Victim Privacy in Crowdsourcing Based Public Safety Reporting: A Case Study of LiveSafe

Huichuan Xia
Syracuse University
hxia@syr.edu

Yun Huang
Syracuse University
yhuang@syr.edu

Yang Wang
Syracuse University
ywang@syr.edu

ABSTRACT

Prior works in criminology have studied victims' privacy protection in extreme cases such as rape, but little is known about victims' privacy concerns and experiences in less severe incidents. Also, little has studied on privacy issues in crowdsourcing based reporting systems. In this paper, we conducted a case study with LiveSafe which is a popular crowdsourcing based safety reporting system. We reported our initial interview results with several victim students about their privacy concerns and experiences, and then we discussed about how to protect victim privacy as well as some special challenges to achieve it. To the best of our knowledge, this work is pioneering in this research field.

1. INTRODUCTION

Victims are a vulnerable group. Privacy protection for crime victims has been discussed in extreme situations, e.g., rape, under the notions of victims' constitutional privacy rights [1]; and the conflicts between such rights and the freedom of the press to disclose the victims' identity [2] or the mandatory HIV testing under certain conditions [10]. In less severe incidents, however, victims' privacy concern and protection have not been extensively studied. Prior research also suggested that crowdsourcing based safety reporting system could bring certain privacy concerns, e.g., identity disclosure, to victim [4], but it still lacks empirical data from the victims to support it.

Inclusive privacy and security are important for victims because privacy concerns may deter them from using the reporting application, discourage their reporting intention, and leave them long-term psychological shadow for reporting behavior. In our study, we found that even in less severe contexts, such as harassment and burglary, some victims were still concerned about their privacy for various reasons. In a broad context, victims using a mobile crowdsourcing system for reporting can be seen as "crowd members" whose privacy could also be at stake due to deliberate data triangulation (e.g., [6]). For example, LiveSafe is using Google Map which may be linked to a user's Google account, and it can be signed up with a user's Facebook account. Also, LiveSafe has the functions to "Watch a friend walk" and "Ask friends to watch me walk" which once enabled, will access to the contacts on the phone. If a victimization occurs, it could inter-connect and inter-depend the victim and her friends' privacy and safety together. These features add up potentialities to de-anonymize a user.

In the remainder of the paper, we will first introduce the LiveSafe app, including its functionality and privacy policy; then we will report several LiveSafe users, who were victims as well, about their privacy perceptions and experiences; finally, we will discuss about how to better protect victims' privacy and some special challenges to achieve it.

2. LIVESAFE APP

LiveSafe is a crowdsourcing based public safety reporting application that has been adopted and promulgated widely in U.S. universities and communities [7]. The major reporting functions include: (1) "Report Tips," which include 11 types of non-emergent incident types, e.g., alcohol/drug, and each offers the choices to add picture, audio, and video files to report, either anonymously or non-anonymously; and (2) "Emergency Options," which have the options to call 911, call or message Department of Public Safety (DPS) on campus. LiveSafe also has other social features such as "Safety Map," which provides the location information for nearby safety or health facilities on Google Map, and "Safe Walk," which allows the users' friends to watch her walk, e.g., in some remote area; or let the user to watch her friend's walk.

As regards its privacy policy on the app, it acknowledges that the app may collect sensitive information upon the user's consent to provide, such as the contact list, current health status, potential criminal activity, and social or ethical origin. Reasonably, the app would also collect the location information, but the app could also obtain information from other sources, e.g., Facebook, if the user chooses to sign up with their Facebook account [8]. We notice, however, the privacy protection is not quite strong on the app other than the option of sending the report anonymously. For example, in taking a picture or video in an non-emergent harassment incident, the victim's face or other identifiable information may be revealed in the photo or video, even if the witness reported it anonymously.

3. VICTIM PRIVACY CONCERNS

From March 2017 to April 2017, we conducted an interview study with 15 participants in our university about their perception and usage of LiveSafe. Nine were victims of different

Symposium on Usable Privacy and Security (SOUPS) 2017, July 12–14, 2017, Santa Clara, California.

crimes and most of them were not in severe cases such as rape. Our study has been approved by the IRB department in our university.

3.1 Concern about Tracking

One victim used to hear about her friend's story of being stalked online and offline, after her experience in a harassment incident, she becomes more alert about being tracked by the harasser:

"So after this experience [harassment] I have a very high concern that the man can use Facebook and search where I am and where I go, I'm afraid I am really targeted and he started to do something really deep and horrible to me, so I do have that concern so that's why I didn't post it onto like Facebook or say something about it" (V1, Female, Harassment).

This victim was worried about being stalked or retaliated by the harasser because social media like Facebook has become so prevalent and traceable to people's life and trajectory, thus she chose not to reveal it on Facebook or to her friends.

3.2 Concern about Officer's Responsibility

Another victim was reserved to disclose his identity until he could ascertain the officer to be responsible and trustworthy:

"I would like to be anonymous first and then until the officer who is in responsible for this who want to talk with me about the further details, then I will definitely provide my name or any address" (V2, Male, Burglary).

In this case, the victim prefers anonymity until he could ascertain that the officer is responsible and reliable to deal with the incident. It implies the importance of mutual trust between the victim and the police or DPS officer in charge.

3.3 Concern about Individual and Organization's Reputation

Another female victim was in a more severe case of sexual assault. Using the third person's tone, she told us her understanding of anonymity to victims in a sexual assault case:

"Wanting to be anonymous is like victims of assault or something where they feel embarrassed or ashamed and they need help and they want justice in a certain situation and don't know how to get it, or if there's an association with bigger organization and it's bigger than the person" (V10, Female, Sexual assault).

She explained that her concern to remain anonymous is related with individual embarrassment and shame in some assaults. What she meant of "bigger organization" is that some reporting, if done non-anonymously, could blemish the reputation of an organization which the victim is belong to (in her case, it is the Greek Life Sorority). Hence, in her mind, privacy concern is not merely about an individual's interest, but also associated with some organization's reputation "bigger than the person."

3.4 Concern about Exploitation and Shame

The same victim also shared with us her view as a witness on the scene, about taking photo/video of a victim:

"I would hate for someone to take a video of me in that condition [being drunk], so that's why I was more concerned with getting her help [her friend in intoxication] immediately and getting her in private behind doors...for me there are many people that I still do not tell about my sexual assault just because it is a big shame for women feel being intoxicated in public and being a victim of sexual assault...I would feel so exploited and so self conscious if somebody took a video of me drunk."

As a former victim in a sexual assault, she showed her empathy and care for her friend's privacy, even though her friend was not in a severe incident. Echoing to her own victim case above, it implied that her privacy consciousness is not only about the information collection and revelation, but is also about the exploitation and shame on a female victim.

4. VICTIM PRIVACY PROTECTION

First, we propose the protection beyond anonymity; then we provide ideas to adjust photo/video features for reporting; finally, we discuss the special challenges to victim privacy.

4.1 Privacy Protection beyond Anonymity

First, data minimization, so long as not at the expense of losing essential details for investigation, should be applied. Data minimization means that three aspects of data collection should be minimized: (1) the possibility to collect an individual's personal data; (2) the collecting behavior within certain boundaries; and (3) the retention of the collected data [9]. to protect victim privacy, this principle indicates that contextually, irrelevant personal identifiable information (PII), e.g., health information, should not be collected; the victim's comfortableness of disclosure should be respected as a boundary; and collected information from the victim should have limited retention. As regards LiveSafe, it leaves little control for victim in reporting and it has a very generic privacy policy on data retention [8].

Second, unlinkability should be applied to the extent that a victim user could not be easily de-anonymized. Unlinkability means that a user can use multiple resources or services without other people being able to link these usages together [9]. For crowdsourcing based system such as LiveSafe, we propose that it should at least consider the trade-off between linking and un-linking to a user's Facebook account or Google account. For example, linking the app to a user's Facebook account could increase the probability of de-anonymizing the user, and increase the risk of online tracking and stalking which as our participant V1 articulated, would be a strong privacy concern for the victim.

Finally, social transparency, to a certain degree, should be implemented to enhance mutual trust between the victim reporter and the police or the DPS officer. Social transparency is "the availability of social metadata surrounding information exchange" [11]. Prior research has found that certain social transparency, such as revealing profile information could increase mutual trust and credibility [11]. In the context of public safety reporting, we propose that the system could consider revealing some policemen or DPS officers' profile information according to different incident types, which echoing to V2's viewpoint, could mitigate certain disclosure pressure and privacy concern.

4.2 Adjusting Photo/Video Features to Report

First, system user should be able to adjust the photo/video resolution for reporting. For example, there could be a hori-

zontal slider in the photo/video reporting page that enables the user, e.g., a witness, to adjust the resolution of the shooting image. In extremely offensive and sensitive cases like rape or sexual assault, the witness could slide the bar to mosaic to blur the victim's face or other identifiable information, e.g., the name of the sorority, in order to protect the victim's privacy; in less sensitive but more public incident like car accident or vandalism, the witness could slide the bar to high resolution to report more details of the context.

Second, the reporting system, such as LiveSafe, could consider to apply default photo/video resolutions for different incident types. For example, the default resolution for the sexual assault situation should be mosaic, and for accident or vandalism could be high. Resolution adjustment and image blurring techniques have been proposed and applied in several domains to protect people's privacy. For example, Frome et al. [3] proposed image blurring in Google Street View to protect pedestrians and drivers' privacy; Lasecki et al. [5] demonstrated a method to adjust the obfuscation level of online behavioral videos for coding while protect participants' privacy therein. We propose that similar efforts should be tested and applied in public safety reporting.

Finally, we noticed that in LiveSafe, photo/video will be stored at the user's phone. It may be necessary for keeping the evidence occasionally, but it might disrespect victims' privacy or willingness in more sensitive and severe circumstances. We propose that the reporting system should at least give its users the choices to send with or without storing the photo/video locally.

4.3 Special Challenges to Victim Privacy

Comparing to conventional phone-call, crowdsourcing based reporting system could introduce special challenges to victim privacy. First, it can offer multiple media and channels for reporting which may contain more victim's private information. In LiveSafe, a safety report can combine photo, audio, video, and texts to depict the incident and the victim, which can reveal much more personal information, such as her body condition and victimization status, than in a phone-call report. In addition, such "multimedia based" report can be sent instantly within a few buttons by a crowd of witnesses on which the victim literally has no control.

Second, crowdsourcing based reporting system could easily broadcast the situation to the multitudes. For instance, LiveSafe users not only can report to the police or DPS, but also to their friends. The broadcasting feature is an advantage of crowdsourcing based reporting system comparing to phone-call [12]. But such broadcasting could also compromise victim privacy since sensitive information, like that in photo/video could be taken and disseminated more widely.

Third, a special challenge is to balance between revealing sufficient detail for investigation and not revealing too much detail of the victim. In severe cases like rape, the conflicts between the victim's privacy right and the press freedom or the mandatory HIV testing [2, 10] may be understandable, but we found and propose that in less severe cases, conflict and compromise still exist between to reveal or not to reveal. Both sides could be legit in the name of benefiting the victim yet neither could achieve it if one side overwhelms the other.

5. CONCLUSION

In this paper, we discussed about victim privacy with a case study of LiveSafe and reported our pilot interview results with several victims about their privacy concerns and experiences. We propose that future research in inclusive privacy and security needs to learn furthermore about victim privacy and to collaborate with crowdsourcing system designers as well as criminology scholars to better protect victim privacy.

6. ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under Grant No. 1464312. Any opinions, findings, and conclusions or recommendations in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. We also thank Qunfang Wu and Qiuyan Liu for their contribution to the project.

7. REFERENCES

[1] D. E. Beloof. Enabling rape shield procedures under crime victims' constitutional privacy rights. *Suffolk UL Rev.*, 38:291, 2004.

[2] D. W. Denno. The privacy rights of rape victims in the media and the law: Perspectives on disclosing rape victims' names. 1993.

[3] A. Frome, G. Cheung, A. Abdulkader, M. Zennaro, B. Wu, A. Bissacco, H. Adam, H. Neven, and L. Vincent. Large-scale privacy protection in google street view. In *2009 IEEE 12th International Conference on Computer Vision*, pages 2373–2380.

[4] Y. Huang, C. White, H. Xia, and Y. Wang. A computational cognitive modeling approach to understand and design mobile crowdsourcing for campus safety reporting. *International Journal of Human-Computer Studies*, 102:27–40, 2017.

[5] W. S. Lasecki, M. Gordon, W. Leung, E. Lim, J. P. Bigham, and S. P. Dow. Exploring privacy and accuracy trade-offs in crowdsourced behavioral video coding. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1945–1954. ACM, 2015.

[6] M. Lease, J. Hullman, J. P. Bigham, M. S. Bernstein, J. Kim, W. Lasecki, S. Bakhshi, T. Mitra, and R. C. Miller. Mechanical turk is not anonymous. *Available at SSRN 2228728*, 2013.

[7] LiveSafe. http://www.livesafemobile.com/press/.

[8] LiveSafe. Privacy policy of the app, Retrieved date: 05/22/2017.

[9] A. Pfitzmann and M. Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. 2010.

[10] B. P. Sadler. When rape victims' rights meet privacy rights: Mandatory hiv testing, striking the fourth amendment balance. *Wash. L. Rev.*, 67:195, 1992.

[11] H. C. Stuart, L. Dabbish, S. Kiesler, P. Kinnaird, and R. Kang. Social transparency in networked information exchange: a theoretical framework. In *Proceedings of the ACM 2012 conference on CSCW*, pages 451–460. ACM, 2012.

[12] E. Tan, H. Xia, C. Ji, R. V. Joshi, and Y. Huang. Designing a mobile crowdsourcing system for campus safety. *iConference 2015 Proceedings*, 2015.