(Work In Progress) 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 [32]) 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.

USEC '17, 26 February 2017, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2017.23030

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

(see, for example [6, 34]. 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.

Part 1

Read the news article from the URL below and answer the following questions.

${articleUrl}

1. In a sentence, please summarize the article above.

   _____

2. Is this article primarily about a privacy incident?

   ○ Yes ○ No ○ Not sure

3. Briefly describe why it is or is not a privacy incident.

   _____

4. Is this article primarily concerned with the collection, use or exposure of sensitive information?

   ○ Yes ○ No ○ Not sure

5. Is this article primarily concerned with information that is either being collected, used or shared in digital form?

   ○ Yes ○ No ○ Not sure

6. Consider now that for an article to be primarily about privacy incident, the answers to the previous two questions must be yes. Given this, do you think the article is primarily about a privacy incident?

   ○ Yes ○ No ○ Not sure

7. If you changed your mind, please describe why.

   _____

Fig. 1. The main portion (first part) of the survey completed by AMT workers. The demographic questions (second part) are in the Appendix.

The first part of our survey (Figure 1) begins by capturing the participant's initial conception of a privacy incident in questions 2 and 3. Questions 4 and 5 ask participants to consider whether issues of collection, usage and exposure of *digital* information are present in the article and question 6 whether the article describes a privacy incident if those issues are viewed as necessary conditions. By comparing answers to questions 6 and 7 with answers to questions 2 and 3 we can gauge whether participants initially considered digital information collection, use and/or exposure to be attributes of a privacy incident. Evidence that these aspects help resolve differences between participants speaks to whether a definition that relies upon them is implementable.

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.[1]

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

[1]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.

Broad Category	Example
Data Breach	Blippy allows some **credit card numbers** to be **indexed** by search engines [13].
Emerging Tech	Police departments building **DNA databases** of potential suspects [12].
Surveillance	PA SD **remotely activates cameras** to locate school laptops.
Privacy Regulation	Google removes links regarding old criminal conviction, 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].
Targeting	Facebook uses visits to sites with "like" button to **target ads** [37].
Emerging Tech	"Hello Barbie" **records voices** of **kids** [14].
Surveillance	Kentucky man shoots down **drone** over property [5].
Data Breach	**Hacker accesses records** of 15M T-Mobile customers [28].
Data Breach	Bug gives users **access** to **Facebook friends' chats** [51].
Emerging Tech	**Man charged** with 10 counts of murder based on **genetic data from son** [39].
Revenge Porn	Woman posts **revenge porn** pictures; later convicted under UK law [7].

TABLE II. EXAMPLE ARTICLES FROM THE SET, N.

Broad Category	Example
NSA Surveillance	US Congress criticized for seeming to only care about surveillance when its members are personally impacted [45].
Privacy Regulation	Safe Harbor invalidated by the European Court of Justice [46].
Physical Security Breach	Security breach at a Donald Trump rally [52].
Celebrity Privacy Request	Professional athlete asks for privacy as he enters drug rehab [24].
Wildlife Privacy	Park visitors disturb privacy of animals during mating season [48].
Security Breach	Security of an electronic road sign is compromised [50].
Privacy Standards	EFF announces a stronger DNT standard [9].
Security/Privacy Law	Companies warn about privacy implications of cybersecurity bill [44].

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/qRcFCx

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, $C(\cdot)$, which takes an article, A, as input:

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

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

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

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

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

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., [4]) 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 [47], "*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 [23], "*It's about pricacy [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 [11], "*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 [50], 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 [49], "*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 III provides example 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

TABLE III. EXAMPLES FROM SETS P AND N OF ARTICLES FOR WHICH A MAJORITY OF PARTICIPANTS REPORTED THE ARTICLE TO BE A PRIVACY INCIDENT (POSITIVE MAJORITY EXAMPLES), NON-PRIVACY-INCIDENT (NEGATIVE MAJORITY EXAMPLES) OR DID NOT REACH A CONSENSUS, BY COLUMN. ALL THE "NO CONSENSUS" ARTICLES, RECEIVED 1 YES, 1 NO AND 1 "NOT SURE". ANSWERS TO QUESTIONS 2 AND 6 WERE THE SAME ACROSS THE ARTICLES IN THE FIRST TWO COLUMNS.

Article Set	Positive Majority Examples	Negative Majority Examples	No Consensus
P	(1) "*This is a privacy incident as Google did not announce doing this, nor had permission from either Apple nor its Safari users to backdoor a tracking cookie.*" Article on surveillance, [36]	(1) "*It's not really about a specific incident, but about ongoing privacy concerns and government power.*" Article on tracking, [38]	(1) "*I believe it is not a privacy incident as sensitive information is not being collected or shared with others.*" Article on app data collection [41]
	(2) "*Private information that had been collected electronically was stolen and could lead to identity theft.*" Article: [28]	(2) "*It is not so much about privacy as it is about comfort in reporting an assault.*" Article: [40]	(2) "*The article doesn't mention a specific privacy incident, just privacy in general.*" Article: [3]
N	(1) "*It is about the privacy of everyone. Even europeans who have data moved to the us.*" Article on safe harbor invalidation [46]	(1) "*Though it would make people uncomfortable, it is not about privacy.*" Article on N.C's HB2, [20]	(1) "*It's a privacy issues because Apple customers still believe they can be tracked regardless if they opt out*" Article on tracking opt-out [10]
	(2) "*It is a privacy incident because it focuses on DNT and the privacy that is at risk.*" Article on DNT standard, [9]	(2) "*It seems more like a report on a polling about the privacy and security of the people, and how they feel their private lives are.*" Article on surveillance perceptions, [26]	(2) "*It is not an incident on privacy, it is about a report written on privacy in general.*" Article on surveillance report, [25]

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

[1] Amazon Mechanical Turk, https://www.mturk.com.
[2] A. Besmer and H. R. Lipford, "Privacy perceptions of photo sharing in Facebook," in *Proc. SOUPS*, 2008.
[3] N. Bilton, "Price of Facebook privacy? Start clicking," *The New York Times*, May 12, 2010.

[4] R. Calo, "The boundaries of privacy harm," *Indiana Law Journal*, vol. 86, no. 3, p. 1131, 2011.

[5] R. Cummings, "Hillview man arrested for shooting down drone; cites right to privacy," July 31, 2015.

[6] Eurobarometer, "Data protection fact sheet," http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf, June 2015.

[7] B. Farmer, "Revenge porn: First woman sentenced for offence is spared jail," *The Telegraph*, September 1, 2015.

[8] S. Garfinkel and M. F. Theofanos, "A collection of non-breach privacy events," February, 2016.

[9] S. Gibbs, "Privacy pressure group EFF announces stronger Do Not Track standard," *The Guardian*, August 4, 2015.

[10] ——, "Facebook's new opt-out for tracking ads is not enough, says privacy expert," *The Guardian*, September 18, 2015.

[11] ——, "EU states agree framework for pan-European data privacy rules," *The Guardian*, June 15, 2015.

[12] J. Goldstein, "Police agencies are assembling records of dna," *The New York Times*, June 12, 2013.

[13] J. V. Grove, "Blippy users' credit card numbers exposed in Google search results," *Mashable*, April 23, 2010.

[14] S. Halzak, "Privacy advocates try to keep 'creepy,' 'eavesdropping' Hello Barbie from hitting shelves," *Washington Post*, March 11, 2015.

[15] E. Hargittai *et al.*, "Facebook privacy settings: Who cares?" *First Monday*, vol. 15, no. 8, 2010.

[16] R. Herold and F. CISM, "Building an effective privacy program," *Information Systems Security*, vol. 15, no. 3, pp. 24–35, 2006.

[17] C. J. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*. Cambridge University Press, 2016.

[18] R. Kang, S. Brown, L. Dabbish, and S. B. Kiesler, "Privacy attitudes of Mechanical Turk workers and the US public." in *SOUPS*, 2014, pp. 37–49.

[19] N. Kaya and M. Weber, "Cross-cultural differences in the perception of crowding and privacy regulation: American and turkish students," *Journal of Environmental Psychology, Volume 23, Issue 3*, pp. 301–309, September 2003.

[20] T. Kopan and E. Scott, "North Carolina governor signs controversial transgender bill," *CNN*, March 24, 2016.

[21] H. Krasnova, N. Veltri, and O. Gunther, "Self-disclosure and privacy calculus on social networking sites: The role of culture," *Journal of Business and Information Systems Engineering, Volume 4, issue 3*, pp. 127–135, June 2012.

[22] P. Kumaraguru, L. F. Cranor, and E. Newton, "Privacy perceptions in India and the United States: An interview study," in *The 33rd Research Conference on Communication, Information and Internet Policy (TPRC)*, 2005, pp. 23–25.

[23] A. Liptak, "There are some super shady things in Oculus Rift's terms of service," *Gizmodo*, April 2, 2016.

[24] T. Lutz, "Johnny Manziel asks for privacy as he enters rehab," *The Guardian*, February 2, 2015.

[25] E. MacAskill, "Privacy campaigners win concessions in UK surveillance report," *The Guardian*, July 13, 2015.

[26] T. McMullen, "Guardian readers on privacy: 'we trust government over corporations'," *The Guardian*, October 18, 2015.

[27] P. K. Murukannaiah, J. Staddon, H. R. Lipford, and B. P. Knijnenburg, "Principedia: A privacy incidents encyclopedia (working paper)," *Privacy Law Scholars Conference*, 2016.

[28] R. Nasr, "Experian data breach hits more than 15m T-Mobile customers, applicants," *CNBC.com*, October 1, 2015.

[29] NCSU, UNCC, Clemson University, and RIT, "The privacy incidents database research project," https://research.csc.ncsu.edu/privacyincidents/index.php.

[30] H. Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.

[31] C. O'Donoghue and C. Taylor, "UK first: Right-to-be-forgotten notice issued against Google Inc." *JD Supra Business Advisor*, September 3, 2015.

[32] G. A. Office, "Report to congressional requesters: Data breaches are frequent, but evidence of resulting identity theft is limited; however, the full extent is unknown," GAO-07-737, 2007.

[33] D. M. Poland and M. M. York, "Standing requirement of actual or imminent injury continues to thwart data breach lawsuits," *Godfrey and Kahn Law: Data Privacy and Cybersecurity Flash*, October 2014.

[34] L. Rainie and M. Madden, "Americans' privacy strategies post-snowden," Pew Internet & American Life Project, http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/, Tech. Rep., March 16 2015, accessed: December 12 2016.

[35] S. Romanosky, "Examining the costs and causes of cyber incidents," *Twelfth Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective*, January, 2016.

[36] C. Savage, "White house seeks to clarify F.B.I. powers vis-à-vis e-mail," *The New York Times*, July 29, 2010.

[37] T. Simonite, "Facebook's like buttons will soon track your web browsing to target ads," *MIT Technology Review*, September 16, 2015.

[38] R. Singel, "Google busted with hand in Safari-browser cookie jar," *Wired*, February 17, 2012.

[39] N. Singer, "In fighting crime, how wide should a genetic net reach?" *The New York Times*, July 24, 2010.

[40] ——, "The war on campus sexual assault goes digital," *The New York Times*, November 13, 2015.

[41] B. Sullivan, "A shock in the dark: Flashlight app tracks your location," *NBC News*, JAN 16 2013.

[42] S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S. R. Rajagopalan, "A human capital model for mitigating security analyst burnout," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 347–359.

[43] Supreme Court of the United States, "Spokeo, Inc. v. Robins," October Term 2015, argued November 2, 2015—Decided May 16, 2016.

[44] S. Thielman, "Tech giants warn cybersecurity bill could undermine users' privacy," *The Guardian*, October 15, 2015.

[45] T. Timm, "Lawmakers only care about others' privacy when their own is at stake," *The Guardian*, December 30, 2015.

[46] ——, "The Snowden effect: New privacy wins await after data transfer ruling," *The Guardian*, October 8, 2015.

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

inside your car," *The New York Times*, January 10, 2014.
[48] H. Warwick, "Photographers – don't pap our wild animals, they need some privacy too," *The Guardian*, November 10, 2015.
[49] Wikipedia, "Steubenville high school rape case," https://en.wikipedia.org/wiki/Steubenville_High_School_rape_case.
[50] C. Wolf, "Some local prankster keeps hacking the road sign on Bumby Avenue," *Orlando Weekly*, September 22, 2015.
[51] J. Wortham, "Facebook glitch brings new privacy worries," *The New York Times*, May 5, 2010.
[52] J. Zhou, "Watch: Donald Trump shielded by secret service agents after security breach at rally," *Epoch Times*, March 12, 2016.

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.

Part 2

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.

Variable	**Distribution**
Gender	Male: 59.08%; Female: 40.52%; Other: 0.2%; Decline to State (DTS): 0.2%
Age Group	18–20: 3.39%; 21–29: 35.66%; 30–39: 32.67%; 40–49: 15.74%; 50–59: 8.76% 60 Plus: 3.78%
US State (Top 5)	California: 12.15%; Texas: 7.17%; Florida: 6.37%; New York: 6.18%; Pennsylvania: 5.18%
Location Type	Rural: 15.57%; Suburban: 50.9%; Urban: 33.53%
US National	Yes: 92.63%; No: 6.37%; Not Sure: 0.6%; DTS: 0.4%