



DALHOUSIE UNIVERSITY

Retrieved from DalSpace, the institutional repository of
Dalhousie University

<https://dalspace.library.dal.ca/handle/10222/73885>

Version: Post-print

Publisher's version: Alamiri D., Blustein J. (2016) Privacy Awareness and Design for Live Video Broadcasting Apps. In: Stephanidis C. (eds) HCI International 2016 – Posters' Extended Abstracts. HCI 2016. Communications in Computer and Information Science, vol 617. Springer, Cham

Privacy Awareness and Design for Live Video Broadcasting Apps

Dhuha Alamiri¹(✉) and James Blustein^{1,2}

¹ Faculty of Computer Science, Dalhousie University, Halifax, Canada
dh481896@dal.ca, jamie@cs.dal.ca

² School of Information Management, Dalhousie University, Halifax, Canada

Abstract. We investigate the use and privacy perception of applications that allow broadcast of live video to the WWW; and some that allow the video to remain accessible for up to 24 h. We conducted an online survey based on theories of social capital, motivation, network externalities, and uses and gratification, and a model of online self-disclosure. Based on our survey results, we are designing prototypes to increase users' awareness of privacy and to protect the broadcaster's privacy.

Keywords: Live video broadcasting apps · Live streaming video · Broadcaster · Periscope · Meerkat · Temporal social media · Self-destructing · Privacy awareness · Privacy perception · Self-disclosure · Visual privacy · Location privacy

1 Introduction

Transmitted video is a medium of social interaction. Currently, most consumer video (herein, video content generated by individuals) is either VoIP (video over internet protocol) for point-to-point communication (e.g., Skype, Facetime), or pre-recorded user content permanently posted to Internet sites (e.g., YouTube, Instagram). A newer standard consists of live video that can be broadcast, or “streamed”, (e.g., Livestream). At a consumer level, a number of products are now available that provide similar functionality (e.g., Periscope, YouNow, Meerkat), for individuals.

Live video broadcasting applications (LVBAs) that do not create (store) permanent materials on the Internet are called temporal-content social media. That term is used because the video is never been accessible on the Internet or that the video is automatically deleted after (up to 24 h [1]). Typically, when using such apps, an event is encoded as it happens and is then broadcast directly to the Internet without editing or review. Research on the usage of such apps is lacking. In particular there are concerns about privacy and security aspects that have not been issues previously.

Studies investigating the use of video chat (e.g., Skype, Facetime) found that people use it to communicate with others who they have close relationship with [2–4]. In workplace, people use it for meetings [2]. Because video chat is mainly used for communication with selected individuals, when used properly there are few or no privacy concerns [2, 3]. On the other hand, people share material on YouTube permanently to a wide international audience, so to demonstrate skills and seeking

popularity [5]. However, such videos are “prepared” (can be edited), and therefore, when used properly those who upload videos do not have privacy concerns [6].

Streaming webcams are another form of streaming video, typically focused on a technology demonstrations, tours, presentations, TV, and social events [7]. It is also used for monitoring, and emergency situations to allow authorities to see events as they occur [8]. No privacy concerns are reported about this type of broadcast.

Temporal content social media (e.g., Periscope, Meerkat) have unique issues. In live video, events occur spontaneously, and actions that are not meant to be shared might be shared. Because the videos are not saved, broadcasters may be operating with an illusion of security and privacy. However, live video increases the likelihood of violating the privacy of others who happen to be caught in the video. A broadcaster could intentionally capture copyrighted material [9]. A broadcaster could be a target for malicious people. Employers might also view such broadcasts, which could create issues for employer-employee relations. Finally, because of the licensing agreement, the companies that supply these apps may capture and use the broadcast for their own marketing purposes without the broadcaster’s explicit permission [10]. In addition, privacy-by-design is not considered by many live video broadcasting applications. Periscope, for example, shows the broadcaster’s precise location to the public as a default.

As a first phase of this research, we conducted an online survey of live video broadcasters. The survey addressed the patterns of, and reasons for, use, and their perceptions of the privacy and security issues associated with that use.

2 Methodology

Procedure: We used an online, anonymous, international, English language, 33-item survey (which is ongoing) to assess the propensities and activities of users of temporal social media (YouNow, Meerkat, Periscope or other similar apps). The survey design was based on theories of social capital [11], motivation and network externalities [12], uses and gratification [13], as well as models of online self-disclosure. Some questions of the survey were adopted and/or modified from other surveys. We specifically asked participants about their patterns of use, type of content, the time of, and the mood while broadcasting because these may have implications for privacy and self-disclosure. Some questions focus on privacy, but the survey does ask about breaches of privacy/legality that broadcasters may not have considered (e.g., the broadcasting of images of other non-involved persons, re-transmission of copyrighted material).

Participants were recruited by notices on Twitter, Facebook, Google+ and Instagram using #hashtag for YouNow, Meerkat and Periscope. The study was restricted to those who used these apps only for creating broadcasts.

Participants: Age in years was captured in 4 ranges as 18 to 27 ($N = 17$), 28 to 37 ($N = 8$), 38 to 47 ($N = 2$) and 48 to 57 ($N = 2$). Education was captured in five ordinal categories as less than high school ($N = 4$), high school ($N = 8$), college ($N = 5$), undergraduate ($N = 10$), and graduate or professional ($N = 6$). Self-reported *comfort with technology* was collected using a five-point scale from 1 (“very comfortable”) to 5

(“very uncomfortable”). The mean was 1.65 (SD: 0.95), but the full range was used. Self-reported *knowledge of security* was collected using a three-point scale (0 = “I have no knowledge at all”, 1 = “I have minimal knowledge”, 2 = “Good: I feel secure”. The mean was 1.06 (SD: 0.97; there were two missing values). Participants were generally comfortable with technology and had some knowledge of security.

3 Results and Discussion

The use of YouNow, Meerkat and Periscope or “other apps” was coded on a seven-point scale (0 to 6) from “Never”, through “Less than once a month”, “Once a month”, “Once a week”, “Several times a week”, “Once a day”, to “Several times a day”. The number of participants who used Periscope (17), YouNow (8), Meerkat (9), and other apps (6). The mean rating of frequency for Periscope was 3.09 (SD: 2.27, N = 17), YouNow was 1.05 (SD: 1.62, N = 8), Meerkat was 1.50 (SD: 2.28, N = 9), and for other apps was 4.00 (SD: 2.16, N = 6). Six users cited the use of an alternative app but only three identified those as “Blab” or “Snapchat”. Only 7 of the 33 participants used more than one app: 12 used Periscope exclusively, 6 used YouNow exclusively, 6 used Meerkat exclusively, 2 used some other app exclusively. The use of Periscope was significantly higher than those of YouNow, Meerkat and Other ($\chi^2(3) = 8.8, p < .049$).

Most of the use was to maintain contact with “online friends” (39.4%), “offline friends” (18.2%), or “online strangers” (12.1%). However some use was directed to find “new friends online” (30.2%), or “new followers online” (15.2%). Altruistic endeavors were noted under “advocating for change” (6.1%), “helping people in need” (18.2%), and “advising young people” (12.1%). Finally, business endeavors were noted under promoting “my professional profile” (15.2%), “my business or activities” (12.1%), or “my events” (6.1%). About half the users (45.5%) cited more than one reason. Three participants simply stated “none”, “to waste my free time” and “entertainment”.

Table 1. Types of broadcasts created by users

Type of BCs	Any of (33)		Private		Public	Planned	
	N	%	Single	Multiple		Yes	No
Formal of self	22	66.7	9.1	22.7	40.9	50.0	40.9
Informal of self	25	75.8	16.0	40.0	32.0	20.0	72.0
Formal of others	20	60.6	20.0	15.0	5.0	50.0	40.0
Informal of others	21	63.6	14.3	33.3	9.5	33.3	52.4
Non-human	19	57.6	5.3	15.8	57.9	15.8	68.4

Participants were asked about the nature of their broadcasts (BC) within five categories (see Table 1), and within three levels of audience type (private single, private multiple and public). The *nonhuman* category explicitly referred to videos that did not contain humans. Values for private, public and planned are expressed as the proportion

of individuals within each BC type (i.e., 50.0% of the 22 users who created Formal BCs of Self did so as planned BCs). Table 1 also includes the information about whether the BC was planned or spontaneous (unplanned).

Most participants (69.7%) engaged in a mix of BC types: In fact, 45.5% engaged in all five types (2 participants did not supply a breakdown). Of that, 9.1% engaged in formal BC exclusively, 15.2% engaged in informal BCs exclusively, 21.2% engaged in BCs of self exclusively 6.1% engaged in BCs of others exclusively, and 3.0% engaged in BC of non-human topics exclusively.

Table 2 provides the location of the broadcast. All values are expressed as the proportion of individuals within each BC type. Only five participants created BCs from only one location.

Table 2. Place of broadcast by type of BC

Type of BCs	Work	Home	Public	Parties	Driving
Formal of self	45.5	63.6	40.9	22.7	18.2
Informal of self	24.0	72.0	40.0	28.0	16.0
Formal of others	30.0	35.0	60.0	15.0	15.0
Informal of others	28.6	38.1	42.9	33.3	14.3
Non-human	26.3	47.4	42.1	21.1	21.1

Table 3 provides the mood while broadcasting, again as proportions. The category stims refers to broadcasting while under the influence of stimulants (e.g., alcohol).

Table 3. Mood of broadcasts by type of BC

Type of BCs	Happy	Sad	Angry	Worried	Compelled	Stims
Formal BCs of self	59.1	4.5	4.5	36.4	13.6	4.5
Informal BCs of self	88.0	16.0	20.0	16.0	20.0	0.0
Formal BCs of others	60.0	0.0	5.0	20.0	10.0	10.0
Informal BCs of others	76.2	0.0	14.3	9.5	19.0	4.8
Other BCs	57.9	15.8	15.8	31.6	36.8	10.5

Most BCs are created while happy, but a substantial percent are created when worried, angry or sad, particularly of self, which is a concern. At such times, the broadcaster might not be as careful about privacy or security.

Participants did express concerns in several areas using a four-point scale (1 = “Very Concerned”, 2 = “Concerned”, 3 = “Not at all Concerned” and 4 = “Never thought about it”). The mean rating of concern for social reputation was 2.07 (SD: 0.94), physical harm was 1.85 (SD: 0.79), economic harm (e.g., ID theft) was 1.81 (SD: 0.80), intellectual property theft was 2.19 (SD: 0.85), unauthorized use of screen shots was 2.07 (SD: 1.01), for the lack of control over who views the material was 2.13 (SD: 0.78), for the lack of control over who views the users location was 1.83 (SD: 0.83), for lawsuits was 2.19 (SD: 0.75), and for potential monitoring by employer was 2.40 (SD: 0.76). Generally, participants were more concerned about legal issues (intellectual

property, lawsuits) than about personal harm. “Never thought about it” reaches 37.3%, which implies that many are not thinking about security or privacy.

Using a checklist, participants endorsed several advantages to the ephemeral nature of the videos. It maintains the secrecy of the broadcast (36.4%), and reduces the potential for profiling (41.5%). It also protects the privacy (50.65%), anonymity (24.2%), intellectual property of the broadcaster (24.2%) and others (39.2%), limits unwanted viewers (46.6%), and the ability of companies to learn about the broadcaster (29.1%). Users consider the temporary nature of the video as a protection. It was also considered a drawback because the content could be valuable (50.2%) and would require time to recreate (41.5%). It also limited the ability to identify viewers (47.9%), the chances to view videos (45.2%), the potential for popularity (41.5%), and potential exposure of the broadcaster (33.1%). Note that the endorsement of negatives was higher than that of positives ($p < .001$). The ephemeral nature of the temporal content social media may not last long. In that regard, 72.7% of participants wanted additional feedback about who viewed their locations. Participants indicated their desire to be able to hide face (18.2%), voice (6.1%), exact (54.5%) and approximate location (21.2%), surroundings (9.1%), other people (12.1%), their inappropriate behavior (45.5%) and of others (15.2%). Thus, there is a desire for more control.

4 Conclusion and Future Work

Users of existing video-based social media (e.g., video chat applications, webcam broadcasts, YouTube) have not reported high levels of privacy or security concerns. However, the emerging standard of temporal content video streaming creates additional concerns that broadcasters may not be aware of. Most broadcasters cited numerous concerns for privacy and security, and some wanted specific features to be incorporated into these apps. It would seem that the app developers will need to take responsibility for the inclusion of privacy features.

All significant data that gathered from the online survey will be used to propose context sensitive features to increase privacy awareness and control when deemed necessary. The final goal is to protect the privacy of live video broadcasters. We will apply our proposal designs on Periscope due to showing the broadcasters’ location, which makes Periscope more critical. We will provide real-time feedback about the viewers who check the location. In addition, we will provide designs for default visual privacy techniques to protect the privacy of broadcasters who are in atypical mood.

References

1. O’Reilly, T.: What is web 2.0: design patterns and business models for the next generation of software. *Commun. Strat.* **1**, 17 (2007)
2. Massimi, M., Neustaedter, C.: Moving from talking heads to newlyweds: exploring video chat use during major life events. In: *Proceedings of the 2014 Conference on Designing Interactive Systems*, pp. 43–52. ACM, June 2014

3. Judge, T.K., Neustaedter, C.: Sharing conversation and sharing life: video conferencing in the home. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 655–658. ACM, April 2010
4. Wang, J., Mughal, M. A., Juhlin, O.: Experiencing liveness of a cherished place in the home. In: Proceedings of the ACM International Conference on Interactive Experiences for TV and Online Video, pp. 3–12. ACM (2015)
5. Courtois, C., Mechant, P., Ostyn, V., De Marez, L.: Uploaders' definition of the networked public on YouTube and their feedback preferences: a multi-method approach. *Behav. Inf. Technol.* **32**(6), 612–624 (2013)
6. Misoch, S.: Stranger on the internet: online self-disclosure and the role of visual anonymity. *Comput. Hum. Behav.* **48**, 535–541 (2015)
7. Juhlin, O., Engström, A., Reponen, E.: Mobile broadcasting: the whats and hows of live video as a social medium. In: Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services, pp. 35–44. ACM, September 2010
8. Landgren, J., Bergstrand, F.: Mobile live video in emergency response: its use and consequences. *Bull. Am. Soc. Inf. Sci. Technol* **36**(5), 27–29 (2010)
9. Vaidya, J.: Sports Broadcast Rights Holders Slowly Adapting to Live-Streaming Apps Such as Periscope [Web log post], 27 July 2015. <https://sportsjournalismuk.wordpress.com/2015/07/27/sports-broadcast-rights-holders-slowly-adapting-to-live-streaming-apps-such-as-periscope/>
10. Pearson, J.: Periscope Could Have a Privacy Problem, 26 March 2015. <http://motherboard.vice.com/read/periscope-could-have-a-privacy-problem>
11. Pfeil, U., Arjan, R., Zaphiris, P.: Age differences in online social networking—a study of user profiles and the social capital divide among teenagers and older users in MySpace. *Comput. Hum. Behav.* **25**(3), 643–654 (2009)
12. Lin, K.Y., Lu, H.P.: Why people use social networking sites: an empirical study integrating network externalities and motivation theory. *Comput. Hum. Behav.* **27**(3), 1152–1161 (2011)
13. Stanley, B.: Uses and gratifications of temporary social media: a comparison of Snapchat and Facebook. Doctoral dissertation, Cal State University, Fullerton (2015)