Sex, Lies, or Kittens? Investigating the Use of Snapchat's Self-Destructing Messages

Franziska Roesner[1], Brian T. Gill[2], and Tadayoshi Kohno[1]

[1] University of Washington, Computer Science & Engineering
[2] Seattle Pacific University, Mathematics

Abstract. The privacy-related Snapchat smartphone application allows users to share time-limited photos or videos, which "disappear" after a specified number of seconds once opened. This paper describes the results of a user survey designed to help us understand how and why people use the Snapchat application. We surveyed 127 adult Snapchat users, finding that security is not a major concern for the majority of these respondents. We learn that most do not use Snapchat to send sensitive content (although up to 25% may do so experimentally), that taking screenshots is not generally a violation of the sender's trust but instead common and expected, that most respondents understand that messages can be recovered, and that security and privacy concerns are overshadowed by other influences on how and why respondents choose to use or not use Snapchat. Nevertheless, we find that a non-negligible fraction (though not a majority) of respondents have adapted or would adapt their behavior in response to understanding Snapchat's (lack of) security properties, suggesting that there remains an opportunity for a more secure messaging application. We reflect on the implications of our findings for Snapchat and on the design of secure messaging applications.

1 Introduction

The privacy-related Snapchat smartphone application[1] allows users to share time-limited photos or videos with friends. Users take photos or videos using the application and specify the number of seconds (up to ten) for which the recipient is allowed to view the content. After this time, the content "disappears" — i.e., it is no longer accessible via the Snapchat user interface, but it is not actually securely deleted from the device. Snapchat's popularity has increased dramatically in recent months, with over 8 million adult users [31], 350 million "snaps" sent every day [17], and a possible valuation of up to $3.5 billion [6].

We surveyed 127 adult Snapchat users, finding that security is not a major concern for the majority of them, despite our sample being slightly skewed towards users with higher self-reported security expertise. We find that most respondents do not use Snapchat primarily for sensitive content (although up to 25% may do so experimentally), that screenshots are common and expected, and that most respondents understand that messages can be recovered. However, a non-negligible fraction (though not a majority) of respondents has adapted or would adapt their behavior in response to weakened trust in Snapchat, suggesting that there remains an opportunity for a more secure messaging application.

[1] `http://www.snapchat.com`

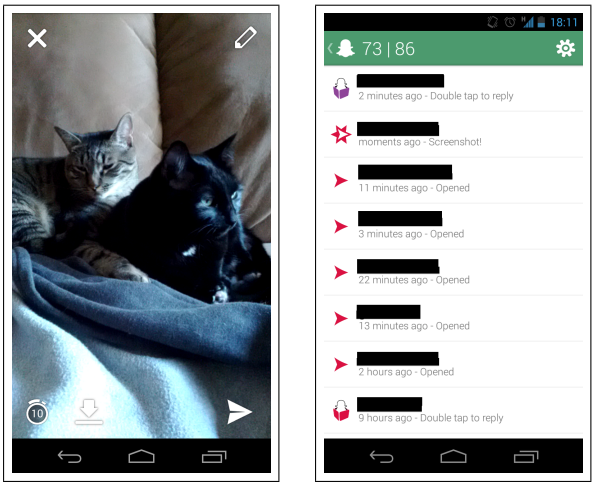

Fig. 1. Snapchat screenshots. *On the left, Snapchat runs on an Android phone. The timer indicates the number of seconds that this image will be viewable by recipients. Users can add caption text or draw arbitrarily on top of the picture. On the right, Snapchat's log shows sent and received "snaps" (usernames hidden for anonymity), e.g., indicating that the recipient of the second message in the list took a screenshot.*

2 Background and Motivation

We first provide background on Snapchat, an application that allows users to send photos and videos that "disappear" after a specified number of seconds. Figure 1 shows a screenshot of the Snapchat application running on Android.

Snapchat usage. Snapchat's primary feature is that each message "disappears" once the recipient has opened it and the sender-specified timeout (of up to ten seconds) has elapsed. The ephemeral nature of Snapchat messages naturally evokes the idea of its use for privacy-sensitive content — indeed, much media buzz has been made about Snapchat's potential use for sexual content ("sexting") [21]. In practice, however, it appears that Snapchat is used for a variety of creative purposes that are not necessarily privacy-related. For example, many people make use of the application's support for easily drawing on photos [24], and others (including Snapchat itself) argue that disappearing messages also reduce inhibitions for sending non-sensitive, in-the-moment content, challenging the "never forgets" nature of the Internet and other social media services [14, 16]. These and similar anecdotes led us to ask: *How and for what do people really use Snapchat? What are common, uncommon, or surprising usage patterns?*

Saving and retrieving snaps. Importantly, the way in which Snapchat implements message destruction is not secure. In practice, there are many ways to save or retrieve "snaps" on a user's device after their timeout has elapsed. In one class of data exfiltration, recipients can take screenshots of messages as they view them, using the operating system's application-agnostic screenshot capabilities (e.g., holding the volume down and power buttons on a Samsung Galaxy Nexus device). The Snapchat application can (generally) detect these

kinds of screenshots, in which case it notifies the sender (e.g., the second message in the list in Figure 1). However, this notification is not always reliable, as users have discovered ways to take screenshots without alerting the Snapchat application (e.g., [10]). In light of these capabilities, websites have emerged that encourage people to post screenshots of embarrassing or sensitive "snaps" (e.g., SnapchatLeaked [1]). In our study, we attempt to answer the following questions: *What are users' screenshot practices? To what extent are screenshots a common and expected use of the application, rather than a violation of the sender's trust?*

Another class of attacks exploits the fact that Snapchat doesn't actually delete from the device messages that have passed their timeout. Instead, it simply renames the files and makes them inaccessible via its user interface. As a result, people with moderate technical expertise can retrieve these files from a device even for destroyed messages (e.g., [8, 9]). Snapchat itself does not claim perfect security, warning that deleted data can sometimes be retrieved [26]. Thus, we ask: *Do users have a realistic mental model with respect to Snapchat's security? Do they trust Snapchat? Does this mental model affect their use of the application?*

3 User Survey

To explore the above questions, we designed a survey that was taken by 127 adult Snapchat users. We estimate that the survey, which consisted of at most 41 optional questions per respondent, took 15-30 minutes to complete. We surveyed only adults (18 years or older), who we recruited primarily by sharing the survey link via our own and our contacts' social media pages and via university email lists. As a result, our sample is slightly skewed towards respondents with higher self-reported security expertise — however, reported security expertise did not significantly affect most responses. Furthermore, while reports suggest that Snapchat is also popular among 13-18 year olds [29], sexting-style behavior is not necessarily more common among younger users [28]. This study was reviewed and found exempt by our institution's human subjects ethics review board.

Of 206 initial recruits, 18 (8.7%) responded that they do not know what Snapchat is and were screened out. Of the remaining 188 respondents, 61 (32.4%) responded that they had never used Snapchat. We report the remainder of our results considering only the 127 self-reported Snapchat users. Unless otherwise noted, questions were multiple choice; free responses and multiple-choice "other" responses were coded independently by two of the authors.

Demographics. 68.5% of Snapchat-using respondents were male and 29.9% female (two did not specify). Although our population is skewed towards male respondents, we find almost no statistically significant gender differences. Most respondents (81.9%) were between the ages of 18-24; 14.2% were between the ages of 25-34, 1.6% between 35-44, 0% between 45-54, and 1.6% between 55-64.

When asked to describe their level of familiarity with computer security on a scale of 1 (novice) to 5 (expert), 12.6% considered themselves an expert and only 4.7% a novice, with a plurality (31.5%) selecting option 4 on the scale. (Note that ten respondents were not asked about security expertise because we added the question to the survey after they had already completed it. All other questions

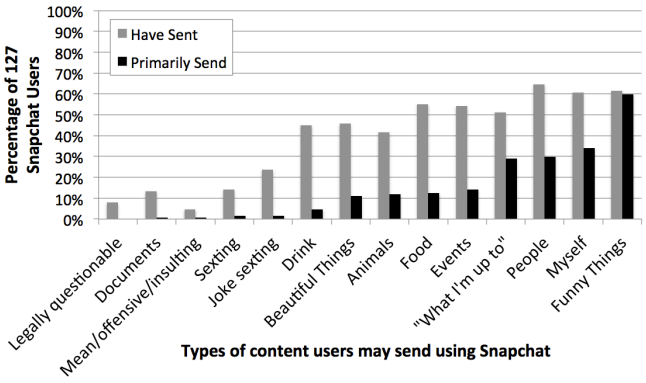

Fig. 2. Do respondents send sensitive content? *For each type of content we asked about, respondents indicated whether they primarily send it and/or have sent it. They report sending sensitive content (sexual, legally questionable, mean/offensive/insulting content, and documents) uniformly less than non-sensitive content.*

were unmodified.) We also asked respondents to rate their agreement with three privacy-related prompts, allowing us to classify them according to the Westin Privacy Index [18] as *Privacy Fundamentalists*, *Privacy Pragmatists*, or *Privacy Unconcerned*. We found that 39.4% of respondents are Privacy Fundamentalists, 45.7% are Privacy Pragmatists, and 12.6% are Privacy Unconcerned.

3.1 Common Usage Patterns

We first explore whether our respondents use Snapchat to send sensitive (such as sexual) content, and then consider whether respondents' message timeout behaviors and reported reasons for using Snapchat suggest privacy considerations.

Do respondents send sensitive content? We asked respondents about whether they *primarily send* and/or *have sent* certain types of sensitive content using Snapchat, including sexual, legally questionable, mean/offensive/insulting content, and documents. We provided additional non-sensitive options to avoid priming respondents; Figure 2 shows the response options and responses.

We find that only 1.6% of respondents report using Snapchat *primarily* for "sexting" — although 14.2% admit to *having sent* sexual content via Snapchat at some point. (More, 23.6%, admit to having sent content classified as "joke sexting," in which sexual or pseudo-sexual content is sent as a joke.) Though some do appear to use Snapchat for sensitive content, respondents in aggregate report sending sensitive content types uniformly less than non-sensitive content (Figure 2). However, we may consider self-photographs to be borderline sensitive: while most content types show no significant differences between Westin Privacy types, Privacy Unconcerned respondents are slightly more likely to say that they primarily send "photos/videos of myself" (62.5%) than Pragmatists (31%) or Fundamentalists (28%) (Fisher's exact test, 2 d.f., $p = 0.042$).

While we recognize that respondents may have underreported how often they send sensitive content (as we discuss further in Section 4), our findings suggest that they do seem to find Snapchat useful for non-sensitive content. In a free re-

sponse question about additional Snapchat experiences, several respondents emphasized using Snapchat for fun, sending messages with silly or mundane content that they might not otherwise send via a messaging platform that emphasizes archival rather than temporariness. For example, one respondent mentioned that Snapchat "lets me have more cats in my life because my friends who don't normally post pictures of their cats on other social media will snapchat their cats to me." Others mention that they use it to send photos of "stupid faces" and another wishes for an option to "add moustaches to those faces." Indeed, of the content options presented in our survey, respondents most commonly chose funny content as their primary use for Snapchat (59.8%).

Does message timeout behavior reflect privacy considerations? A possible explanation for Snapchat's recent success is its implied security and privacy properties. To evaluate this claim, we consider whether our respondents' use of message timeouts or their choice of Snapchat suggest privacy considerations.

First, we asked respondents multiple choice questions about the message timeout that they set (up to ten seconds). About half (52.8%) use a fixed or arbitrary timeout length, regardless of content type or recipient. The remaining 47.2% report adjusting the timeout depending on content and/or recipient. When asked about the reason,[2] many of these respondents report setting shorter timeouts for embarrassing photos (22.8% of 127) or for secret information (10%). Many also report setting longer timeouts for people they trust more (18.9%) or shorter timeouts for people they trust less (10%).

A possible explanation for shorter timeouts is an attempt to control screenshots by recipients. Two respondents explained in "other" responses that they set shorter timeouts if a screenshot should be avoided and longer timeouts if one is desired (particularly for photos of cats, according to one respondent). Another mentioned "a tacit agreement that if the timeout is 10sec, then a screenshot is almost expected." However, not all timeout manipulation is for privacy reasons: 12 respondents (9.4%) explained in "other" responses that they set a longer timeout if the message takes more time to comprehend (e.g., includes a lot of text), and more may have selected this answer choice had we included it explicitly.

These results suggest that up to a quarter of respondents do adjust timeouts with privacy in mind (e.g., in an attempt to avoid screenshots). However, most do not explicitly manage timeouts. We observed no significant associations between Privacy Index or reported security expertise and timeout behavior.

Do respondents use Snapchat for security/privacy reasons? We asked respondents why, when they use Snapchat, they choose it over other services such as email, text messaging, Facebook, or Twitter. We included two security-related options, as well as additional options to avoid priming respondents. While a non-negligible (though not majority) of respondents prefers Snapchat because content is unlikely to or can't (according to the respondent's belief) be saved

[2] Respondents could select multiple answers: I set shorter timeouts for embarrassing photos; I set shorter timeouts for content containing secret information; I set longer timeouts for people I trust more. I set shorter timeouts for people I trust less; Other.

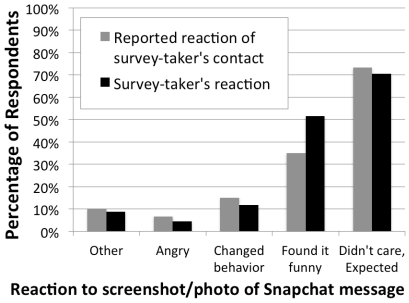

Fig. 3. Do screenshots violate trust? *Only a minority of respondents reports that the victim changed his or her behavior or was angry after learning of a screenshot or photo. Respondents more commonly selected neutral ("didn't care") or positive ("thought it was funny") answer choices. Note that respondents could select multiple response options.*

(46.5% chose one or both of these answer choices), not all of these respondents appear to like message disappearance for security or privacy reasons. Instead, some explicitly report liking it because it becomes socially acceptable to send more casual, in-the-moment content and/or to "spam" friends: 6 respondents (4.7%) who selected the "other" response wrote in sentiments like: "expectation of spam means it's ok to spam," "some content, whether or not it's risque, does not need to be seen more than once (e.g., photos of food)," or "Snapchat allows for less serious communication." Respondents more frequently selected answer choices unrelated to security or privacy, most commonly that Snapchat is easy and simple (66.1%) and/or more fun to use (55.9%).

3.2 Screenshot Practices

One might argue that screenshots circumvent Snapchat's intended usage model and violate the sender's trust, thus expecting that screenshots are taken rarely.

How often do respondents take screenshots? Contrary to expectation, we find that it is common for respondents to take screenshots of Snapchat messages: 47.2% admit to taking screenshots and 52.8% report that others have taken screenshots of their messages. We also found that a small numbers of respondents have used a separate camera to take a photo of a Snapchat message (5 respondents, or 3.9%) or report that someone has used a separate camera to take a photo of their message (3 respondents). While most respondents didn't select reasons for taking screenshots that indicated the explicit intent to violate trust, 10.2% admit that they have done so to embarrass the sender.

How do respondents and their contacts react to screenshots? If message senders feel that their trust is violated by a screenshot, they may react with anger or by changing their behavior: by sending messages with shorter timeouts or different content, by no longer sending messages to that recipient, and/or by taking a screenshot in retaliation. Using these alongside options indicating neutral (e.g., "didn't care") and positive (e.g., "thought it was funny") sentiments, we asked respondents both about their own reactions to screenshots of their messages as well as about the reactions of people of whose messages they took screenshots. Figure 3 summarizes these responses.

Only 11.8% of respondents reported reacting by changing their own behavior; only 15.0% reported that their contact changed his or her behavior. Even fewer respondents reported themselves or their contacts reacting with anger (4.4% and

6.7%, respectively). Respondents more commonly chose answer choices indicating neutral ("didn't care") or positive ("thought it was funny") reactions.

Thus, screenshots seem to be an ordinary and expected component of Snapchat use among our respondents. Recall also from Section 3.1 the anecdote that longer timeouts implicitly permit the recipient to take a screenshot. Interestingly, Privacy Unconcerned respondents were more likely to report having taken a screenshot (64.7%) than Pragmatists (33.7%) or Fundamentalists (22.0%) (Fisher's exact test, 2 d.f., $p = 0.0026$). This finding suggests that privacy-sensitive respondents, who may be more likely to view a screenshot as a trust violation, are less likely to take a screenshot themselves.

3.3 Effects of Security Weaknesses

Since Snapchat is marketed as a secure messaging application, one might expect discoveries about its insecurity to threaten its popularity. We directly asked respondents about their views of Snapchat's security, and we infer additional security-related views from their reported behaviors.

Do respondents know Snapchat message destruction is insecure? We asked respondents whether they believe that someone with technical expertise can recover expired Snapchat messages on a device. (As discussed in Section 2, the correct answer to this question is "yes" [8, 9].) We find that a majority of respondents (79.4%) says that they know or think that recovering "snaps" is possible. Only a minority of respondents thinks or "knows" that expired messages cannot be recovered (14.1%); the rest (5.5%) responded that they don't know.

Our sample is skewed towards respondents with security expertise, who may have more realistic security mental models than the average Snapchat user. Indeed, knowing the message destruction is insecure was associated with higher levels of security expertise (Wilcoxon rank sum test, $p = 0.014$). Respondents may also have been made suspicious by the availability of certain answer choices. Nevertheless, we were surprised at the large majority of respondents who reported knowing or suspecting that Snapchat's message destruction is insecure.

Do respondents report security-related behavior changes? We asked respondents about whether and how they would change their Snapchat use in response to learning that message destruction is insecure. We find that a small majority (52.8%) reports that experts finding a way to recover expired messages would not affect their use of the application at all. However, a non-negligible (38.6%) report that they would change or have changed their behavior (by using Snapchat less, sending different content, and/or sending messages to different people) in response to learning that message destruction is not secure. A majority of these behavior-changing respondents do not report that they would use Snapchat less (14.2% of 127), suggesting that Snapchat's lack of security may not dramatically reduce its user base. Nevertheless, since they would use it differently (24.4% of 127), our results suggest that there remains an opportunity for a more secure ephemeral messaging application, as we discuss in Section 4.

Does lack of trust in Snapchat affect content respondents send? Above, we described how respondents said they would change their behavior upon learn-

ing that Snapchat messages can be recovered. Because the majority already knew or suspected that message destruction is insecure, these responses don't yet give us a clear idea of how respondents' behavior is affected by their (lack of) trust in Snapchat. We thus also examine what types of content respondents report not sending via Snapchat and why.[3] Overwhelmingly, respondents are willing to send most types of content via Snapchat, with the following exceptions:

- 74.8% of respondents are not willing to send content classified as "sexting" or "joke sexting." The primary reported reason is that these respondents "never take pictures of that kind of thing" (47.2%), followed by fear of screenshots (25.2%) and distrust of Snapchat (14.2%).
- 85.0% of respondents are not willing to send photos of documents via Snapchat, primarily because they "never take pictures of that sort of thing" (30.7%). Many would "rather send it another way" (e.g., email, text message, Facebook, Twitter) (26.8%), in part because they don't want documents to disappear (18.1%). Only 11.8% wouldn't trust Snapchat with documents.
- 86.6% of respondents are not willing to send messages containing legally questionable content, again primarily because they "never take pictures of that kind of thing" (66.9%). Concerns about screenshots and Snapchat's trustworthiness were also present in this case (12.6% and 8.7% respectively), possibly because of the risk of legal ramifications. Indeed, three of 16 free responses explaining additional reasons for not using Snapchat for certain content were related to legality issues and/or concerns that Snapchat may allow government access to user data, the latter now known to be true [25].
- 93.7% of respondents are not willing to send content considered mean, offensive, or insulting, reporting primarily that they "never take pictures of that kind of thing" (73.2%), followed by "I don't want to bother people" (15.7%).

Thus, although most respondents don't use Snapchat for certain types of content primarily because they don't produce such content, the remaining respondents commonly selected fear of screenshots or lack of trust in Snapchat as reasons for avoiding it. Considering sexual, legally questionable, offensive content and/or documents as "more sensitive," we find that respondents were more likely to be concerned about screenshots or about trusting Snapchat for these than for less sensitive types of content. Only 3.1% of respondents indicated concern about screenshots for non-sensitive content compared to 33.1% for potentially sensitive content (McNemar's test, $p < 0.001$), and only 1.6% don't send non-sensitive content because they don't trust Snapchat, compared to 26.0% for potentially sensitive content (McNemar's test, $p < 0.001$).

More generally, we find a significant difference among the Privacy Index groups (Kruskal-Wallis rank sum test, $\chi^2 = 9.88$, 2 d.f., $p = 0.0072$) in how

[3] For each type of content in Figure 2 that a respondent would not be willing to send via Snapchat, he/she could select multiple reasons for why not: I'm afraid someone will take a screenshot or photo; I don't trust the Snapchat application; I never take pictures of that kind of thing; I don't want to bother people; I don't want it to disappear; I want to share it more publicly; I'd rather send it another way (such as using email, text message, Facebook, Twitter).

frequently they use Snapchat at all: Privacy Unconcerned report using it more frequently than both Pragmatists ($p = 0.021$) and Fundamentalists ($p = 0.002$). That is, privacy-sensitive respondents tend to use Snapchat less frequently.

4 Discussion

We reflect on the implications of our findings, including perspectives from respondents given with "other" responses to multiple choice questions or in a free-response question asking about additional thoughts regarding Snapchat.

Implications for Snapchat. Some potential Snapchat users may assume that the application is intended or commonly used for "sexting" or other sensitive content. For example, before ending the survey for 61 respondents who reported not using Snapchat, we asked them about why they have chosen not to use it. While mostly simply expressed lack of interest, several voiced concerns related to sensitive content, including that Snapchat "has a bad reputation (for sexting)," that it "seems useful for only inappropriate content," and that "there are additional connotations that go along with this particular app." By contrast, we find that although some of our 127 Snapchat-using respondents do use Snapchat for sensitive content, they don't report using it primarily for this purpose, and they commonly report finding it useful for non-sensitive content (e.g., funny content).

Our findings are also in contrast with media coverage of every new Snapchat vulnerability (e.g., [8–10]), which often implies that Snapchat's success depends on it being actually secure. Instead, our survey results suggest that Snapchat's success is not due to its security properties but because users find Snapchat to be fun. Because they don't often send sensitive content, respondents may not need messages to disappear *securely*, but the mere disappearance of messages from the user interface seems to appeal to some. Some report feeling comfortable sending casual content more frequently via Snapchat because "it doesn't feel like spam" and "it makes it easy not to think about the storage of old messages."

Thus, Snapchat may be better served by advertising itself without implied security properties, focusing rather on the "fun" factor and the change in social media norms introduced by ephemeral content. There is evidence that Snapchat has already begun to embrace this shift in its role: for example, after the launch of our survey, Snapchat introduced "stories" that live for 24 hours [27]. The company has also explicitly backed away from security promises [26].

Implications for secure messaging applications. Most respondents appear to understand Snapchat's weaknesses and most report they have not or would not change their behavior in response. However, recall that about 40% report that they would change or have changed their behavior in response to this knowledge, and that security-sensitive respondents reported using Snapchat less frequently.

Indeed, a non-trivial fraction of respondents reports that they don't send sensitive content in part because they don't trust Snapchat or they are worried about screenshots. Respondents may also have underreported sending sensitive content or already incorporated their knowledge of Snapchat's weaknesses into their reported behaviors. Some emphasized using Snapchat for fun while remaining aware of its lack of absolute security. For example, one respondent said, "I

use Snapchat knowing that it's a limited tool (screencaptures at the OS-level are easy), so I use it knowing that the impermanence is artificial (meaning that I have to trust my friends to play along)." Another expressed hesitation: "I like the idea of Snapchat, but it definitely worries me that the photos are 'out there' somewhere, even if the snaps I'm sending don't have sensitive content."

Combined, the above two paragraphs suggest that while Snapchat is useful and fun for a large set of users for non-sensitive content, a more secure messaging platform would still be a valuable addition to the set of communication tools for many users. In particular, these users would likely value the following properties in a more secure messaging system: (1) privacy on the server-side (i.e., from company employees), (2) privacy in transit, (3) more secure message destruction on the device and in the cloud, and (4) a higher bar for message recipients to save messages, e.g., by completely preventing screenshots. In practice, many of these features may be challenging or impossible to achieve — for example, message recipients can always use another device to take photos even if screenshots are prohibited (i.e., the "analog hole"). Nevertheless, an application that adequately addresses even a subset of these issues would significantly raise the bar over Snapchat and may attract some of these more privacy-sensitive users.

Study limitations. We highlight several limitations that prevent us from generalizing our results to the entire population of Snapchat users. First, our survey did not reach a random sample of users but rather propagated through our own social and university networks (snowball sampling). Additionally, we only surveyed respondents at least 18 years of age, though reports suggest that Snapchat is also popular among younger users [29]. Finally, we asked about respondents' behaviors rather than observing them directly, allowing respondents to underreport potentially sensitive behaviors or beliefs, and we used primarily multiple choice questions that limit our ability to explore respondents' behaviors and mental models more generally. Future studies are thus needed to better understand Snapchat use in the wild among a more general population.

5 Related Work

Finally, we briefly summarize related work. In the research community, there have been a number of efforts toward creating self-destructing data, including early work by Perlman [22] and more recent work on Vanish [11, 12], as well as work on attacking specific implementations of Vanish with Sybil attacks [33]. An analysis of different approaches for secure data deletion appears in [23]. There have also been significant efforts toward ephemeral two-way communications, such as the off-the-record messaging system [4, 13].

Commercial examples of messaging applications that reportedly support message destruction include TigerText [30], Wickr [32], and Facebook's Poke [2], which emerged as a potential competitor to Snapchat and reportedly encrypts messages and deletes the encryption key after two days [7]. Another Snapchat-inspired idea is BlinkLink [3], a link that disappears after some number of views.

Other researchers have studied users' interactions with social media from a security and privacy perspective. For example, studies have shown that users

struggle to understand and apply Facebook privacy settings (e.g., [15, 19]) and that privacy violations on Twitter are a growing problem [20]. Others have considered the privacy strategies of users on social networks more generally [5].

6 Conclusion

We surveyed 127 adult users of the privacy-related Snapchat smartphone application, which allows users to send messages that "disappear" after a timeout. We found that security and privacy are not major concerns for the majority of respondents. Respondents more commonly respond that they use Snapchat because it is fun, not because of its implied or actual security properties. Indeed, most respondents understand that Snapchat's message destruction is insecure, but they do not send sensitive messages (such as sexual or legally questionable content) more commonly because they don't produce such content than because they don't trust Snapchat or their friends. We find that screenshots are common and that respondents appear not to consider them a trust violation. Nevertheless, we observe that a non-negligible fraction (but not a majority) of respondents adapt their behavior in response to Snapchat's weak security properties, and thus conclude that these users may still have a use for a more secure messaging application in addition to the more casual, fun-focused Snapchat.

Acknowledgements. We thank our shepherd, Serge Egelman, and the anonymous reviewers for their valuable feedback. We thank our survey respondents for their participation, Tamara Denning for feedback on the survey, and Greg Akselrod for feedback on an earlier draft. The cats Tony and Fidget posed for Figure 1. This work is supported in part by the National Science Foundation (Grant CNS-0846065 and a Graduate Research Fellowship, Grant DGE-0718124) and by a Microsoft Research PhD Fellowship.

References

1. Snapchat Leaked, http://snapchatleaked.com/
2. Aguilar, M.: Poke: Facebook just cloned Snapchat (Dec 2012), http://gizmodo.com/5970590/
3. Allsopp, C.: BlinkLink Post-Mortem (Aug 2013), http://clayallsopp.com/posts/blinklink/
4. Borisov, N., Goldberg, I., Brewer, E.: Off-the-record communication, or, why not to use PGP. In: ACM Workshop on Privacy in the Electronic Society (2004)
5. boyd, d., Marwick, A.E.: Social privacy in networked publics: Teens attitudes, practices, and strategies. In: Oxford Internet Institute Decade in Internet Time Symposium (2011)
6. Colao, J.: Is Snapchat Raising Another Round At A $3.5 Billion Valuation? (Oct 2013), http://www.forbes.com/sites/jjcolao/2013/10/25/is-snapchat-raising-another-round-at-a-3-5-billion-valuation/
7. Constine, J.: Your Facebook pokes are stored for two days, then their encryption keys are deleted (Dec 2012), http://techcrunch.com/2012/12/22/your-facebook-pokes-are-stored-for-two-days
8. Ducklin, P.: Snapchat images that have "disappeared forever" stay right on your phone... (May 2013), http://nakedsecurity.sophos.com/2013/05/10/snapchat
9. Dunn, G.: Yet another way to retrieve deleted Snapchat photos (Jun 2013), http://www.salon.com/2013/06/04/yet_another_way_to_retrieve_deleted_snapchat_photos_partner/

10. Empson, R.: Not-So-Ephemeral Messaging: New SnapChat "Hack" Lets Users Save Photos Forever (Jan 2013), http://techcrunch.com/2013/01/22/not-so-eph
11. Geambasu, R., Kohno, T., Krishnamurthy, A., Levy, A., Levy, H.M., Gardner, P., Moscaritolo, V.: New directions for self-destructing data. Tech. Rep. UW-CSE-11-08-01, University of Washington (2011)
12. Geambasu, R., Kohno, T., Levy, A., Levy, H.M.: Vanish: Increasing Data Privacy with Self-Destructing Data. In: 18th USENIX Security Symposium (2009)
13. Goldberg, I.: Off-the-record messaging, https://otr.cypherpunks.ca/
14. Hoover, R.: What's the Deal with Snapchat? (Dec 2012), http://ryanhoover.me/post/38569508918/whats-the-deal-with-snapchat
15. Johnson, M., Egelman, S., Bellovin, S.M.: Facebook and privacy: it's complicated. In: 8th Symposium on Usable Privacy and Security (2012)
16. Jurgenson, N.: Temporary Social Media (Jul 2013), http://blog.snapchat.com/post/55902851023/temporary-social-media
17. Koh, Y.: Snapchat Sends 350 Million 'Snaps' (Sep 2013), http://blogs.wsj.com/digits/2013/09/09/snapchat-sends-350-million-snaps/
18. Kumaraguru, P., Cranor, L.F.: Privacy indexes: A survey of Westin's studies. Tech. Rep. CMU-ISRI-5-138, Institute for Software Research International, School of Computer Science, Carnegie Mellon University (2005)
19. Liu, Y., Gummadi, K.P., Krishnamurthy, B., Mislove, A.: Analyzing Facebook privacy settings: user expectations vs. reality. In: Internet Measurement Conf. (2011)
20. Meeder, B., Tam, J., Kelley, P.G., Cranor, L.F.: RT @IWantPrivacy: Widespread Violation of Privacy Settings in the Twitter Social Network. In: IEEE Workshop on Web 2.0 Security and Privacy (2010)
21. Nye, J.: iPhone's new app Snapchat which destroys photos after a few seconds is promoting sexting among teens (Nov 2012), http://www.dailymail.co.uk/news/article-2236586/
22. Perlman, R.: The ephemerizer: Making data disappear. Journal of Information System Security 1, 51–68 (2005)
23. Reardon, J., Basin, D., Capkun, S.: SoK: Secure Data Deletion. In: IEEE Symposium on Security and Privacy (2013)
24. Russell, K.: 10 Unusual Ways People Are Using Snapchat (Jul 2013), http://www.businessinsider.com/weird-ways-people-use-snapchat-2013-7?op=1
25. Schaffer, M.: Who Can View My Snaps and Stories (Oct 2013), http://blog.snapchat.com/post/64036804085/who-can-view-my-snaps-and-stories
26. Snapchat: How Snaps Are Stored And Deleted (May 2013), http://blog.snapchat.com/post/50060403002/how-snaps-are-stored-and-deleted
27. Snapchat: Surprise! Introducing Snapchat Stories (Oct 2013), http://blog.snapchat.com/post/62975810329/surprise
28. Survata: Is Snapchat only used for sexing?, http://survata.com/blog/is-snapchat-only-used-for-sexting-we-asked-5000-people-to-find-out/
29. Tan, G.: Tenth grade tech trends (2013), http://blog.garrytan.com/tenth-grade-tech-trends-my-survey-data-says-s
30. TigerText: Secure text messaging app for the enterprise, http://tigertext.com/
31. Van Grove, J.: Snapchat snapshot: App counts 8M adult users in U.S. (Jun 2013), http://news.cnet.com/8301-1023_3-57590968-93/
32. Wickr: Wickr: Leave No Trace, https://www.mywickr.com/
33. Wolchok, S., Hofmann, O.S., Heninger, N., Felten, E.W., Halderman, J.A., Rossbach, C.J., Waters, B., Witchel, E.: Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs. In: Network & Distributed System Security Symp. (2010)