants closely associate sensitive data collection, usage and/or sharing with privacy incidents, and to explore whether there are unanticipated incident categories either within or outside of the scope of our working definition (see Section II).

We find that although users appear to closely tie sensitive data collection and usage to privacy, they can conflate privacy and security and are inclined to view perceived or anticipated privacy issues as grounds for an incident. The latter differs from privacy legal rulings which often require harm to be “actual or imminent” [33, 43]. We also find that participants tend to classify cyberbullying incidents involving sexual assault as not privacy incidents and have difficulty determining how to classify legal privacy events. Based on participant comments and patterns in article responses, we suggest ways to improve the study of this topic.

In conclusion, we make the following contributions regarding end user perceptions of privacy incidents:

- Evidence that issues of sensitive data collection, usage or sharing are closely associated with privacy incidents.
- Evidence that anticipated or perceived privacy harm is sufficient for an incident.
- Suggestions for future studies in this area to test patterns found in this initial study.

Organization: In Section I-A we discuss related work. We state our working definition of privacy incident in Section II and describe the study design. Study findings are in Section III and we discuss limitations of the study and plans for future work in Section IV. We conclude in Section V.

A. Related Work

Our work lies in the research area of human perceptions of privacy/security, an active ongoing area of research both in academia (e.g., [2, 15, 22] and private research organizations.
Our work is perhaps closest to the study of security operations centers (SOCs) as SOCs include incident response responsibilities (e.g., [42]). However, we focus on privacy rather than security incidents.

We are motivated by recent efforts to aggregate and analyze privacy incidents [8] [27] [35]. Our findings are directly related to those efforts as well as legal analysis of privacy harm [4] and trends in privacy regulation and legislation (e.g., [17]). We support such work with an initial exploration of how such incidents are defined.

II. STUDY DESIGN

Our study explores end user perceptions of privacy incidents as characterized by the following working definition (also associated with the Privacy Incidents Database project [29]).

Definition. A privacy incident is:

1) An instance of accidental or unauthorized collection, use or exposure of sensitive information, OR,

2) An event that creates the perception that unauthorized collection, use or exposure of sensitive information may happen, AND,

3) Involves information that is either being collected, used or shared in digital form.

Research questions for this initial study focus both on whether participants view the specifics of the working definition as closely associated with privacy incidents (RQ1 and RQ2) and whether there are privacy events considered by participants to be incidents but that are beyond the working definition’s scope (RQ3):

RQ1. Do end users perceive the collection, usage and/or sharing of sensitive data to be closely associated with privacy incidents?

RQ2. Do end users recognize events in which it is perceived or anticipated that sensitive data is or will be collected, used or shared, as privacy incidents?

RQ3. Are there privacy events beyond the scope of the working definition (e.g., the release of privacy-enhancing products or privacy laws) that end users recognized as incidents?

To answer these research questions, we conducted an end user study on Amazon Mechnical Turk (AMT) [1]. Our study consists of an online survey with two parts. The first part presents a participant an URL to a news article and asks a series of questions about the participant’s privacy perceptions on the presented news article. The second part asks demographic questions. Our instructions ask the participants to complete the parts and answer the questions within the parts, sequentially.

We asked each participant to complete three HITs at most (a HIT is an instance of the survey associated with a specific article) and paid USD 0.7 (plus USD 0.14 AMT fee) for each HIT. This rate was calculated based on the pilot (described below), so that the hourly rate would be at least the US minimum wage on average. Our study was approved by the Institutional Review Board (IRB) at NC State and we collected an informed consent from each participant.

Tables I and II provide examples from P and N respectively. For a given article, each survey was completed by at least three AMT workers; 97% of the surveys with positive responses from all three AMT workers were used. For a survey to be included in the study, at least two AMT workers must have agreed that the article is a privacy incident. Furthermore, if a participant’s answers are not consistent with the other two, the participant’s responses are excluded from analysis.

The news articles used in the survey consist of 204 of the “positive” examples, P, (a portion of those in the Privacy Incidents Database [29]) and 63 “negative” examples, N, that include incidents involving a security breach with no apparent privacy breach, articles about physical world security, and articles in which privacy is mentioned but is not core to the story. Articles were presented to participants with no indication of whether they came from P or N.

These categories are compatible with our working definition rather than meeting any legal or moral guidelines. The categories are used solely to help us understand participant perceptions.
examples and 100% of the surveys with negative examples, were completed by exactly three participants, for a total of 482 participants.

TABLE I. EXAMPLE ARTICLES FROM THE SET, P. DESCRIPTIONS ARE BOLDED IN PLACES FOR READABILITY.

<table>
<thead>
<tr>
<th>Broad Category</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Breach</td>
<td>Blippy allows some credit card numbers to be indexed by search engines [13].</td>
</tr>
<tr>
<td>Emerging Tech</td>
<td>Police departments building DNA databases of potential suspects [12].</td>
</tr>
<tr>
<td>Surveillance</td>
<td>PA SID remotely activates cameras to locate school laptops.</td>
</tr>
<tr>
<td>Privacy Regulation</td>
<td>Google removes links regarding old criminal convictions, but news articles about removal cause conviction to still be found via search. UK’s ICO issues first public enforcement notice for “right to be forgotten” [31].</td>
</tr>
<tr>
<td>Targeting</td>
<td>Facebook users visit sites with “like” button to target ads [37].</td>
</tr>
<tr>
<td>Surveillance</td>
<td>Kentucky man shoots down drone over property [3].</td>
</tr>
<tr>
<td>Data Breach</td>
<td>Hacker accesses records of 15M T-Mobile customers [28].</td>
</tr>
<tr>
<td>Data Breach</td>
<td>Bug gives users access to Facebook friends’ chats [33].</td>
</tr>
<tr>
<td>Emerging Tech</td>
<td>Man charged with 10 counts of murder based on genetic data from son [39].</td>
</tr>
<tr>
<td>Revenge Porn</td>
<td>Woman posts revenge porn pictures, later convicted under UK law [27].</td>
</tr>
</tbody>
</table>

TABLE II. EXAMPLE ARTICLES FROM THE SET, N.

<table>
<thead>
<tr>
<th>Broad Category</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSA Surveillance</td>
<td>US Congress criticized for seeming to only care about surveillance when its members are personally impacted [45].</td>
</tr>
<tr>
<td>Privacy Regulation</td>
<td>Safe Harbor invalidated by the European Court of Justice [46].</td>
</tr>
<tr>
<td>Physical Security Breach</td>
<td>Security breach at a Donald Trump rally [52].</td>
</tr>
<tr>
<td>Celebrity Privacy Request</td>
<td>Professional athlete asks for privacy as he enters drug rehab [34].</td>
</tr>
<tr>
<td>Wildlife Privacy</td>
<td>Park visitors disturb privacy of animals during mating season [48].</td>
</tr>
<tr>
<td>Security Breach</td>
<td>Security of an electronic road sign is compromised [50].</td>
</tr>
<tr>
<td>Privacy Standards</td>
<td>EFF announces a stronger DNT standard [9].</td>
</tr>
<tr>
<td>Security/Privacy Law</td>
<td>Companies warn about privacy implications of cybersecurity bill [44].</td>
</tr>
</tbody>
</table>

We arrived at the survey wording shown in Figure 1 after a small pilot of three positive and two negative articles, each shown to three participants. The pilot survey differed from the final form in two ways. First, we asked whether the article discussed a privacy incident in a broader way. Specifically, question 2 was, “Does this article describe a privacy incident?”. Second, while the pilot also asked about the collection, usage and exposure of digital information, it did not state that one of those conditions was necessary for an event to be a privacy incident. Specifically, the wording was, “Considering your answers to the previous two questions, please answer the following question again in case your view has changed: Does this article describe a privacy incident?”.

In the pilot, all of the articles (positive and negative) were reported to be privacy incidents initially and only a single participant changed their answer to be negative after considering the digital information issues. The comments indicated the participants were casting a very wide net and looking for any potential privacy aspect to the articles. To remedy this we added the “primarily” language, to try to focus the participants on the main aspects of the articles and we were more explicit about the necessary link between digital information issues and privacy incidents.

We ran a small follow-up pilot, of five positive and five negative articles, with the new language. The responses for the follow-up pilot were more diverse than the first pilot. Thus, we launched the survey more broadly and gathered the data described in Section III.

The participants came from 46 states, with the highest numbers from California (61), Texas (36), and Florida (32). We did not evaluate the privacy or security knowledge of the participants, however we note that previous studies have found AMT participants to be more privacy-aware than the general public [18]. Additional details on the distributions of demographic variables are in Appendix (Table IV).

The complete list of articles tested (both P and N) is available at: [http://goo.gl/qRcFxC]

III. FINDINGS

As is typical in crowd-sourced classification tasks, we require a majority of participants to agree before considering an article to be classified as a privacy incident or a non-privacy-incident. That is, we define a crowd-sourced classifier function, $C()$, which takes an article, $A$, as input:

$$C(A) = \begin{cases} 1 & \text{majority: } A \text{ is a privacy incident} \\ 0 & \text{majority: } A \text{ is not a privacy incident} \\ \text{undef} & \text{no majority} \end{cases}$$

We calculate the precision of our positive set, $P$, as:

$$\text{Precision}(P) = \sum_{A \in P; C(A) \in \{0,1\}} \frac{C(A)}{|P|}$$

Analogously, the precision of our negative set, $N$, is:

$$\text{Precision}(N) = \sum_{A \in N; C(A) \in \{0,1\}} \frac{1 - C(A)}{|N|}$$

We measure precision both initially (question 2) and after data privacy aspects are raised (questions 4, 5, and 6) and we refer to those measurements as the initial precision and final precision, respectively.

COLLECTION/USAGE/SHARING (RQ1)

Among the positive articles, $P$, we find little change in precision, with an initial precision of 0.799 and a final precision of 0.794. Among the negative articles, $N$, initial precision is 0.54 and final precision is 0.60.

The fact that precision is fairly stable both before and after participants are exposed to the working definition indicates that
participants view sensitive data collection, usage and/or sharing as core to their understanding of the term “privacy incident.” It appears that participants are more likely to see the collection, usage and sharing aspects as necessary for a privacy incident, than as sufficient, since when considering articles in \( N \) that did not involve those aspects, several participants changed their assessment from incident to non-incident, whereas assessments for articles in \( P \) changed little.

In addition, we note that data collection, use and exposure frequently came up in the incident summaries. Participants mentioned both actual cases of collection, use and exposure as well as the possibility of each, when reporting an article was about a privacy incident.

**Anticipated/Perceived Privacy Harm (RQ2)**

Since the difficulty in measuring privacy harm (e.g., \( H \)) means that whether harm is perceived/anticipated or actual is often the subject of debate, we take a conservative approach and only consider articles about privacy events that are yet to be experienced by most users and so are unlikely to have led to instances of concrete harm. In particular, we consider technologies that are emerging (e.g., usage of DNA testing and face recognition technology; 13 articles) and so necessarily have anticipated privacy issues, and privacy policy changes (5 articles) that are newly in effect or waiting to go into effect.

In the case of emerging technologies, we see a strong trend toward classifying the articles as privacy incidents—precision of 0.769 both before and after the definition. One participant said the following about an article concerning planned data collection by cars \( C \), “The article points out a problem of data collection in new vehicles without the owner having any control of the data recorded.”

The trend is less pronounced in the case of privacy policy changes—a precision of 0.714 before the definition and 0.643 after. However, none of the articles achieved a majority of non-incident designations, indicating participants had difficulty assessing these events in the context of the definition. Several participants indicated the definition did not match because the article was not about an incident, but rather an event that potentially impacts multiple incidents. As one participant said in regard to an article about Oculus Rift’s privacy policy \( O \), “It’s about privacy [sic] of a device, but not one particular incident.”

**Definition Scope (RQ3)**

Participant responses suggest privacy law events and security breaches that do not involve privacy breaches, are not consistently viewed as non-incidents even though our definition is not intended to include them. Our sample included 13 articles about legal privacy events (related to privacy laws and regulations, not organization-level policies), and participants only considered 3 of them to be non-incidents before the definition was given, and 2 of them, after. The fact that the laws are closely motivated by privacy incidents was referenced by several participants. For example, one participant said the following about an article concerning the unification of EU data protection laws \( L \), “The entire article talks about privacy. That there is a whole new framework taking place to protect the privacy of European citizens.”

Our sample contains 3 articles about digital security incidents that do not involve a privacy breach, of which 2 were reported to be privacy incidents. Comments from participants suggest difficulty in separating the notions of security and privacy. For example, in response to an article about the hacking of a road sign to post funny messages \( S \), one participant said, “There are laws in place to try to protect the privacy of people’s networks and computers, and someone (or more than one person) has hacked into the system to make changes that they were not given permission to do, and this is a crime.”

Another point of disagreement between our data sets and participant views was cyberbullying incidents involving sexual assault. None of the 4 such articles were considered privacy incidents, likely because the violent nature of the events was seen as their dominant attribute. As one participant said about a cyberbullying case that ended in suicide \( U \), “I don’t think it is a privacy incident so much as it is an article about the stupidity of some high school students in this cruel, immoral act. They did document it via social media which helped with their convictions but it was more about rape than about privacy.”

Finally, we note that participants viewed 2 of the 3 articles about the release of privacy-enhancing products as privacy incidents. They also tended to view privacy position pieces (e.g., editorials) as privacy incidents. Privacy position pieces are in set \( N \), however, since in many cases the articles do describe various privacy incidents at least briefly, it is debatable whether they should be in \( N \) or \( P \).

Table \( T \) provides examples of articles with high positive agreements, high negative agreements, and those with a lack of consensus.

In summary, the stability of precision results for \( P \), a set of positive examples gathered by applying our definition, is evidence that the working definition is compatible with end-user expectations for privacy incidents. In addition, the increase in precision on the set \( N \) when aspects of the definition are emphasized, suggests data collection, usage and exposure are core to user perceptions of privacy. However, there is still substantial disagreement amongst articles in \( N \). With further analysis we hope to determine if that disagreement suggests ways to improve the definition.

**IV. Limitations and Future Work**

Using news articles to study incident perceptions presents challenges, as it introduces additional variables that may influence participant responses. For example, the perceived authoritativeness and/or neutrality of the news is one particular influencing variable. Our initial study does not control for this variable, or explore its impact.

We noticed after the study that six of the articles in our sample are behind a paywall and so participants may have only had the first paragraph of the article on which to base their responses. For the rest of the articles, full text is available from the links we provided.

Related to this is the influence of language, and specifically, whether participants are biased by the presence of the word “privacy” in the articles. While such bias is likely, “privacy” does not appear to have been viewed by participants as a
necessary and sufficient condition for a privacy incident. In the positive set, $P$, 14 articles that contain “privacy” were reported to not be privacy incidents by a majority of participants. Similarly, 4 of the 25 articles in $N$ that were reported to be privacy incidents, do not contain “privacy”.

In subsequent work, we plan to include articles from different sources covering the same events to control for bias associated with source. We also plan to increase the article support across several areas to test some of our low-support findings. For example, we find participants have some difficulty distinguishing security and privacy, but since we have only 3 articles that concern digital security but not digital privacy, it is not possible to identify specific incident attributes that make the task difficult. With a broader data set it will be possible to explore whether certain areas of security are more intertwined with privacy and whether the language used to present the event increases separation difficulty.

While the simplicity of our survey helped reduce response time, there are several areas that can be explored with a more complex survey. In particular, while we gather data on the incident attributes participants consider when deciding whether an event is an incident, we do not know what actions they expect to be associated with incidents, if any. If, for example, a participant expects the Federal Trade Commission (FTC) or another regulatory body to investigate incidents, rather than a smaller investigation conducted just by the organization(s) involved, that may influence their response. Similarly, if participants are given a task that their responses support, e.g., identifying incidents for a repository (e.g., [29]), this task may influence responses (e.g., by perhaps encouraging the selection of news articles over editorials in the former case, as these are more likely to focus on new events). In future work, we will explore what expectations (if any), participants have for privacy incident response and how those expectations may influence selection.

Our category analysis (e.g., the identification of articles about privacy policy changes, emerging technologies, etc.) relies on single coder (one of the authors). We have confidence in the coding because the categories are coarse, but in future work, where we seek a more nuanced understanding of perception, multiple coders will be essential.

Finally, our findings may be specific to the US end user population since we restricted our study to AMT participants from the US. Our motivation in doing so was to reduce potential culture-specific biases on privacy perceptions among participants. Studying how users from different cultures perceive privacy incidents is an interesting avenue for future work.

V. Conclusion

We presented what is, to the best of our knowledge, the first study of end user conceptions of privacy incidents. Understanding end user perceptions of “privacy incidents” is increasingly important, given the prevalence of privacy incident response teams and the fact that, given the rapid growth of the privacy profession, it is likely that professionals with little or no formal training on the concept of privacy incident are tasked with incident response work. Our study suggests gaps that training should address, such as conflation of security and privacy. In addition, our findings suggest that anticipated or perceived privacy harm may be more important to users than to privacy law; and so are criteria worth considering when evaluating whether an event should be considered a privacy incident.

Acknowledgment

Thanks to the US Department of Defense (Science of Security Lablet grant) for partial support.

References

[47] J. Trop, “The next data privacy battle may be waged


APPENDIX

Figure [2] shows the demographics survey we asked AMT workers, who participated in our study to complete and Table [IV] shows the distributions of the participants responses.

<table>
<thead>
<tr>
<th>Part 2</th>
</tr>
</thead>
</table>

Please answer the following questions about demographics.

1. What is your gender?
   - Male
   - Female
   - Other
   - Decline to state

2. Which of the following categories includes your age?
   - 18–20
   - 21–29
   - 30–39
   - 40–49
   - 50–59
   - 60 or more
   - Decline to state

3. In what US state or territory do you live in?

4. Which of the following best describes the area you live in?
   - Urban
   - Suburban
   - Rural
   - Other
   - Decline to state

5. Are you a US national?
   - Yes
   - No
   - Not sure
   - Decline to state

6. If you are not a US national, how long have you been living in the US?

7. Please provide additional comments, if any.

---

Fig. 2. The demographics survey completed by AMT workers.

**TABLE IV.** The distribution of demographic variables based on AMT workers’ responses.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Male: 59.08%; Female: 40.52%; Other: 0.2%; Decline to State (DTS): 0.2%</td>
</tr>
<tr>
<td>Location Type</td>
<td>Rural: 15.37%; Suburban: 50.9%; Urban: 33.53%</td>
</tr>
<tr>
<td>US National</td>
<td>Yes: 92.63%; No: 6.37%; Not Sure: 0.6%; DTS: 0.4%</td>
</tr>
</tbody>
</table>