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, there is a dearth of study on privacy issues in crowdsourcing-based reporting systems. In this paper, we reported a case study with LiveSafe which is a popular crowdsourcing-based safety reporting system. We presented our initial interview results on several student victims' privacy concerns and experiences; we also discussed how to protect victim privacy, and the special challenges to achieve it. To the best of our knowledge, our work is pioneering in this research field.

Author Keywords
Victim, Privacy, Crowdsourcing, LiveSafe

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous; See [http://acm.org/about/class/1998/]: for full list of ACM classifiers. This section is required.

Introduction
People who have been crime victims are a vulnerable group. Privacy protection for this group has been discussed in extreme situations, such as rape, under the purview of victims' constitutional privacy rights [1], and the conflicts between

such rights and some constraints, for example, the freedom of the press to disclose victims' identity [2] or mandatory HIV testing under certain conditions [9]. In less severe incidents, however, victims' privacy concerns and protection have not been extensively studied. In addition, prior research suggests that crowdsourcing-based safety reporting systems could alleviate certain privacy concerns, e.g., identity disclosure, [5], but there is still a lack of empirical data from the victims' perspective.

Inclusive privacy and security are important for victims because privacy concerns may deter them from using the reporting application, or 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 be at stake due to deliberate data triangulation (e.g., [6]). As regards LiveSafe, it uses Google Maps, which may be linked to a user's Google account, and it can be signed into with a user's Facebook account, which potentially could be used to de-anonymize a user.

LiveSafe App

LiveSafe is a crowdsourcing-based public safety reporting application that has been adopted and promulgated widely at U.S. universities and communities [4]. The major reporting functions include: (1) "Report Tips," which include 11 types of non-emergency incident types, e.g., alcohol/drug, and each offers choices to add picture, audio, and video files to reports, either anonymously or non-anonymously; and (2) "Emergency Options," which have the options to call 911, call or message the 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 Maps, and "Safe Walk," which allows users' friends to watch them walk, e.g., in remote areas; or let the user to watch a friend walk. LiveSafe's privacy policy acknowledges that the app may collect sensitive information upon the user's consent, such as the contact list, current health status, potential criminal activity, and social or ethnic origin. The app could obtain information from other sources, e.g., Facebook, if the user chooses to sign up with their Facebook account [7]. A screenshot of its main functions can be seen in Figure 1.

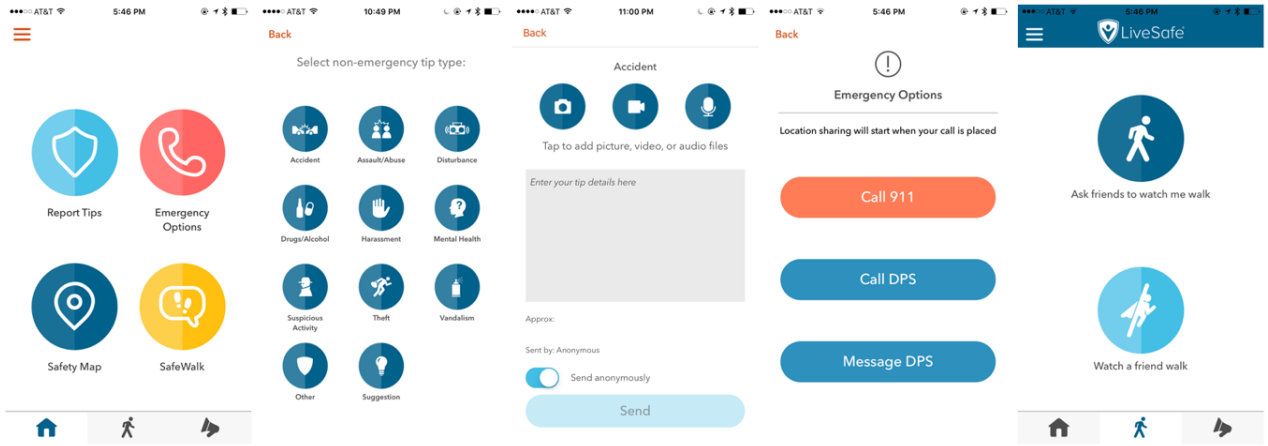
Victim Privacy Concerns

From March 2017 to April 2017, we conducted a round of interviews for this study with 15 participants at our university to probe their perception and usage of LiveSafe. Nine were victims of different crimes and most of the crimes were not severe cases such as rape. Our study has been approved by the IRB department in our university.

Concern about Tracking

One victim had heard her friend's story of being stalked online and offline; after her experience in a harassment incident, she became 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 lives and trajectories, so in the end, she chose not to reveal her incident



(a) Home View (b) Tip Categories (c) Report a Tip (d) Emergency Options (e) SafeWalk

Figure 1: Screenshot of LiveSafe's Main Fuctions

on Facebook or tell it to her friends.

Concern about Officer's Responsibility
Another victim in a burglary was hesitant to disclose his identity until he could ascertain the responding officer is responsible and trustworthy: *"I would like to be anonymous first until the officer who is responsible for this and who wants to talk with me about the further details, and then I will definitely provide my name or any address" (V2, Male, Burglary).*

In this case, the victim preferred anonymity until he could ascertain that the officer was responsible and would reliably deal with the incident. It emphasizes the importance of mutual trust between the victim and the police or DPS officer in charge.

Concern about Individual and Organization's Reputation
Another female victim was in a more severe case involving sexual assault. Using the third person tone, she told us her understanding of anonymity as it relates 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 a bigger organization and it's bigger than the person" (V10, Female, Sexual assault).*

She explained that her concern about remaining anonymous is related to individual embarrassment and shame that may follow an assault. What she meant by "bigger organization" is that some reporting, if done non-anonymously, could tarnish the reputation of an organization that the victim belongs to (in her case, it was the "Greek Life Sorority").

Hence, in her mind, privacy concerns are not merely about an individual's interest, but also associated with an organization's reputation that is "bigger than the person."

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 immediately and getting her [her intoxicated friend] 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, 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" (V10, Female, Sexual assault).*

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

Victim Privacy Protection

We propose several strategies to protect victim's privacy and also discuss some special challenges to achieve it.

Privacy Protection beyond Anonymity
First, data minimization, so long as it is not at the expense of losing essential details for investigation, should be applied. Data minimization means that the possibility of collecting data, the boundaries of collecting behavior, and the retention of the collected data should be minimized [8]. We advocate to apply this principle to protect victim privacy, which indicates that irrelevant private information should not be collected in certain contexts; the victim's comfortableness of disclosure should be respected as the boundary for data collection; and collected information from the victim should have limited retention.

Second, unlinkability should be applied to the extent that a user who is a victim of a crime 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 [8]. To protect victim privacy, we propose that a trade-off should be evaluated between linking and un-linking to a user's different accounts. For example, linking the app to a user's Facebook account could facilitate sign-up process but also increase the probability of de-anonymization and tracking which as our participant V1 said, would be a strong privacy concern.

Adjusting Photo/Video Features to Report
On the technical side, we first propose that system users should be able to adjust photo and video resolution for reporting. For example, there could be a horizontal slider in the photo/video reporting page that enables a user, e.g., a witness, to adjust the resolution of the shooting image. In 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 to protect the victim's privacy; in less sensitive 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, should apply default photo/video resolutions for different incident types. For example, the default resolution for the sexual assault situation could be mosaic, and for an 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, in Google Street View [3]. We propose that similar efforts

should apply to public safety reporting to protect victim's privacy.

Special Challenges to Victim Privacy

As compared to conventional phone-calls, crowdsourcing-based reporting systems could introduce some special challenges for victim privacy protection. For example, LiveSafe can easily broadcast an incident to the multitudes. Users not only can report to the police or DPS, but also can disseminate to their friends. The broadcasting feature is an advantage of crowdsourcing-based reporting systems as compared to phone-calls [10], but such broadcasting could also compromise victim privacy since sensitive information. For instance, in a victimization, photo/video could be taken and disseminated in a few buttons by a crowd of witnesses over which the victim literally has no control. In addition, a special challenge is to balance between revealing sufficient details for investigation and not revealing too many of the victim's personal details, although both sides could be legitimate in benefiting the victim, yet neither–revealing nor withholding information–could achieve a desired outcome if one side overwhelms the other.

Conclusion

In this paper, we discussed victim privacy with a case study of LiveSafe and reported our pilot interviews with several victims about their privacy concerns and experiences. We propose that victim privacy should be better respected and protected, and suggested several strategies to protect it. Also, we discussed some special challenges to protect victim's privacy.

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.

REFERENCES

1. Douglas E Beloof. 2004. Enabling Rape Shield Procedures Under Crime Victims' Constitutional Privacy Rights. *Suffolk UL Rev.* 38 (2004), 291.
2. Deborah W Denno. 1993. The Privacy Rights of Rape Victims in the Media and the Law: Perspectives on Disclosing Rape Victims' Names. (1993).
3. Andrea Frome, German Cheung, Ahmad Abdulkader, Marco Zennaro, Bo Wu, Alessandro Bissacco, Hartwig Adam, Hartmut Neven, and Luc Vincent. Large-scale privacy protection in google street view. In *2009 IEEE 12th International Conference on Computer Vision*. 2373–2380.
4. LiveSafe: http://www.livesafemobile.com/press. 2017. (2017).
5. Yun Huang, Corey White, Huichuan Xia, and Yang Wang. 2017. A computational cognitive modeling approach to understand and design mobile crowdsourcing for campus safety reporting. *International Journal of Human-Computer Studies* 102 (2017), 27–40.
6. Matthew Lease, Jessica Hullman, Jeffrey P Bigham, Michael S Bernstein, Juho Kim, Walter Lasecki, Saeideh Bakhshi, Tanushree Mitra, and Robert C Miller. 2013. Mechanical turk is not anonymous. *Available at SSRN 2228728* (2013).
7. LiveSafe. 2017. Privacy Policy of the App (Retrieved on 05/22/2017). (2017).

8. Andreas Pfitzmann and Marit Hansen. 2010. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. (2010).

9. Bernadette Pratt Sadler. 1992. When Rape Victims' Rights Meet Privacy Rights: Mandatory HIV Testing, Striking the Fourth Amendment Balance. *Wash. L. Rev.* 67 (1992), 195.

10. Elliot Tan, Huichuan Xia, Cheng Ji, Ritu Virendra Joshi, and Yun Huang. 2015. Designing a Mobile Crowdsourcing System for Campus Safety. *iConference 2015 Proceedings* (2015).