Usable Sexurity: Studying People’s Concerns and Strategies When Sexting
Christine Geeng, Jevan Hutson, and Franziska Roesner, *University of Washington*
https://www.usenix.org/conference/soups2020/presentation/geeng

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.
August 10–11, 2020
978-1-939133-16-8

Open access to the Proceedings of the Sixteenth Symposium on Usable Privacy and Security is sponsored by USENIX.
Usable Sexurity: Studying People’s Concerns and Strategies When Sexting

Christine Geeng
Paul G. Allen School of Computer Science & Engineering
University of Washington

Jevan Hutson
School of Law
University of Washington

Franziska Roesner
Paul G. Allen School of Computer Science & Engineering
University of Washington

Abstract

Sexting, while becoming commonplace in the age of mobile phones, is still not well-studied outside of the context of youth or risk prevention. Taking the perspective that sexting is a normal intimacy-building behavior rather than a deviant practice that should be prevented, this work studies the computer security and privacy mental models and technology use of adults who sext. We conducted an online survey of adults who have sexted ($N = 247$), asking participants about which platforms they use to sext, their general sexting behaviors, what security and privacy concerns they have around sexting, and how they mitigate those concerns. We find, for example, significant concerns around sexts participants send “getting out” and being misused, as well as concerns around receiving unsolicited sexts. We also find that while participants use some technical strategies (e.g., using platforms with disappearing messages), they commonly rely on non-technical strategies like trust in their partner to mitigate concerns. We ground our findings in Citron’s legal framework of sexual privacy to support individual autonomy, intimacy, and equality, and we make design recommendations for communication platforms to support usable security and privacy for sexting.

1 Introduction

Sending or receiving nude or semi-nude photos and other media (often called “sexting”) is a common sexual behavior for adults in the United States, as technology has allowed greater ease of sharing and accessing sexual media [34]. The rise of ubiquitous mobile devices has supported sexting practices — for example, the major social media platform Snapchat was founded based in part with the idea of making it less risky to sext [28], and many other apps exist that aim to provide privacy protections for interpersonal communications.

While sexting has become common, much of psychology work has characterized it as deviant behavior [64]. This perspective leaves out the opportunity to understand and design for sexting as a normal human behavior. Sexting does carry real risks — not due to an inherent immorality, but because sexts can be abused. For example, 1 in 25 Americans has been a victim of “revenge porn” (in which sexual imagery of someone is distributed without their permission) or threats of it. Women below 30 are more likely to be targeted than men or older women, and queer individuals are more likely to be targeted than heterosexual individuals [39]. But sexting also provides significant benefits, enabling self-expression and intimacy building in consensual relationships [15].

Thus, in this work, we engage with sexting as a normal adult practice and study people’s technology-related concerns and practices related to sexting. Our work builds on and complements a call from the law and policy community to “conceptualize sexual privacy clearly and to commit to protecting it explicitly” [15]. We aim to understand how people navigate and conceptualize issues of privacy and security, and begin to articulate a framework for future research and development in usable security and privacy for sexting. We ask the following research questions:

1. $RQ1$: Practices and Experiences. What are people’s general practices and experiences with technology-mediated sexting?

2. $RQ2$: Concerns. What are people’s computer security concerns and threat models related to technology-mediated sexting?

3. $RQ3$: Mitigations. What are people’s (technical or non-technical) mitigation strategies for managing these concerns?

We present results from an anonymous online survey of adults who have sexted at some point in their lives ($N = 247$). We asked questions about with whom, how often, and on what platform people sext, as well as about their concerns and mitigation practices. We find significant concerns around both
sending sexts (e.g., that they will “get out” somehow, be misused in specific ways, or be seen accidentally by the wrong person) as well as receiving them (e.g., receiving unsolicited sexts or shoulder-surfing of solicited sexts). We further find that people rely heavily on non-technical strategies for mitigating these risks, including conscientiously establishing trust and social contracts with their sexting partners — suggesting a potential role for sexting platforms in helping scaffold or support these social contracts.

We close by making design recommendations and identifying opportunities for future research, grounded in Citron’s legal sexual privacy framework to support individual autonomy, intimacy, and equality around sexting. Our work lays a foundation for considering and supporting security and privacy for sexting as a normal behavior among technology-using adults.

2 Motivation and Related Work

We define “sexting” as the technology-mediated interpersonal exchange of sexual media, including flirtatious or sexually explicit text or emojis, and nude or semi-nude photos and videos. In this section, we survey prior scholarship on sexting and usable security, identifying gaps that motivate our work.

2.1 Scholarship on Sexting

Sexting has become a common practice: Herbenick et al. found that 27% of adult women and 24% of adult men in the United States sent nude or semi-nude photos of themselves to someone [34], and Madigan et al. found that 14.8% and 27.4% of teens send and receive sexts, respectively [42].

Academic Framing. Despite the pervasiveness of sexting, much of the academic work has focused on youth and young adults [22, 33, 64]. Furthermore, early literature on sexting treated it as a high-risk, deviant behavior, rather than an important part of adult social life that is just as normal as not sexting [21, 37]. Döring calls for an approach to sexting that acknowledges both “vulnerability and sexual agency” [21].

Research on youth has pointed out important concerns, such as adolescents feeling pressured to sext due to the erroneous belief that “everyone is doing it” [41, 77]. While youth and adult sexting both share some of the same risks and questions, it is important to also study the adult risk landscape. Our work seeks to better understand how adults (not just students) sext, from a perspective that views sexting as normal (and even important) intimate communication. Research scholarship on consensual sexting behavior has highlighted its positive role in relationship satisfaction [11, 20, 72], and that the affordances of sexting may lead to stronger sexual norms around explicit communication and consent [32]. Other work highlights potential issues that can arise with sexting, such as if the content is distributed without authorization, or if it occurs under pressure or as the result of coercion [5, 13, 73].

Mitigation Strategies. Our study expands on prior work on sexting concerns and mitigations. Sex education researchers have studied how to teach youth about safe sexting and navigating consent, coercion, and digital footprints [36, 61]. Renfrow et al. found that college students minimized perceived risks through strategies around controlling sexting content, including ‘keeping it fun’ (avoiding more vulgar terms), limiting explicitness, and creating plausible deniability [64]. Amundsen [5] conducted qualitative interviews with women about the role trust has as a mitigation strategy for non-consensual sext sharing, and how the responsibility of mitigating risk may disproportionately fall upon victims, which are themes reflected in other work [74]. These prior studies do not deeply consider the role of technology (which can both create new concerns and support new mitigations) in sexting. In this work, we take a computer security point of view.

Beyond academic research, there are numerous applications that aim to (or are commonly used to) support sexting, as well as online guides for how to sext “securely”. For example, Vice [45] lists guidelines including: get consent and set expectations, check for identifying details in photos, turn off services that automatically backup photos, wipe photos of EXIF metadata, and choose a communication app based on one’s concerns. In terms of applications, Snapchat is popular with disappearing messages (which disappear quickly from the user interface, and are deleted from Snapchat servers within 30 days [1]), among other features such as screenshot notifications and a password-protected photo album. Other sexting guides list encrypted messaging platforms such as Signal, Whatsapp, and Facebook Secret Messenger. Less well-known examples include Kaboom (which allows users to send a disappearing message through a link, so that the receiving party can see the message without installing Kaboom) and Confide (a messaging app that has disappearing encrypted messages and screenshot notifications).

2.2 Sexual Privacy Framework

Legal scholar Danielle Citron argues that sexual privacy — “the social norms (behaviors, expectations, and decisions) that govern access to, and information about, individuals’ intimate lives” — is a privacy value of the highest order because it is central to sexual agency, intimacy and equality: “[w]e are free only insofar as we can manage the boundaries around our bodies and intimate activities” [15]. Citron outlines how sexual privacy is foundational to (1) securing autonomy, (2) enabling intimacy, and (3) protecting equality.

While other privacy frameworks exist, such as contextual integrity [56], we find sexual privacy to be most appropriate for framing our study, as it forefronts the existence of unequal vulnerabilities (something that norm-based privacy theory does not do [49]). We briefly summarize these properties here, helping to motivate why protecting sexual privacy is crucial. We then place our results and recommendations in terms of
Securing Autonomy. Citron and others argue that sexual privacy is fundamental to the exercise of human agency and autonomy [15]; it is what allows individuals to manage the boundaries of their bodies and their intimate lives [3,48]. This autonomy, in turn, is viewed as fundamental to individual self-development and identity formation (who we are and who we might be in the future) [8,48,52,62].

Enabling Intimacy. Scholars have also argued that sexual (and other) privacy is critical to cultivating interpersonal intimacy, affection, and trust [15,26,65]. Indeed, research demonstrates that sexual privacy is key to the formation, maintenance, and growth of intimate relationships [4,10,27,63,76]. Intimacy is associated with important consequences for individual personal welfare, including health, well-being, community attachment and sexual sociality [30]; research has further established a positive relationship between sexual activity and such outcomes as lifespan [59] and overall happiness [9].

Protecting Equality. Sexual privacy also implicates issues of equality, justice, and power [18,66], as women, sexual minorities, and nonwhites continue to bear the disproportionate burden of sexual privacy harms, such as surveillance, harassment, and abuse [14,15,67,70,71]. More broadly, political theorists argue that intimacy is a matter of justice, as access to access to intimacy is critical to accessing primary social goods such as wealth and self-respect [6,15]. Scholars also underscore how the intimate sphere, both digital and non, is inextricably tied to relations of power [7,8,14,23,35,58] and has historically been a key determinant of social and economic welfare [6,23,31].

2.3 Scholarship in Usable Security & Privacy

Finally, our work is situated in the broader space of usable security and privacy research, particularly studies on how people navigate sharing information in interpersonal relationships, such as account and device sharing in relationships [46,60], online dating [16], social media [43], and human trafficking [12]. Freed et. al and others have studied how technology and information shared during the beginning of a trusting relationship gets abused when that turns into intimate partner violence [24,25,47]. These various settings surface both overlapping lessons (e.g., how changes in relationships over time lead to different security or privacy vulnerabilities [40], such as a parent giving a child more privacy as they grow older [29]) as well as distinct challenges for different populations. At the highest level, these works reflect that threat modeling and design must follow a socio-technical approach, considering the properties of technology, how people use it, how people interact with each other, and societal expectations for such behavior.

3 Methods

We designed an anonymous online survey, using both close- and open-ended responses, to investigate the technology-related sexting behaviors and concerns of adults.

3.1 Ethical Considerations

Our study was reviewed and determined exempt by our institution’s IRB. Given the potentially sensitive nature of our topic of study, we did not collect any identifying information from participants. Only participants who indicated that they were 18 years old or older were able to complete the survey. The opening paragraph to the survey emphasized that sexting is a common practice and that we as researchers are not taking a judgemental stance on it. The majority of questions were optional, including the choice “Prefer not to say”. Participants could opt out of allowing their (anonymous) quotes from free-response answers to be used in this publication. The quotes we include in our results were chosen to illustrate patterns of behavior, rather than any individual’s unique or potentially identifiable situation.

3.2 Recruitment

To recruit participants, we posted links to the survey on our personal Facebook, Twitter, and TikTok accounts. To widen recruitment beyond our personal networks, we distributed our survey via physical fliers in a major U.S. city and posted online to Reddit “subreddits” (e.g., /r/sex). Because prior literature often fails to capture the nuances of sexting among sexual and gender minority communities (e.g., [19]), we also recruited specifically from queer social media groups and apps; this may explain why we sample more non-straight identifying participants than reflected in the United States population [55]. Four $20 gift cards were provided to random participants.

Upon beginning the anonymous online survey and after indicating their informed consent, participants were directed to questions that established whether they were at least 18 years old and whether they have ever engaged in sexting. If participants were under the age of 18 or indicated never having participated in sexting, they were dismissed from further data collection and analysis. We excluded people who had not sexted before because our research questions focus on existing behaviors.

3.3 Procedures

We chose an online survey method to allow us to capture a broad population of people who sext [54]. We were especially interested in engaging with individuals over 18 because existing literature skews heavily towards youth and adolescent sexting practices [64]. To ensure that our research reflected
<table>
<thead>
<tr>
<th>Gender</th>
<th>Sexual Orientation</th>
<th>Age Range</th>
<th>Intimacy Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>30.36%</td>
<td>46.96%</td>
<td>18-24 52.23%</td>
</tr>
<tr>
<td>Female</td>
<td>61.54%</td>
<td>2.02%</td>
<td>25-34 37.25%</td>
</tr>
<tr>
<td>Non-binary</td>
<td>9.72%</td>
<td>8.10%</td>
<td>35-44 6.07%</td>
</tr>
<tr>
<td>Prefer not to say</td>
<td>0.81%</td>
<td>7.29%</td>
<td>45-54 3.24%</td>
</tr>
<tr>
<td>Self-describe:</td>
<td>1.21%</td>
<td>23.08%</td>
<td>55-64 1.21%</td>
</tr>
<tr>
<td>Trans</td>
<td>5.67%</td>
<td>Asexual</td>
<td>1.21%</td>
</tr>
<tr>
<td>Cis</td>
<td>89.47%</td>
<td>6.48%</td>
<td>1.21%</td>
</tr>
<tr>
<td>Questioning</td>
<td>3.24%</td>
<td>1.62%</td>
<td>1.62%</td>
</tr>
</tbody>
</table>

Table 1: Demographics of 247 survey participants included in our analysis. Gender and intimate status categories were not mutually exclusive, so participants could use multiple labels to describe themselves.

<table>
<thead>
<tr>
<th>Relationship Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monogamous</td>
</tr>
<tr>
<td>Polyamorous</td>
</tr>
<tr>
<td>Prefer not to say</td>
</tr>
</tbody>
</table>

Table 2: Participants’ relationship practice (N = 247).

the full constellation of gender identity, we followed Klaus et al.’s HCI Guidelines for Gender Equity and Inclusivity [68] in designing our demographics questions, which were asked at the end of the survey.

We asked three classes of questions in our survey, corresponding to our three research questions: (1) questions about general technology-enabled sexting practices; (2) questions about sexting-related concerns; and (3) questions about mitigation strategies to manage those concerns. The full survey instrument can be found in Appendix A.

For questions related to concerns around sending or receiving sexts, we first asked an open-ended free response version, followed by a multiple-choice version. The goal was to first elicit concerns naturally, without priming participants about what they could or should be concerned about. The multiple choice options were based on our own hypotheses as well as informed by an existing survey related to concerns among university students around sexting [64].

For participants who completed the survey, they could opt-in to submitting their email to be entered into a raffle for a $20 gift card. Their email was not linked to their survey data.

3.4 Data Analysis

We collected a total of 330 finished surveys, 249 with respondents who selected that they were at least 18 years old and had sexted before. Three researchers went through the open-ended data to look for disingenuous (e.g., joke) answers; we removed 2 respondents and completed our data analysis based on the remaining 247 responses.

For each open-ended free-response question, three researchers independently inductively coded those questions before discussing and agreeing on a set of qualitative codebooks (a separate codebook for each open-ended question). For questions where we asked an open-ended question followed by a similar multiple choice question, we incorporated the multiple choice options into our codebooks where appropriate. With the finalized codebooks, two researchers independently recoded the open-ended responses. All open-ended responses could have been coded with multiple labels.

Following McDonald et al.’s guidelines on when to seek coding agreement [50], for open-ended questions with simple responses, we used only one coder. For open-ended questions with more complex responses that we discuss quantitatively (concerns about sending sexts, and managing sending concerns), two researchers double-coded all responses. We calculated Cohen’s κ for inter-coder reliability, given that we had two coders and nominal data [51]. For concerns about sending sexts, we had a κ of “substantial” (0.61–0.80) to “almost perfect agreement” (0.81–1.00) for 91.3% of categories. For managing sending concerns, we had a κ of “substantial” to “almost perfect agreement” for 93.76% of categories. (More details on κ per category can be found in Appendix C). We discussed discrepancies between coders for all codes until we reached a near-consensus.

We compare answers to some multiple choice questions across genders for statistical differences. Since respondents were able to select multiple genders, we evaluate differences with a test of multiple marginal independence, which is calculated using a modified Pearson’s Chi-squared statistic and a bootstrapping method to estimate the sampling distribution [38]. We use a significance level of α = 0.05. We report Cramer’s V for effect size on a scale of 0 to 1 (with associations > 0.10 indicating at least a small effect [17]). We discarded participants who selected “Prefer to self-describe” (2 respondents with different answers) or “Prefer not to say” for their gender, leaving us with three nominal variables (male, female, non-binary). Since we asked if participants were transgender in a separate question, we cannot distinguish that category with this analysis, and our results are limited in that respect.

3.4 Data Analysis

We collected a total of 330 finished surveys, 249 with respondents who selected that they were at least 18 years old and had sexted before. Three researchers went through the open-ended data to look for disingenuous (e.g., joke) answers; we removed 2 respondents and completed our data analysis based on the remaining 247 responses.

For each open-ended free-response question, three researchers independently inductively coded those questions before discussing and agreeing on a set of qualitative codebooks (a separate codebook for each open-ended question). For questions where we asked an open-ended question followed by a similar multiple choice question, we incorporated the multiple choice options into our codebooks where appropriate. With the finalized codebooks, two researchers independently recoded the open-ended responses. All open-ended responses could have been coded with multiple labels.

Following McDonald et al.’s guidelines on when to seek coding agreement [50], for open-ended questions with simple responses, we used only one coder. For open-ended questions with more complex responses that we discuss quantitatively (concerns about sending sexts, and managing sending concerns), two researchers double-coded all responses. We calculated Cohen’s κ for inter-coder reliability, given that we had two coders and nominal data [51]. For concerns about sending sexts, we had a κ of “substantial” (0.61–0.80) to “almost perfect agreement” (0.81–1.00) for 91.3% of categories. For managing sending concerns, we had a κ of “substantial” to “almost perfect agreement” for 93.76% of categories. (More details on κ per category can be found in Appendix C). We discussed discrepancies between coders for all codes until we reached a near-consensus.

We compare answers to some multiple choice questions across genders for statistical differences. Since respondents were able to select multiple genders, we evaluate differences with a test of multiple marginal independence, which is calculated using a modified Pearson’s Chi-squared statistic and a bootstrapping method to estimate the sampling distribution [38]. We use a significance level of α = 0.05. We report Cramer’s V for effect size on a scale of 0 to 1 (with associations > 0.10 indicating at least a small effect [17]). We discarded participants who selected “Prefer to self-describe” (2 respondents with different answers) or “Prefer not to say” for their gender, leaving us with three nominal variables (male, female, non-binary). Since we asked if participants were transgender in a separate question, we cannot distinguish that category with this analysis, and our results are limited in that respect.
Figure 1: Participants reported how often they sent and received nude or semi-nude videos, photos, and sexual or intimate messages \((N = 247)\). *1 person selected “Prefer Not To Say” for how often they received videos.

### 4.1 Sexting Practices and Experiences

We begin by considering general sexting practices and experiences, to help provide context for the concerns, mitigations, and design recommendations that follow.

#### 4.1.1 Sexting Frequency

We found that 58.6% (144) of our participants said they currently sext, 33.6% said they have sexted before and may again in the future, and 8.8% said they have sexted before but no longer plan to. Considering sexting medium (i.e., video, image, or text), we found that text-based messages and nude or semi-nude photos were the most common, compared to nude or semi-nude videos (which only half of our sexting participants reported sending or receiving). The results look similar for sending and receiving frequency, suggesting this behavior is reciprocal. Figure 1 breaks this down in detail.

For participants who reported not currently sexting (regardless of whether they plan to in the future), we asked them why they stopped sexting. This question was multiple choice and optional; 106 participants responded. Of those, 45 said they stopped because they were no longer in a relationship with the person they sexted, and 31 said it was because they were no longer in a long-distance relationship. 28 said they were not interested, and 10 said they had had a poor experience.

In a free-response follow-up question, out of the 10 people who selected having had a poor experience, 3 said sexting felt awkward, and 1 person said they were scammed.

For people who said they would sext again in the future, the majority marked their reason for stopping as no longer being in a relationship. For the people who said they would not sext again in the future, the majority marked their reason as not interested, with their explanations including “I honestly wasn’t super into it”, “no longer feels private”, and “it felt like I was forcing myself into it”.

#### 4.1.2 Device and Platform Usage

Our participants primarily sext on their smartphone devices: 244 use their phone, 73 use their computer, and 16 use their tablet (with some using multiple devices, i.e., these responses are not mutually exclusive).

When asked about how they use social media to send
We explicitly asked participants about their practices around sexting-related photos/video, the majority of our participants answered that they use Snapchat direct message (114; see Table 3 for the full breakdown). For other platforms, SMS had the highest usage (for sending photos/video) at 137 participants, possibly because it is a phone’s default messaging app. (2 “Other” responses explicitly mentioned iOS Message, which respondents may have also counted as SMS.) “Other” responses included: Tumblr, Whisper, Kik, Skype, Reddit, Discord, Wired, Burner, email, and other dating sites. We do not have data about whether participants used these exclusively for sexting or also for other purposes. Considering sexual and intimate text messages, the distribution of platforms used looks similar to what we see for photos/video in Table 3.

Some participants reported using platforms that explicitly include security- and/or sexting-related functionality. For example, Snapchat has disappearing messages, screenshot notifications, and a password-protected photo album. Considering the more obscure platforms mentioned by participants: Burner provides a temporary new phone number that allows for communication while obscuring one’s actual phone number. Wire is an end-to-end encrypted communication app, and Kik and Whisper tout themselves as anonymous social media services. We return to people’s uses (or non-uses) of these features in Section 4.3.

### 4.1.3 Storing Sexts

We explicitly asked participants about their practices around storing their own and other people’s nude or semi-nude images or videos (which we refer to by the shorthand “nudes” below). We note that these responses must be interpreted under the risk of social desirability bias: participants may have underreported socially undesirable behaviors, such as storing or sharing sexts without consent.

With respect to one’s own nudes, we found that out of 247 responses, 130 (52.6%) said they stored nude or semi-nude photos or videos of themselves, 114 said they did not, and 3 said preferred not to answer. We find that storing nudes received from other people is even more common: among 234 participants who reported having received a sext and answered this question, 145 (62.0%) stated they have saved nude photographs or videos they received, 85 said they had not saved any, and 4 preferred not to answer.

For participants who store others’ nudes, we asked additional questions about why and how they are saved (which may help explain why more participants’ save other people’s nudes than their own). In response to an open-ended question about why, most participants mentioned saving others’ nudes for later use (e.g., nostalgia, to masturbate). Several participants mentioned saving to share with friends, but none of those responses explicitly mentioned getting consent from the sender to share. Two people noted they saved content with no intention of sharing it, and 9 people thought it was assumed they would save a partner’s photos. We note that 24 people did mention that they saved nudes with permission from sender (and 4 people mentioned they were even asked by the sender to save). In this case, this number is a lower bound on how many participants received explicit consent to save nudes, since we did not specifically ask this in the question.

In the words of one participant:

“I saved them because my girlfriend took the time to take a nice photo, just for me, and she’s given me the OK to save them. When I miss her, it helps to look through a medley of sexual and non-sexual photos of her.” – Male, straight, 18-24

In another question, we asked explicitly about whether senders knew that nudes had been saved by the participant. Out of 145 responses, 110 said that senders knew, 24 said some of the senders know, 7 said they do not know, and 4 preferred not to say. When we consider how nudes were saved, we note that only a small number of participants reported methods that explicitly aim to avoid knowledge by the recipient: 56% of participants directly stored to device, 37% took a screenshot, 5% (10) took a photo (presumably to circumvent screenshoting notifications, i.e., taking advantage of the “analog hole”), and 3% selected “Other”: one respondent mentioned using screenshotting apps to prevent Snapchat screenshot notifications (e.g., Private Screenshots), and an-

<table>
<thead>
<tr>
<th>Other Platforms</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS</td>
<td>137</td>
<td>62.27%</td>
</tr>
<tr>
<td>Whatsapp</td>
<td>38</td>
<td>17.27%</td>
</tr>
<tr>
<td>Grindr</td>
<td>19</td>
<td>8.64%</td>
</tr>
<tr>
<td>Tinder</td>
<td>11</td>
<td>5.00%</td>
</tr>
<tr>
<td>Telegram</td>
<td>10</td>
<td>4.55%</td>
</tr>
<tr>
<td>Signal</td>
<td>6</td>
<td>2.73%</td>
</tr>
<tr>
<td>OkCupid</td>
<td>4</td>
<td>1.82%</td>
</tr>
<tr>
<td>Hinge</td>
<td>3</td>
<td>1.36%</td>
</tr>
<tr>
<td>Kaboom</td>
<td>1</td>
<td>0.45%</td>
</tr>
<tr>
<td>Confide</td>
<td>1</td>
<td>0.45%</td>
</tr>
<tr>
<td>Other</td>
<td>28</td>
<td>12.73%</td>
</tr>
</tbody>
</table>

Table 4: Multiple-choice responses to what other platforms participants use to send/receive photos or videos (N = 220).

<table>
<thead>
<tr>
<th>Reasons for Saving Received Nudes</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>To use/look at later</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Insurance</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Saving is app default</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Partner is away</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Asked by sender to save</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>To share with friends/others</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>To be able to find more easily</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Mutual saving</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Coded counts of participant open-ended responses to why they saved sexts sent to them (N = 145).
other mentioned saving to a private folder.

For participants who save other people’s nudes, 75 said they store on their device’s photo storage (e.g., “Camera Roll”), 49 said a separate on-device album, 32 said a specific secret-keeping app (e.g., Snapchat’s “My Eyes Only” folder, Vault, or an encrypted folder on a desktop/laptop computer), and 17 said online (e.g., Google Photos, Dropbox; some apps mentioned in the prior option are also online storage). Only 5 participants noted that their reason for saving is because this is the app’s default behavior, but we suspect that this is an under-count, since many participants mentioned using SMS and other apps that automatically save content by default.

Out of the 145 participants who said they save other people’s nudes (see Figure 6), most said they would save until asked to delete. For respondents who selected “Other” and “Save them for some amount of time”, many explained that they might save until the end of the relationship, or save for time periods ranging from a week to years. One person mentioned they assume the photos would be automatically deleted when iPhone’s cache is full, and another person mentioned that they have not thought that far ahead.

Overall, our results suggest common practice involves saving received nudes — not typically for nefarious purposes, and often (reportedly) with the consent and knowledge of the sender. Given these legitimate uses, a recommendation or platform-enforced policy of not saving received nudes would often be impractical and overly restrictive.

### 4.1.4 Sharing Sexts

We also asked explicitly about whether participants shared received sexts with others. Out of 247 responses, 32 said yes, 213 said no, and 2 said they prefer not to say. For yes answers, many people mentioned showing to friends or partners, and some mentioned sharing unsolicited photos for support and mockery. Some participants took measures to protect the privacy of the sext’s creator, including getting explicit permission to share or anonymizing or otherwise editing the sexts — for instance, cropping and censoring identifying information.

### Concerns Sending Sexts

<table>
<thead>
<tr>
<th>Concerns Sending Sexts</th>
<th>N</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sexts get around to other people</td>
<td>93</td>
<td>75.00%</td>
</tr>
<tr>
<td>Sexts used as blackmail</td>
<td>83</td>
<td>66.94%</td>
</tr>
<tr>
<td>Receiver’s devices will get hacked and the content will get out</td>
<td>78</td>
<td>62.90%</td>
</tr>
<tr>
<td>Receiver will intentionally share content with others</td>
<td>72</td>
<td>58.06%</td>
</tr>
<tr>
<td>Sexts will get out</td>
<td>93</td>
<td>75.00%</td>
</tr>
<tr>
<td>Sexts used as blackmail</td>
<td>83</td>
<td>66.94%</td>
</tr>
<tr>
<td>Sexting causes ridicule from others</td>
<td>49</td>
<td>36.94%</td>
</tr>
<tr>
<td>Not sure I sent it to the right person</td>
<td>38</td>
<td>29.78%</td>
</tr>
<tr>
<td>Bullying or harassment from others</td>
<td>29</td>
<td>21.27%</td>
</tr>
<tr>
<td>Unwanted attention</td>
<td>28</td>
<td>21.27%</td>
</tr>
<tr>
<td>Legal liability</td>
<td>25</td>
<td>18.87%</td>
</tr>
<tr>
<td>Sexting makes people feel led on, or misunderstood</td>
<td>24</td>
<td>18.18%</td>
</tr>
<tr>
<td>Damages relationships</td>
<td>19</td>
<td>14.61%</td>
</tr>
<tr>
<td>Conflicts at work</td>
<td>19</td>
<td>14.61%</td>
</tr>
<tr>
<td>Unwanted sexual contact</td>
<td>15</td>
<td>11.11%</td>
</tr>
<tr>
<td>Engagement with law enforcement</td>
<td>10</td>
<td>7.69%</td>
</tr>
<tr>
<td>Other</td>
<td>9</td>
<td>6.79%</td>
</tr>
</tbody>
</table>

Table 7: Multiple-choice responses to what concerns participants have when sending sexts (N = 124). This excludes 122 participants who send sexts but did not indicate that they have concerns around sending sexts.

### 4.2 Concerns around Sexting

We now turn to our participants’ concerns around sending and receiving sexts. For both types of concerns, we first asked an open-ended question to elicit natural, non-primed concerns, followed by a multiple-choice question that allows us to evaluate the frequency of named concerns.

### 4.2.1 Concerns Around Sending Sexts

Table 7 shows participant concerns about sending sexts in response to our multiple choice question. The following concerns were most prevalent: “Sexts get around to other people” (93) and “Sexts used as blackmail” (83). Similarly, the most-used codes for the open-ended concern question (which, again, was asked before the multiple choice) was “Sexts will get out” (38) and “Shared/shown to others” (24). While some participants indicated only generic concern, others indicated a more specific threat model, specifying adversary (e.g., partner or platform) or consequence (e.g., impact on career or possible negative judgement). For example, one participant wrote:

> “We live in a society of prudes — I worry that things will leak and get out there and people will judge me for what I have shared with someone under the pretext that it was going to be private.” – Non-binary, asexual, 25-34

Many fewer participants in the open-ended response mentioned “Sexts used as blackmail” (9), “Revenge porn” (8),
Concerned about sexts being used as blackmail?

<table>
<thead>
<tr>
<th></th>
<th>No</th>
<th>Yes</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>57</td>
<td>17</td>
<td>74</td>
</tr>
<tr>
<td>Female</td>
<td>93</td>
<td>59</td>
<td>152</td>
</tr>
<tr>
<td>Non-Binary</td>
<td>15</td>
<td>9</td>
<td>24</td>
</tr>
</tbody>
</table>

Table 8: N = 243. N here and for Table 9 includes all participants who said they send sexts and who selected at least Male, Female, or Non-binary for their gender.

Concerned about sexts causing ridicule from others?

<table>
<thead>
<tr>
<th></th>
<th>No</th>
<th>Yes</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>69</td>
<td>5</td>
<td>74</td>
</tr>
<tr>
<td>Female</td>
<td>123</td>
<td>29</td>
<td>152</td>
</tr>
<tr>
<td>Non-Binary</td>
<td>20</td>
<td>4</td>
<td>24</td>
</tr>
</tbody>
</table>

Table 9: N = 243.

or “Misuse” (11) as concerns, compared to the 83 responses to “Sexts used as blackmail” in the multiple-choice question; there is a similar discrepancy with the hacking concern. Participants may not have considered the multiple-choice concerns without being prompted to, or found the multiple-choice questions easier and/or less effort to answer.

Our open-ended question surfaced concerns we had not anticipated in our multiple choice options. The language “revenge porn”, “blackmail”, and “misuse” was used rather than “Bullying or harassment” (from the multiple choice question). Some responses also gave insights into participants’ thoughts about potential adversaries: 10 respondents noted they were not concerned because they trusted their partner, and 3 noted they were not concerned because they trusted the app. On the flip-side, 6 respondents mentioned not trusting the platform companies, and 3 respondents were concerned about bugs or vulnerabilities in the app. Other concerns not mentioned in the multiple choice options included deanonymization (7), recipient will save sexts (6), insecure network or cloud (2), photos will be modified (1), and images will be used to impersonate sender (1). Referring to both saving sexts and deanonymization concerns, one participant wrote:

“People will save the photos. Specifically photos of my face and body together.” – Male, gay, 18-24

In the open-ended questions, many responses were vaguely worded and did not specify the person or platform that somehow distributes or leaks their content. Such responses could be a reflection of vague or broad threat models in the mind of the participant, or of survey fatigue and the limitation of not being able to follow up for elaboration. To the extent that these responses suggest genuinely adversary-less threat models, they reflect Venema et al.’s findings, in which the responsibility of people who share explicit photos without consent is invisible in how the risks are described (e.g., “they [i.e., the photos] spread” or using the passive voice) [74].

Concerns Receiving Sexts

<table>
<thead>
<tr>
<th>Concerns Receiving Sexts</th>
<th>No</th>
<th>Yes</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiving unsolicited content</td>
<td>43</td>
<td>66.15%</td>
<td></td>
</tr>
<tr>
<td>Shoulder surfing</td>
<td>34</td>
<td>52.31%</td>
<td></td>
</tr>
<tr>
<td>My device will get hacked and their content will get out</td>
<td>29</td>
<td>44.62%</td>
<td></td>
</tr>
<tr>
<td>Not really the person I think it is</td>
<td>10</td>
<td>15.38%</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>6</td>
<td>9.23%</td>
<td></td>
</tr>
</tbody>
</table>

Table 10: Multiple-choice responses to what concerns participants have when receiving sexts (N = 65). This excludes 185 participants who receive sexts but did not indicate that they have concerns around receiving sexts.

Gender Differences for Sending Concerns. Men were significantly less likely to be concerned about blackmail (p = 0.02, V = 0.15), with 22.97% of men, 38.82% of women, and 37.50% of non-binary individuals selecting being concerned (Table 8). Men were also significantly less likely to be concerned about ridicule (p = 0.04, V = 0.15), with 6.76% of men, 19.08% of women, and 16.67% of non-binary individuals selecting being concerned (Table 9). We did not see significant gender differences for other sending-related concerns.

4.2.2 Concerns About Receiving Sexts

Table 10 breaks down participant concerns about receiving sexts in response to our multiple-choice question. The greatest concern was over unsolicited sexts — a concern that is well-founded, given that out of 247 responses, 56% of people (138) said they have previously received unsolicited sexts.

Another major concern was shoulder-surfing, a concern for both receiving and sending sexts. One participant wrote:

“I want a warning before. [I] do not want to open a snap with a nude and have my grandmother sitting next to me. [I] must have warning in advanced.” – Female, lesbian, 18-24

Again, our open-ended question surfaced additional concerns, including the sender may escalate behavior/harassment (3), receiving a sext in an inappropriate context (2), being triggered(1), future regrets (1), receiving illegal material (1), and false accusations (1). There were 10 multiple-choice responses to concern over sender authenticity (i.e., being sure about the identity of the sender), versus only 1 response in the open-ended question.

Another concern was feeling forced to reciprocate the sext (4), i.e., forced to send back a sext or engage in other related behavior. For example:

“I am concerned that by me receiving sexts, it gives off the impression that I am open to any sexual activity/interaction with the other party.” – Female, straight, 18-24
Gender Differences for Unsolicited Sexts. Women and non-binary individuals were significantly more likely to receive unsolicited sexts ($p = 0.005, V = 0.19$) and be concerned about that ($p = 0.04, V = 0.15$). 63% of women, 69.5% of non-binary people, and 44% of men have received an unsolicited sext (Table 11), and 21.85% of 151 women, 20.83% of 24 non-binary people, and 9.33% of 75 men indicated that they were concerned about this.

Women were also significantly more likely to be concerned about shoulder-surfing ($p = 0.02, V = 0.15$), with 17.88% of 151 women, 6.67% of 75 men, and 8.33% of 24 non-binary individuals being concerned. These comparisons can be viewed in table form in Appendix B. This result echoes the earlier finding that women are more likely to be concerned about negative judgement (ridicule) as a consequence of sending sexts. We did not see significant gender differences for other receiving-related concerns.

4.3 Mitigation Strategies

Finally, this section reports on participants’ mitigation strategies for the concerns mentioned above, again elicited via both open-ended and free-response questions. We observed that participants mentioned both technical as well as significant non-technical mitigations strategies.

4.3.1 Technical Strategies

In both the open-ended question (34) and in the multiple choice question (57), participants mentioned that they manage concerns by picking a platform with specific features they want. The most common featured mentioned (23 in open-ended) was disappearing messages. (The most-mentioned disappearing message app was Snapchat, consistent with responses about platforms used for sexting.) Another feature often mentioned (and also supported by Snapchat) is notifications when the recipient takes a screenshot of a sent message or image. While these UI-based features may be sufficient to enforce privacy in most circumstances, we note that this mitigation feature alone would not be sufficient if someone is concerned about a receiver sharing supposedly ephemeral

<table>
<thead>
<tr>
<th>Have you received an unsolicited sext?</th>
<th>No</th>
<th>Yes</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>42</td>
<td>33</td>
<td>75</td>
</tr>
<tr>
<td>Female</td>
<td>55</td>
<td>94</td>
<td>149</td>
</tr>
<tr>
<td>Non-Binary</td>
<td>7</td>
<td>16</td>
<td>23</td>
</tr>
</tbody>
</table>

Table 11: $N = 243$. $N$ includes all participants who selected at least Male, Female, or Non-binary for their gender.

“I often feel coerced into responding via reciprocation and if I don’t then the person will be angry.” – Female, bi/pan, 24-34

sexts — we note that there exist screenshot apps to circumvent notifications, and recall that 10 of our participants said they take photos to save nudes rather than screenshot them.

Other technical strategies mentioned include: having a password that protects access to an image, app, or device (e.g., Snapchat’s password-protected “For My Eyes Only” photo album), explicitly deleting messages or media, using encrypted platforms such as Telegram or Signal, and using app or platform settings to ensure that notifications do not make the sexts visible (e.g., to a shoulder-surfer). Some participants explicitly wrote about the threat model they considered when picking a platform. For example, the following participant specifically picks a platform with content deletion because they are concerned about shoulder-surfing:

“Telegram has message & chat history delete functionality and I’m most concerned about messages being *seen* on my device, not on the other person’s device - I trust them.” – Non-binary, pansexual, 18-24

Many participants listed anonymizing sexts as a strategy (29 open-response, 51 in MC) — for example, cropping or blurring faces, or taking photos without identifying features within the frame. Only one respondent out of 20 mentioned being aware of potentially identifying locations in the photo:

“Using Signal, not showing face, no identifying marks/locations, no posting public photos that correspond in time/place to explicit photos, no full nudity, only send images that if they would get out I could claim they were art photography or not of me.” – Female, bisexual and queer, 25-34

No participant mentioned being concerned about EXIF data, image metadata that can compromise privacy and that some online safe-sexting guides recommend deleting [45]. (We note that some apps strip EXIF data automatically. For example, Signal strips EXIF data from photos taken within

<table>
<thead>
<tr>
<th>Concern Management Behavior</th>
<th>Only sexting with people you trust</th>
<th>Using disappearing messages (e.g., Snapchat, Instagram stories)</th>
<th>Prior talks to set rules/boundaries</th>
<th>Choose app with features you want</th>
<th>Limiting how explicit the sext is</th>
<th>Ensuring plausible deniability e.g. not including identifying marks in photo</th>
<th>Password-protect or encrypt sexts</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>110</td>
<td>46.76%</td>
<td>42.45%</td>
<td>41.01%</td>
<td>38.13%</td>
<td>36.69%</td>
<td>22.30%</td>
<td>5.04%</td>
</tr>
<tr>
<td>Female</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Binary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 12: Multiple-choice responses to what kind of actions people take to manage their concerns, both around sending and receiving sexts ($N = 140$).
the app, based on the authors’ testing and some anecdotal online sources [2], though not official Signal documentation).

4.3.2 Non-Technical Strategies

The most common mitigation strategy in both the multiple choice (110) and free-response question (54) was only sexting with someone the person knows and trusts. Communicating rules and boundaries (which includes asking the receiver to delete the photos) was also common (25 in free-response), whether the receiver is a long-term partner:

“I sext with my partner whom I trust and we had several conversations about sexting before we started (when to delete photos, if we were at risk of revenge porning each other (we’re not)), from there we talked about several different platforms and ultimately chose an encrypted platform. It’s not completely safe but it’s a calculated risk.” – Female, bi/pan, 25-34

or someone the participant does not know as well:

“I don’t have extensive conversations with the people, but I’ll say something like...’if I send this, don’t show it to anyone else.’ Usually it’s a one time comment and when they agree to keep it to themselves, everything is on the table to share. I need to have a minimum level of trust with a person before I’ll sext.” – Female, bi/pan, 35-44

Other non-technical strategies included limiting the explicitness of the photo (24 in the free-response) and only sending content the participant would be comfortable appeared in public (3). Three people listed not sexting as their mitigation strategy — i.e., potentially feeling forced to forgo opportunities for building intimacy, as we discuss further in Section 5.

One participant mentioned acquiring collateral as a strategy — i.e., ensuring that the other person sends a photo first that they can save as “insurance”, to discourage the other person from ever misusing their images. For example:

“I save them because usually the person whom I have sent content to had saved mine in chat (Snapchat) or screenshotted them. So I save them as a precaution/insurance/leverage (if it comes to that).” – Female, straight, 18-24

Often, participants mentioned using a mix of technical and non-technical strategies. The particularly high prevalence of interpersonal trust and norms as a mitigation strategy points to an opportunity for platform design that can help create and support such norms, which we discuss further in Section 5.

4.3.3 Mitigations for Unsolicited Sexes

The previously discussed mitigation strategies are ones that can be deployed proactively. By contrast, receiving an unsolicited sext requires a reactive strategy. Table 13 summarizes coded open-ended responses to a question about how participants manage unsolicited sex. Participants used both platform-supported mitigations (such as reporting or blocking senders) as well as ad-hoc, conversation-based approaches. While most participants do not engage with unsolicited sex, some reported reacting by “trolling” the sender in response:

“Don’t pay it much attention. Sometimes mess with them a bit, tell them something like ‘It won’t let me open it (your pic) it keeps giving me an error message’. They spend ages checking their message settings, trying to resend it, and trying to explain to me how to open it. But usually just ignore and don’t respond. Sometimes will have a short conversation and maybe a bit of a laugh about it.” – Female, straight, 35-44

Also, 8 people mentioned that their behavior depends on if the behavior is repeated, and 4 people said their behavior depends on if they know the sender. For example:

“It depends. When it someone I have never spoken to, I will usually screen grab it then delete it from the app – share it with someone who is complaining about their wonderful relationship. However, if it is someone I know and have met, it is more upsetting – and I will either message them about what I don’t want, or stop talking to them altogether. Usually with a simple ‘No.’ and block it.” – Non-binary, asexual, 25-34

<table>
<thead>
<tr>
<th>Handling Unsolicited Sexes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
</tr>
<tr>
<td>Ignore</td>
</tr>
<tr>
<td>Ask them to stop/Confront</td>
</tr>
<tr>
<td>Delete message</td>
</tr>
<tr>
<td>Report to platform</td>
</tr>
<tr>
<td>Troll them</td>
</tr>
<tr>
<td>Change subject (keep talking)</td>
</tr>
<tr>
<td>Take screenshot</td>
</tr>
<tr>
<td>Stop using platform</td>
</tr>
<tr>
<td>Respond positively</td>
</tr>
</tbody>
</table>

Table 13: Coded counts of how participants respond to unsolicited sex (N = 138).

5 Discussion

Our study captures a rich account of adult privacy and security behaviors around sexting and expands existing knowledge of how individuals navigate sexual privacy in the digital age. Through this work we aim to conceptualize usable sexual privacy and security clearly and commit to protecting it explicitly (echoing Citron [15]). To that end, we adopt and embrace Citron’s framework of sexual privacy from legal
scaffolding sexting norms raises serious questions about ways of scaffolding sexting norms that should be explored. Our results surfaced the ad hoc ways in which people articulate and establish norms, expectations, and boundaries around sexting in order to mitigate sexual privacy harms. Critically, our research implicates the role of platforms in scaffolding the articulation and establishment of these norms. Indeed, developing levers to articulate and establish one’s preferences with respect to sexting is arguably key to individual sexual agency and autonomy as well as to establishing trust and ensuring accountability. Yet scaffolding sexting norms raises serious questions about both platform and individual responsibility. We consider two ways of scaffolding sexting norms that should be explored in future research and development: product/platform-level policy and user interface design.

First, platforms can establish product policies or community guidelines with respect to sexting. For example, community guidelines could contain language like “Make sure to ask others for consent before screen-shoting images or messages in chat feeds” or “Receiving a sext does not obligate a response in kind”. In such an approach, the platform plays a central role in articulating norms around sexting (which can in turn reduce user autonomy in some ways).

Second, platforms can leverage user interface design to better enable users to articulate their own preferences and expectations around sexting. For example, platforms could provide fixed disclosure options for users to express particular preferences. The gay dating and hookup platform Grindr already provides an “Accept NSFW Pics” profile disclosure field where users can select “Never”, “Not At First”, and “Yes Please.” Here, the platform plays a more co-constructive role with respect to sexting preferences and expectations.

On the other hand, platforms could provide open-ended disclosure options (similar to a free-form “About Me” field) for users to express more individualized preferences around sexting. Here, the platform allows norms to be driven by individual users rather than the platform itself. Having the latter free-form space would make more sense on a mixed-use messaging app (e.g., Snapchat) than having a specific disclosure field for sexts, as users may use their messaging profile to contact different people for non-intimate reasons.

**Platform Management of Unsolicited Sexts.** Our research aims to understand and support individual actions and mitigation strategies towards sexual privacy and safety, but our results must be viewed in a broader societal context where sexting can be both empowering or disempowering. The negative side, unsolicited sexts are a major concern (and a disproportionate burden for women). While norm-supporting mitigations can help reduce some unsolicited sexts as discussed above, they cannot prevent explicitly malicious behavior. This issue is particularly challenging, because while people can take some proactive actions to manage their concerns about sending intimate content (e.g., avoiding identifying features), they can only take reactive steps to manage unsolicited sexts (short of being forced to opt out of platforms entirely).

This threat model suggests that platforms may need to take a more proactive role in mitigating unsolicited and harassing sexual content, not only in response to user reports. This role could take the form of messaging affordance design: for example, not allowing photos to be sent unless both people in a conversation enable the feature. Platforms could also play a greater role in detecting and blocking certain types of content directly, as others have proposed and begun experimenting with [44]. However, this approach comes with significant challenges that future work must consider — e.g., how to integrate or balance content detection with end-to-end encryption, and how such a feature might interact with (in the U.S.) the First Amendment and a company’s legal liabilities [57].

**5.2 Enabling Intimacy**

**Existing Platform Affordances.** Our study surfaced a number of extant design practices that worked to preserve sexual privacy and enable intimacy. Important affordances that surfaced in our study include screenshot notifications, disappearing messages, and password protection for files. While these features are common on platforms like Snapchat, they do not pervade a variety of the other platforms or mediums people use (but are not necessarily designed) for sexting (e.g., Facebook, SMS, Grindr, Tinder). Our results suggest that these affordances are an important starting point for other platforms looking to account for sexting. We note that the design of these affordances can and should be informed by the real threat models of users like our participants. For example, while Snapchat has been criticized in the past for its disappearing messages not being truly secure [69], we note that even less-than-perfect security may be sufficient against the more common threat models involving violations (sometime accidental) by communication partners rather than company access or sophisticated external “hackers”. (Though supporting stronger threat models is also crucial for some users, especially those particularly vulnerable to targeted attacks).

More generally, the focus of our work has not been on unpacking the technical properties of different platforms used by our participants. Our work lays a foundation for important future work to study these technical properties and to identify — and bridge — any gaps between the threat models they securely support and the threat models important to individuals engaging in sexting.
Designing for Storage. One area of technical design that our results draw attention to is around storage. We found that large fractions of respondents save their own (52.6%) and others’ (62.0%) nudes or sexual images — often for legitimate purposes and with consent — suggesting that platforms must design for this behavior as a norm rather than an indication of the intent to misuse the content. These findings shed light on the need to grapple with the digital footprint of sexting: who stores it, how and where is it stored, and how is it secured? Our findings suggest a variety of overlapping models, including storage on personal devices, storage in a file-sharing service (e.g., Google Drive), and platform-based storage (e.g., some dating and hook-up platforms, like Scruff, Growlr, and Jack’d, provide built-in “private photo” storage where images can be access-controlled and access-monitored). Participants sometimes used a storage strategy deliberately and sometime incidentally (e.g., storing one’s own photos in the device “Camera Roll”). Different strategies support different threat models, and we recommend that both users and platform designers face these choices consciously.

Opting Out as a Last Resort. Finally, while only a few people indicated not sexting as a mitigation strategy, we highlight that this decision relates to (or rather, hinders) enabling intimacy. First, abstaining from sexting is a valid behavior to alleviate sexual privacy risk as well as a valid boundary one might establish with respect to their intimate life. Second, however, if sexual privacy concerns are causing people not to sext, but there are other behaviors or design practices that could mitigate these concerns, then it is not the optimal outcome for people to feel like they have to choose to opt out of sharing sexual media. A goal of sexting platform design or other interventions, then, should be to support positive sexting and not force people to opt out due to unmitigated risks.

5.3 Protecting Equality

Supporting prior work [14, 19, 39, 53, 67, 75], our results provide further evidence to suggest that women and sexual minorities are disproportionately burdened by certain sexual privacy risks — receiving more unsolicited sexts, feeling pressured to sext, worrying more about negative judgments (both for sending and receiving) and the potential misuse of their intimate content. It is crucial that future work in this space further study such disparate impacts and take them into account when designing to mitigate potential risks with sexting.

Our results also highlighted the potentially generic threat models of many participants when asked to consider sexual privacy concerns without prompting. Many participants expressed vague concerns, often in the passive voice, about their sexts “getting out”. Though these responses could be due in part to the survey methodology (where we could not follow up to clarify the vague responses, and participants might have opted to answer the question quickly rather than exhaustively), these results echo findings from prior work [74] and raise concerns that participants have internalized “victim-blaming” perspectives, shifting the responsibility away from untrustworthy partners and other actors who take advantage of normal sexting behavior. We recommend that future work dig deeper into these questions.

6 Limitations

Our survey-based approach is subject to standard limitations of this methodology: for example, we could not ask follow-up questions to clarify or dig further into participants’ responses. Sometimes participants gave generic responses about their concerns, mentioning only “privacy” without additional detail about their mental threat models (e.g., privacy of what, or against whom). Since we could not follow up, we cannot distinguish vague mental models from survey fatigue, and we report our results cautiously in such contexts.

Our sample of participants is not representative of the overall U.S. population — with higher rates of LGBTQ individuals and women in particular, and with only 10.43% participants over 34 — so our results do not support any census-representative claims. With our screening method, it is unclear if older adults were reached and chose not to sext, excluding them from our participant pool, or if they were not reached through our recruitment methods. We also do not capture the sexting concerns of people who haven’t sexted before. We also recognize that an online survey on sexting behaviors will elicit some degree of self-selection bias insofar as those who participate may have higher baseline comfort and knowledge around sexting.

7 Conclusion and Future Work

Via an online survey of 247 adults who sext, our findings contribute to the field of usable privacy and security by expanding our understanding of how adults navigate sexting, using both technical strategies such as disappearing messages and non-technical strategies such as relying on trust. We show (similar to prior work) that men were less likely than women and non-binary individuals to be concerned about certain potential sexting risks, and less likely to receive unsolicited sexts. Placing our results in the context of the sexual privacy framework, we suggest ways platforms can support autonomy, intimacy, and equality through platform affordances and policies.

Future work on usable sexual privacy and security should consider (1) how communication platforms can surface and scaffold individuals’ norms, expectations, and boundaries around sexting, (2) how usable security can address the broader inequities in the experience of sexual privacy harms, and (3) how the technical properties of privacy-enabling affordances compare to user expectations and assumptions around the security and privacy implications of such features.
Acknowledgments

We are especially grateful to our survey participants. We also thank our reviewers and shepherd for their helpful feedback. We thank Ryan Calo, Catherine Holmes, Naveena Karusala, Shrirang Mare, Eric Zeng, Ben Zisk, and the UW Statistical Consulting Services for their guidance and input. And we thank the moderators of reddit.com/r/sex and of queer social groups for helping advertise our study. This research is supported in part by the National Science Foundation under Award CNS-1513584.

References


Sixteenth Symposium on Usable Privacy and Security


A Survey Instrument

1. Are you 18 years old or over?
   - Yes
   - No

2. Have you ever sexted? That is, do you create, send, or receive sexually suggestive messages, or nude or partially-nude photos, through digital communications?
   - Yes, I currently sext.
   - Yes, I have sexted before and may again in the future.
   - Yes, I have sexted before but no longer plan to.
   - No, I have never sexted.
   - No longer in a relationship with the person I sexted with (please elaborate)
   - No longer in a long-distance relationship
   - Not interested (please elaborate)
   - Other: Prefer not to say

3. Why did you stop sexting? (Select all that apply.)
   - No longer in a relationship with the person who I sexted with (please elaborate)
   - No longer in a long-distance relationship
   - Not interested (please elaborate)
   - Poor experience (please elaborate)
   - Other: Prefer not to say

4. How often do you send:
   (Options: Never, Less than once a month, Once a month, Once a week, A few times a week, Almost everyday, Multiple times per day, Almost hourly, Prefer not to say)
   - Nude or semi-nude photos
   - Sexual messages
   - Naked body parts
   - Naked videos
   - Sexual positions

---

Nude or semi-nude videos:

Sexual or intimate messages (such as words or emojis):

5. How often do you receive:
   (Options: Never, Less than once a month, Once a month, Once a week, A few times a week, Almost everyday, Multiple times per day, Almost hourly, Prefer not to say)
   - Nude or semi-nude photos
   - Nude or semi-nude videos
   - Sexual or intimate messages (such as words or emojis)

6. What social media platforms do you use to send/receive nude or semi-nude photos or videos? Select all that apply (or select nothing if you do not send this type of content).
   - Direct Message
   - Private Post
   - Public Post
   - Other: 
   Facebook/FB Messenger, Twitter, Instagram, Snapchat, Other social media app:

7. What other platforms do you use to send/receive nude or semi-nude photos or videos? Select all that apply, if any.
   - SMS
   - Whatsapp
   - Tinder
   - Grindr
   - Hinge
   - OkCupid
   - Signal
   - Telegram
   - Confide
   - Kaboom
   - Dust
   - Other platforms (separated by comma):

8. What social media platforms do you use to send/receive sexual or intimate messages (such as words or emojis)? Select all that apply (or select nothing if you do not send this type of content).
   - Direct Message
   - Private Post
   - Public Post
   - Story
   - Other:
   Facebook/FB Messenger, Twitter, Instagram, Snapchat, Other social media app:

9. What other platforms do you use to send/receive sexual or intimate messages (such as words or emojis)? Select all that apply, if any.
   - SMS
   - Whatsapp
   - Tinder
   - Grindr
   - Hinge
   - OkCupid
   - Signal
   - Telegram
   - Confide
   - Kaboom
   - Dust
   - Other platforms (separated by comma):

10. What devices do you use to send/receive sexts? Select all that apply.
   - Phone
   - Tablet
   - Computer
   - Other

11. With whom do you send nude or semi-nude photos? Select all that apply.
   - Partner
   - Regular sexual hookup (purely sexual relationship)
   - Casual date or one-time hookup
   - Friend-with-benefits
   - Friend
   - Acquaintance
   - New person
   - Other: 

12. With whom do you send nude or semi-nude videos? Select all that apply.
   - Partner
   - Regular sexual hookup (purely sexual relationship)
   - Casual date or one-time hookup
   - Friend-with-benefits
   - Friend
   - Acquaintance
   - New person
   - Other: 

13. With whom do you send sexual or intimate messages (such as words or emojis)? Select all that apply.
   - Partner
   - Regular sexual hookup (purely sexual relationship)
   - Casual date or one-time hookup
   - Friend-with-benefits
   - Friend
   - Acquaintance
   - New person
   - Other: 

14. With whom do you receive nude or semi-nude photos? Select all that apply.
   - Partner
   - Regular sexual hookup (purely sexual relationship)
   - Casual date or one-time hookup
   - Friend-with-benefits
   - Friend
   - Acquaintance
   - New person
   - Other: 

15. With whom do you receive nude or semi-nude videos? Select all that apply.
   - Partner
   - Regular sexual hookup (purely sexual relationship)
   - Casual date or one-time hookup
   - Friend-with-benefits
   - Friend
   - Acquaintance
   - New person
   - Other: 

16. With whom do you receive sexual or intimate messages (such as words or emojis)? Select all that apply.
   - Partner
   - Regular sexual hookup (purely sexual relationship)
   - Casual date or one-time hookup
   - Friend-with-benefits
   - Friend
   - Acquaintance
   - New person
   - Other: 

17. Do you or have you ever saved any of the nude photographs or videos you have received?
   - Yes 
   - No
   - Prefer not to say 
   - Not applicable

18. Why did/do you save them?
   - Directly store to device
   - Screenshot
   - Take a photo
   - Other:

20. What do you plan to do with them?
   - Save them indefinitely
   - Save them for some amount of time
   - Save them until asked to delete them
   - Other: 

21. Approximately how many nudes of other people do you have saved on your device?
   - None
   - 1 to 10
   - 11 to 100
   - 101+
   - Prefer not to say

22. How do you store other people’s nudes? Select all that apply.
   - Device’s photo storage: Camera Roll
   - Device’s photo storage: separate album
   - Online (for example: Google Photos, Dropbox):
   - Specific secret-keeping app
   - Other:

23. Does the person(s) who sent you the nudes know you’ve saved them?
   - Yes
   - Some of the senders know
   - No
   - Prefer not to say

24. Do you store nude or semi nude photos or videos of yourself?
   - Yes
   - No
   - Prefer not to say

25. Approximately how many nudes of yourself do you have saved?
30. How do you manage receiving sexts or nudes from people you do not want to receive them from?
   ◦ Yes (please elaborate how you share): ◦ No ◦ Prefer not to say
31. Do you have any concerns related to sending sexts?
   ◦ Yes (please elaborate below) ◦ No ◦ Prefer not to say
32. If you answered “yes” to the previous question, please elaborate here: What are your concerns related to sending sexts? Or if not, why not?
33. What concerns do you have about sending sexts?
   □ Sexts get around to other people □ Damages relationships □ Conflicts at work □ Legal liability □ Engagement with law enforcement (e.g. police) □ Sexting causes ridicule from others □ Unwanted attention □ Unwanted sexual contact □ Sexts used as blackmail □ Bullying or harassment from others □ Regret □ Sexting makes people feel “led on”, “used”, or “misunderstood” ◦ Not sure I sent it to the right person ◦ Receiver’s devices will get hacked and the content will get out ◦ Receiver will intentionally share the content with others ◦ Other
34. Do you have any concerns related to receiving sexts?
   ◦ Yes (please elaborate below) ◦ No ◦ Prefer not to say
35. If you answered “yes” to the previous question, please elaborate here: What are your concerns about receiving sexts? Or if not, why not?
36. What concerns do you have about receiving sexts?
   □ Not sure if it’s really the person I think it is □ My device will get hacked and their content will get out □ Shoulder surfing □ Receiving unsolicited/non-consensual content □ Other
37. If you don’t have concerns about sexting, why is that?
   □ I’ve done something to manage my concerns □ I trust the people I Sext with □ I trust the platform I use to sext □ I don’t care about how people react to my nudity and sexual expression □ My sexts are already public □ I’m just not really worried about it □ Other
38. Describe your level of concerns related to sending certain types of sexts.
   (Options: Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned, N/A)
   Photo, Video, Text Based
39. Describe your level of concerns related to receiving different types of sexts.
   (Options: Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned, N/A)
   Photo, Video, Text Based
40. You selected that you were concerned about the following when sending sexts: [input]. Do your concerns depend upon the type of person with whom you sext, the type of platform you use, or other considerations?
41. You selected that you were concerned about the following when receiving sexts: [input]. Do your concerns depend upon the type of person with whom you sext, the type of platform you use, or other considerations?
42. Do you do any of the following to manage your sexting concerns?
   □ Choose a platform with specific features you want □ Using disappearing messages e.g. Snapchat, Instagram stories □ Password-protect or encrypt sexts □ Prior conversations to establish rules and boundaries □ Ensuring plausible deniability e.g. not including identifying marks in photo □ Limiting how explicit the sext is □ Only sexting with people you trust □ I do not have any concerns □ I do not have any strategies to manage my concerns □ Other
43. You selected that you use the following strategies to manage your sexting: [input]. Could you please elaborate?
44. Can we use anonymized quotes from your free-response answers in future research publications?
   ◦ Yes ◦ No
45. What gender(s) do you identify as?
   □ Male □ Female □ Non-binary □ Prefer not to say □ Prefer to self-describe:
46. Do you consider yourself transgender?
   ◦ Yes ◦ No ◦ Questioning ◦ Prefer not to say
47. What is your sexual orientation?
   ◦ Straight ◦ Questioning ◦ Gay ◦ Lesbian ◦ Bi/Pan ◦ Queer ◦ Asexual ◦ Prefer not to say ◦ Prefer to self-describe:
48. Do you consider yourself polyamorous or monogamous (regardless of current relationship status)?
   ◦ Polyamorous ◦ Monogamous ◦ Prefer not to say
49. Which racial background(s) do you identify as?
   □ Asian □ Black □ Latino □ Native American □ Pacific Islander □ White □ Prefer not to say □ Prefer to self-describe
50. What is your current intimate status? (Select all that apply)
   - Single
   - Dating
   - Engaged
   - Married
   - Divorced
   - Widowed
   - Friends-With-Benefits
   - Casual sex
   - Casual dating
   - Monogamous relationship
   - Polyamorous relationship
   - Prefer not to say

51. What is your age?
   - 18-24 years old
   - 25-34 years old
   - 35-44 years old
   - 45-54 years old
   - 55-64 years old
   - 65-74 years old
   - 75 years or older

52. What kind of location do you live in?
   - Urban
   - Suburban
   - Rural
   - Prefer not to say

53. Have you ever been in an IT/technology related job?
   - Yes
   - No
   - Prefer not to say

54. I understand how to control or protect my personal data online.
   - Strongly agree
   - Agree
   - Somewhat agree
   - Neither agree nor disagree
   - Somewhat disagree
   - Disagree
   - Strongly disagree

55. What is your education level?
   - GED
   - Some high school
   - Some college/technical training
   - Some graduate school
   - Prefer not to say

B Additional Data on Gender Comparisons

Tables 14 and 15 show the data on gender comparisons for two receiving-related concerns, discussed in Section 4.2.2. The N value for both tables includes all participants who said they receive sexts and who selected at least Male, Female, or Non-binary for their gender.

### Concerned about receiving unsolicited sexts?

<table>
<thead>
<tr>
<th></th>
<th>No</th>
<th>Yes</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>68</td>
<td>7</td>
<td>75</td>
</tr>
<tr>
<td>Female</td>
<td>118</td>
<td>33</td>
<td>151</td>
</tr>
<tr>
<td>Non-Binary</td>
<td>19</td>
<td>5</td>
<td>24</td>
</tr>
</tbody>
</table>

Table 14: N = 242

### Concerned about shoulder-surfing?

<table>
<thead>
<tr>
<th></th>
<th>No</th>
<th>Yes</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>70</td>
<td>5</td>
<td>75</td>
</tr>
<tr>
<td>Female</td>
<td>124</td>
<td>27</td>
<td>151</td>
</tr>
<tr>
<td>Non-Binary</td>
<td>22</td>
<td>2</td>
<td>24</td>
</tr>
</tbody>
</table>

Table 15: N = 242

C Inter-Coder Reliability

Tables 16 and 17 show the breakdown of Cohen’s κ for inter-coder reliability per code, discussed in Section 3.4.

### Concerns About Sending Sexts

<table>
<thead>
<tr>
<th>Concern</th>
<th>κ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only sext with trusted/known person</td>
<td>0.94</td>
</tr>
<tr>
<td>Don’t sext</td>
<td>0.66</td>
</tr>
<tr>
<td>Communicating/establishing rules and expectations</td>
<td>0.90</td>
</tr>
<tr>
<td>Limit explicitness</td>
<td>0.91</td>
</tr>
<tr>
<td>Anonymize sext (no face, tattoos, names, or location)</td>
<td>0.93</td>
</tr>
<tr>
<td>Ask person to delete</td>
<td>1.00</td>
</tr>
<tr>
<td>Acquire collateral</td>
<td>1.00</td>
</tr>
<tr>
<td>Passcode protect image/app/device</td>
<td>1.00</td>
</tr>
<tr>
<td>Disappearing messages</td>
<td>1.00</td>
</tr>
<tr>
<td>Explicitly deleting messages/chat/media</td>
<td>0.66</td>
</tr>
<tr>
<td>Encrypted platforms</td>
<td>0.62</td>
</tr>
<tr>
<td>Screenshot notifications</td>
<td>1.00</td>
</tr>
<tr>
<td>Only send stuff willing to go public</td>
<td>0.49</td>
</tr>
<tr>
<td>Platform choice/Platform affordances</td>
<td>0.88</td>
</tr>
<tr>
<td>Making sure notifications don’t make sexts visible</td>
<td>1.00</td>
</tr>
<tr>
<td>Other</td>
<td>0.82</td>
</tr>
</tbody>
</table>

Table 16: Cohen’s Kappa for codes for elaboration on management strategies for sexting concerns.

### Managing Sending Concerns

<table>
<thead>
<tr>
<th>Concern</th>
<th>κ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact career</td>
<td>1.00</td>
</tr>
<tr>
<td>Sexts will get out (Vague)</td>
<td>0.69</td>
</tr>
<tr>
<td>Sexts used as blackmail</td>
<td>0.87</td>
</tr>
<tr>
<td>Deanonymization</td>
<td>1.00</td>
</tr>
<tr>
<td>Sending to wrong person</td>
<td>0.94</td>
</tr>
<tr>
<td>Bug or vulnerability in app</td>
<td>0.50</td>
</tr>
<tr>
<td>Revenge porn</td>
<td>0.87</td>
</tr>
<tr>
<td>Hacking or stealing</td>
<td>0.92</td>
</tr>
<tr>
<td>Recipient will save sexts</td>
<td>0.83</td>
</tr>
<tr>
<td>End up online</td>
<td>0.73</td>
</tr>
<tr>
<td>Shared/shown to others</td>
<td>0.81</td>
</tr>
<tr>
<td>Seen accidentally by non-recipient</td>
<td>0.77</td>
</tr>
<tr>
<td>Recipient will misuse (Generic, Other)</td>
<td>0.73</td>
</tr>
<tr>
<td>Not concerned because trust partner</td>
<td>0.79</td>
</tr>
<tr>
<td>Not concerned because trust app</td>
<td>0.80</td>
</tr>
<tr>
<td>Not trusting companies</td>
<td>0.72</td>
</tr>
<tr>
<td>Access by government</td>
<td>1.00</td>
</tr>
<tr>
<td>Images will be used to impersonate sender</td>
<td>0.66</td>
</tr>
<tr>
<td>Accidentally posting publicly</td>
<td>1.00</td>
</tr>
<tr>
<td>Judgement from others (also: embarrassing)</td>
<td>0.76</td>
</tr>
<tr>
<td>Insecure network or cloud</td>
<td>1.00</td>
</tr>
<tr>
<td>Photos will be modified</td>
<td>1.00</td>
</tr>
<tr>
<td>Other</td>
<td>0.32</td>
</tr>
</tbody>
</table>

Table 17: Cohen’s Kappa for codes for open-ended question, “What are your concerns related to sending sexts?”