The Sociotechnical Stack: Opportunities for Social Computing Research in Non-Consensual Intimate Media

LI QIWEI, University of Michigan, USA
ALLISON MCDONALD, Boston University, USA
OLIVER L. HAIMSON, University of Michigan, USA
SARITA SCHOENEBECK, University of Michigan, USA
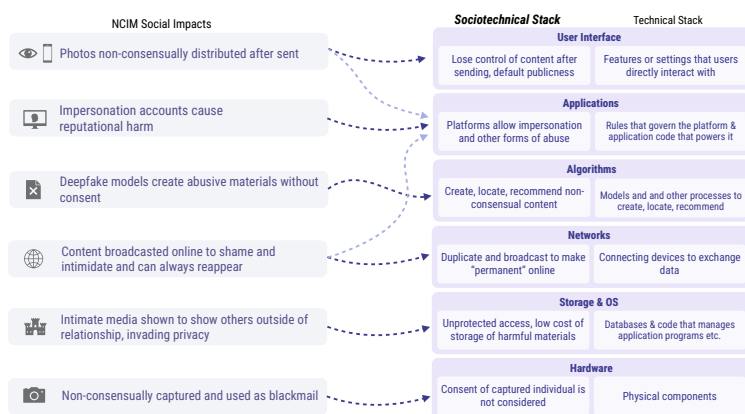ERIC GILBERT, University of Michigan, USA

Fig. 1. The *sociotechnical stack* is a conceptual framework for analyzing sociotechnical problems. It maps social impacts (left) to layers of a traditional technical stack (right). Here, non-consensual intimate media (NCIM) social impacts are analyzed and mapped to corresponding layers in the technical stack. Darker arrows indicate a more direct connection from social impact to stack layer.

Non-consensual intimate media (NCIM) involves sharing intimate content without the depicted person's consent, including "revenge porn" and sexually explicit deepfakes. While NCIM has received attention in legal, psychological, and communication fields over the past decade, it is not sufficiently addressed in computing scholarship. This paper addresses this gap by linking NCIM harms to the specific technological components that facilitate them. We introduce the *sociotechnical stack*, a conceptual framework designed to map the technical stack to its corresponding social impacts. The sociotechnical stack allows us to analyze sociotechnical problems like NCIM, and points toward opportunities for computing research. We propose a research roadmap for computing and social computing communities to deter NCIM perpetration and support victim-survivors[1] through building and rebuilding technologies.

---

[1]Our choice of the term *victim-survivor* reflects that someone has been violated (victim), but is recovering or has recovered (survivor). We adopt these terms and definitions from sexual-abuse activism communities.

Authors' Contact Information: Li Qiwei, University of Michigan, USA, rrll@umich.edu; Allison McDonald, Boston University, USA, amcdon@bu.edu; Oliver L. Haimson, University of Michigan, USA, haimson@umich.edu; Sarita Schoenebeck, University of Michigan, USA, yardi@umich.edu; Eric Gilbert, University of Michigan, USA, eegg@umich.edu.

CCS Concepts: • **Human-centered computing → Collaborative and social computing theory, concepts and paradigms**.

Additional Key Words and Phrases: social computing, online sexual abuse, sociotechnical systems

1 Introduction

Content warning: This paper talks about online sexual abuse.

Non-consensual intimate media (NCIM) is the unauthorized creation, sharing, or distribution of sexual content containing someone's body or likeness. This form of online abuse usually targets women, who constitute about 90% of all cases [1, 33, 53]. NCIM cases can be varied, ranging from sexually explicit deepfakes, to covert recordings, to sextortion (See Fig. 2). NCIM is common—studies suggest 1 in 6 adults have had their intimate content shared without consent [77, 81]. NCIM is also deeply traumatic—almost all victim-survivors experience severe anxiety and depression. About half seriously consider ending their own lives, and in some cases, women and girls commit suicide to escape emotional pain and social shame [26, 33, 53]. While there is widespread agreement that NCIM is harmful and some agreement that it should be regulated, there is less consensus on *how* to do so [22, 23, 28, 35]. The law is evolving to recognize NCIM, but access to legal recourse is limited and cannot prevent continued re-distribution. Victim-survivors may request content removal directly from platforms, but these efforts are typically laborious, emotionally taxing, and frequently futile due to the diverse jurisdictions governing online platforms [28, 66].

Effectively addressing NCIM requires both sociotechnical and computing research. Sexual abuse and patriarchal socio-historical conditions have enabled power and domination of others, typically women, via sex and intimacy. However, new technology has weaponized this at an unprecedented scale.

This paper highlights the essential links between NCIM and its enabling technical components. Drawing on existing surveys and interviews with more than 400 victim-survivors, we identify a critical gap: technologies, including social media platforms, file formats, and content recommendation algorithms, do not merely enable but actively *create* NCIM at scale. To systemically analyze this, we introduce a conceptual framework called the *sociotechnical stack*. In software engineering and computer science, a "tech stack" refers to a layered structure of technologies used to build systems, like the TCP/IP protocols in computing networking. We extend this concept to include *social impacts*, integrating the technical and social dimensions of systems. Our analysis shows how certain layers, such as a content recommendation algorithm, can unintentionally promote NCIM. The sociotechnical stack illustrates the ways our digital environment facilitates risks and harms for NCIM victim-survivors, including the non-consensual creation of sexual content via generative AI and unauthorized redistribution of privately shared intimate media. We propose a roadmap for sociotechnical research to address NCIM and alleviate risks for victim-survivors.

This paper's main contributions are:

- **The sociotechnical stack conceptual framework:** Intended for analyzing social computing issues, the sociotechnical stack framework breaks down complex sociotechnical problems into specific technical components that contribute to social impacts and harms.
- **A sociotechnical analysis of NCIM:** This analysis sheds light on how various elements of the technical stack facilitate NCIM. We identify gaps in the current research on NCIM and demonstrate how adopting a sociotechnical perspective can help address these issues.

• *A research agenda for NCIM:* Finally, we propose important areas for further computing research on NCIM, at different layers of the sociotechnical stack.
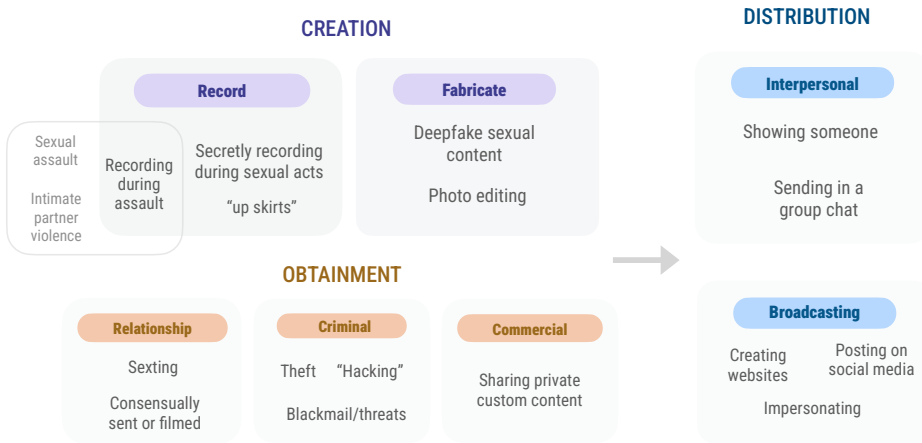

Fig. 2. Non-consensual intimate media (NCIM) creation, obtainment, and distribution.

2 Overview of NCIM

The essence of NCIM revolves around the concept of consent—or its absence. Defined as permission to engage in specific activities, consent in sexual contexts means agreeing to engage in particular sexual acts. However, consent transcends mere agreement; it is a dynamic practice influenced by societal norms and power dynamics [92]. The concept of consent, both within and beyond sociotechnical studies, is complex, nuanced, and frequently debated. The debate extends into how consent is obtained, maintained, and revoked; for example, affirmative consent requires ongoing, explicit agreement from all parties, emphasizing a "yes means yes" standard over the traditional "no means no" [47, 99]. However, this approach has been criticized for not capturing non-verbal cues and ignoring the complexities of sexual power dynamics [57, 96].

Violations of consent can happen at many points in the lifecycle of NCIM. Critical moments in NCIM include content *creation* (e.g., filming through covert cameras or using generative AI models to "nudify" someone), *obtainment* (e.g., with media initially sent during intimate messaging), and *distribution* (e.g., unauthorized sharing via direct messages or public online platforms) (see Fig. 2). Even content initially shared consensually within private contexts can lead to NCIM if shared beyond intended bounds. The impact ranges from isolated incidents to widespread distribution, affecting victim-survivors differently. For instance, sharing a photo with a friend may breach privacy, though without the intent to harm the subject, while uploading to a "revenge porn" site is a deliberate act of injury.

NCIM's prevalence is extensive and likely underreported, compounded by technical challenges in detection and social stigma that deter reporting. One 2017 survey found that 5% of respondents admitted to non-consensually sharing intimate photos [33]. This almost certainly undercounts people who consume NCIM online. A 2014 study estimated around 11,000 websites hosted non-consensual content—a figure that has likely grown [19, 33, 53]. These sites range in character and include those dedicated to photos of "up skirts" (photos taken up a person's legs in public); contests (e.g., which user-uploaded photos get the most likes); trades (treating victim-survivors like baseball cards); or solicitations (in which users ask for photos of someone); and many others [21, 33, 66].

The consequences of NCIM are severe, and a significant majority of victims experience emotional and social repercussions: 93% of NCIM victims experience considerable emotional distress, 82% encounter disruptions in their social and professional lives, 42% seek psychological treatment, and 51% have contemplated suicide [36, 53]. Many face ongoing harassment, including the exposure of their personal information and intimate media online. Such actions not only perpetuate their trauma but also lead to a profound sense of powerlessness against the continual resharing of their content [20, 21, 33, 53, 66].

Addressing NCIM through legal channels has proven challenging, with systemic biases often discouraging victim-survivors from pursuing lawsuits. Many victims refrain from reporting due to past failures of systemic protection and potential for further harm [12, 21, 89]. The financial burden of civil lawsuits further restricts access to justice, leaving many without recourse. The emotional and social impact of NCIM deeply affects how victims are perceived and treated across various societal dimensions, including in employment and legal settings [21, 33, 53, 83].

3 Related Work

Next, we review NCIM scholarship and related CSCW research in greater detail. Despite overlap with established sociotechnical research domains like content moderation, online harassment, and digital consent, current research often falls short in tackling the unique challenges presented by NCIM. Likewise, NCIM work in law, privacy, psychology, usable cybersecurity, and communication offers important insights; however, they usually have limited engagement with NCIM's technical underpinnings. We outline these gaps as significant opportunities for addressing NCIM as a sociotechnical issue.

3.1 Legal lenses of NCIM

A few prominent U.S. legal scholars have strongly advocated for more robust protections against the non-consensual sharing of intimate content. This advocacy has contributed to the proposal and enactment of NCIM laws at the state level in nearly all states [7, 17, 20, 91]. Legal protections stipulate that the victim must be identifiable from the material, the material was intended to remain private, and that consent for its distribution was not given [21]. Dissemination of sexually explicit material is typically a misdemeanor if the image was taken or accessed consensually but then distributed non-consensually. If the images were obtained non-consensually, criminal charges could also include a felony for unlawful surveillance. More recently, Congress established a private right of action, enabling individuals whose intimate images were disclosed non-consensually to file a federal lawsuit against the discloser [14, 27].

Although these laws mark significant progress in combating NCIM, there are still substantial hurdles. Laws in a vacuum cannot immediately halt widespread dissemination, prevent personal information from appearing on abusive websites, or assuage emotional trauma. Civil lawsuits are very expensive, prohibitively so for those who do not have ready access to lawyers and high retainer fees. In criminal cases, victim-survivors may also not trust the legal systems in the domain of sexual harms [12, 20, 82]. Beyond these laws, the primary alternative for redress is the Digital Millennium Copyright Act (DMCA), which enables copyright owners to request the takedown of infringing content [20, 45]. However, this approach is only viable if the victim took the photo themselves and can prove it—for instance, by providing a link to a publicly accessible version of the content, a method more suited for creative works than to intimate content. It also requires that the website be responsive to copyright takedown requests; many are not.

3.2 Empirical studies of NCIM

Empirical psychology studies, including surveys and interviews, offer crucial insights into the prevalence and impact of NCIM [101]. Psychological research has explored the extent of victimhood— how common NCIM is [74], the impacts of this violation on mental health [5, 102], and the factors that contribute to the perpetration of NCIM [24, 86].

Communication and gender studies scholarship frequently apply feminist theories to analyze NCIM as a form of gendered violence, aligning it with other abuses targeted at women and gender minorities [13, 49, 69]. Previous research has detailed the range of harms experienced by victim-survivors, including emotional, economic, practical, social, and psychological impacts [32, 44, 51, 83]. Studies have also examined attitudes towards NCIM, particularly people's allocation of blame between victim-survivors and perpetrators [49]. Research has also addressed the factors leading to NCIM perpetration. Content analyses of revenge porn websites have highlighted the significant role of the performance of masculinity in the illicit sharing of content [31], as well as reporting mechanisms for NCIM on technological platforms [28].

Despite the valuable insights provided by these studies, they often are limited to the human/social/societal aspects of the issue. Moreover, while they offer detailed descriptions and analyses of the problem, there is a notable lack of focus on developing solutions for victim-survivors. This gap highlights the opportunity for research that interrogates technological strategies to mitigate NCIM's impact.

3.3 Challenges in addressing NCIM

3.3.1 Privacy and cybersecurity. Privacy and cybersecurity research characterizes NCIM as a significant privacy challenge. Previous studies have examined safe sexting practices [25, 41], attitudes toward security in intimate partner sharing [73], and defenses against intimate partner violence [15, 37, 97], such as cyberstalking and blackmailing. This body of research underscores the complex social dynamics involved in sharing intimate content and managing threats like intimate partner violence [38, 61, 97].

The concept of contextual integrity in information management suggests that once information is shared, individuals become co-managers of that information [71]. From this perspective, NCIM represents a mismanagement of co-managed information. Privacy research has also led to the development of systems designed to enhance visual privacy online. This research includes managing social media photos to obtain consent programmatically [72], photography in public spaces [9], and preventing unwanted screen photography, screenshotting, and screen-recording [4, 46, 55, 104, 105].

Despite these advancements, research specifically addressing the unique concerns of NCIM remains scarce. Traditional computer science and security approaches often overlook issues related to misogyny and the abuse of women and girls [98, 101]. To address this gap, our work focuses on the specialized privacy needs of victim-survivors when using technologies, exploring how better-designed systems can support their rights and well-being.

3.3.2 Content moderation. Online social platforms are a central locus point for NCIM harms, including doxxing, harassment, and privacy invasions [5, 22, 53]. While Social Computing frequently speaks to online harassment and content moderation, current policies and practices often fail to adequately address NCIM issues.

Research has shown that platforms struggle to protect users from online harassment, with policies often being inconsistent and responses vague [6, 54]. Implementing generic solutions has proven impractical, leading many users to distrust the platforms' ability to effectively manage online harassment [84, 85]. In response, individuals and communities have developed various strategies to mitigate abuse. These include creating collective blocklists [42, 54], classifying and

labeling harassment [6], sharing anti-harassment tools through networks [68], employing auto-moderators or third-party bots [100], and enhancing the visibility of community norms [64]. Despite these efforts, managing online harassment remains a significant emotional burden, particularly for marginalized groups [100].

However, despite the critical importance of content moderation for NCIM, there is a notable absence of studies on how content moderation are applied to NCIM in reality.

3.3.3 Technical interventions for consent. In CSCW research, consent is crucial for developing systems that support sexual intimacy and well-being [48, 58, 70, 93, 106]. Consent in technology is also vital for ensuring agreement, access, and autonomy among users, their data, and other entities in the digital landscape [62]. However, existing systems addressing non-consensual content are limited in both scope and capabilities. Currently, the few systems in place primarily utilize hashing algorithms to focus on a subset of content types, including copyright infringement and child sexual abuse material. These algorithms convert content into a unique string, functioning as a one-way identifier. This means that while anyone can generate the hash from the original content, reconstructing the original from the hash is nearly impossible. This technique is widely used on platforms like YouTube and Twitter to identify and prevent copyright infringement. As another example, one well-known system, PhotoDNA, is used by many platforms to detect and block the distribution of illegal or unauthorized online content, including terrorism and child pornography [34].

StopNCII is a rare system developed specifically for NCIM. It is a hashing-based system initially adopted by Meta to block unauthorized intimate photos from being uploaded to their platforms. Although StopNCII represents a significant step forward, it is similarly severely limited by its dependence on platform participation. Other platforms like WhatsApp and Telegram have introduced features that prevent screenshots and alert senders about attempts, which may deter unauthorized content captures [1].

Despite these developments, systems to combat NCIM are limited. There are significant opportunities for system-building work to address NCIM at its roots. Specifically, we propose expanding on existing work to develop more robust systems tailored to the unique challenges of NCIM, enhancing both detection and prevention capabilities.

4 The *sociotechnical stack*

We introduce the *sociotechnical stack*, an analytic device spanning social and technical realms, which allows us to pinpoint how technological components contribute to social problems. The sociotechnical stack is an extension of the conventional "technology stack" or "tech stack," which is an abstraction used to describe the components that build an application—from hardware at the bottom, through the operating system, to the user interface at the top. See Figure 1 and Section 6 for further details. The sociotechnical stack integrates technical artifacts with social impacts, where each layer, while achieving a technical goal, also facilitates subsequent social impacts given specific contexts. This framework is particularly crucial in contexts with high societal importance like NCIM, where each layer in the stack plays a role in perpetuating harm, illustrating how technical design decisions can have profound social consequences.

The hierarchical nature of the "stack" metaphor suggests that solutions could be applied at various levels. Addressing an issue like NCIM at a lower layer—such as hardware—can potentially resolve it at higher layers like the network or user interface. This holistic view encourages comprehensive solutions that move across the stack. As a conceptual framework, the sociotechnical stack is adaptable to specific system designs. For instance, in distributed computing, the stack might emphasize the network's role in task completion. In a decentralized architecture, the stack might

focus on enhanced user control over content by allowing users rather than platforms to decide on content removal. The decentralized approach could empower users, or communities of users operating as nodes, to manage intimate content but might complicate efforts to control illicit redistribution. At any level and with any technical design choice, the sociotechnical stack lens demonstrates the need to tailor technical stack components to prioritize social impacts on users.

The sociotechnical stack concept can extend beyond NCIM to address other social computing challenges where important social impacts are shaped and mediated by multiple layers of the stack. Take the problem of disinformation as a case study. Disinformation is information that is deliberately false or misleading, often perpetuated as a campaign for political purposes [40, 103]. A sociotechnical stack analysis could identify how layers of the sociotechnical stack enable the sharing and spread of disinformation. At the hardware level, there could be provenance of content capture and distribution (e.g. a photograph taken at a protest). At the storage level, there could be databases of prominent disinformation campaigns that would enable cross-platform collaboration. As with NCIM, a substantial challenge is in developing criteria and policies to agree on what qualifies as disinformation [103]. At the network and algorithm levels, there could be trusted or trustworthiness protocols to deter well-known disinformation campaigns (e.g., Russian trolls in American political campaigns [40]). At the application level, there could be cross-platform coordination in content moderation, rather than requiring that each platform detect and verify disinformation on its own, an expensive task. Finally, at the user interface level, there could be procedures to deter sharing disinformation content, while preserving speech and privacy rights.

A sociotechnical stack analysis could be applied to other problem domains, ranging from bias in large language models to building accessible interfaces to surveillance with facial recognition technologies. The sociotechnical stack approach is useful for domains with large-scale social impacts that are shaped by design choices up and down the stack. Though this paper focuses on the problem of NCIM, Figure 3 provides a template for a visual sociotechnical stack analysis in other domains.[2]
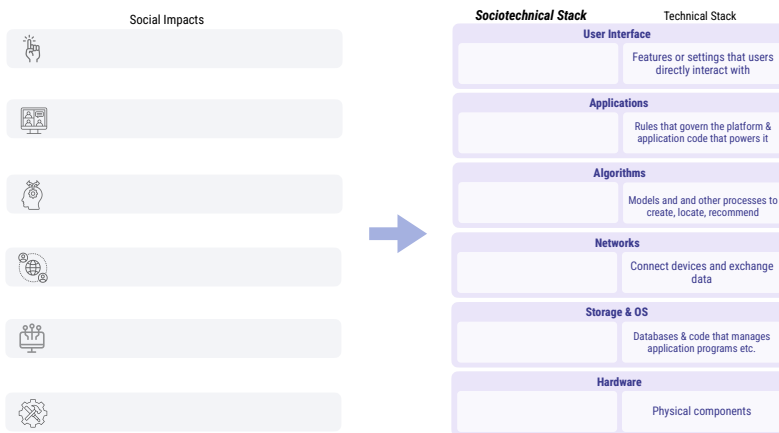

Fig. 3. The conceptual framework *sociotechnical stack* maps social impacts to the layers of the technical stack that facilitates or enables them. We share downloadable versions in PowerPoint and Keynote.

---

[2]A link to the template for reuse is available here for PowerPoint and Keynote.

5 Data Sources

Narratives provide critical insights into the technical mechanisms that facilitate and perpetuate NCIM. To gather evidence and deepen our understanding of NCIM, we review prior works for firsthand accounts of victimization, utilizing interviews, quotes, and vignettes. We then employ a reflexive inductive thematic approach to explore *sociotechnical* themes in these narratives, aiming to connect the technological components with the lived experiences of victim-survivors. We address the significant gap identified in previous sections: the lack of focus on the technologies that enable these violations [101]. We address this gap by analyzing how technologies translate into the lived harms of victim-survivors, posing questions such as "How did technology facilitate the emergence of these experiences?" and "How did technology itself deliver these harms?"

To develop our vignette collection, we performed a literature review focusing on qualitative research related to non-consensual intimate imagery (NCIM). Using the search terms "image-based sexual abuse", "online sexual abuse", "sexting", "revenge pornography", "intimate partner violence", and "non-consensual intimate imagery", we searched ACM Digital Library, ProQuest Research Library, PsycINFO, and Communication & Mass Media Complete databases. The first author selected studies rich in interview data and first-person accounts that detail the impact of NCIM, prioritizing narratives that provide deep and personal insights into harms. This includes interview studies that documented direct quotes from victim-survivors, and reports that contain stories and quotes from victim-survivors. We excluded the majority of legal reviews and quantitative studies due to the lack of focus on personal narratives. We developed hierarchical codes of the interview text in the published articles. The hierarchical codes later became the themes detailed in Section 6. The selected articles were reanalyzed to highlight *how specific technologies facilitated and created these narratives and harms*. The result is a focused yet rich sample of victim-survivor experiences that illustrate how technology directly enabled NCIM. The sources for the vignettes and quotes are:

- An interview study of 75 victim-survivors' experiences with NCIM [50, 66]
- A report drafted for legislators for stronger NCIM laws, including a survey on 361 victim-survivor experiences conducted by the Cyber Civil Rights organization [36, 53]
- An interview study of 18 victim-survivors focused on mental health [5]
- An interview study with 18 adults who have experienced sextortion [102]
- A report on activists' and sex workers' experiences in social media content moderation [8]
- A report containing deepfake abuse survivor testimonies [26]
- An interview study on sex-workers' privacy management strategies [65]

5.1 Vignettes

This section contains vignettes and quotes to illustrate the interplay of the sociotechnical stack's layers, enhancing our understanding of how each component contributes to NCIM harms. Vignettes are selected for their ability to explore these interactions in depth and serve as comprehensive illustrations of the sociotechnical stack in action. Vignettes draw out connections between *multiple* layers, offering a holistic view of the sociotechnical dynamics at play. They serve as emblematic victim-survivor experiences and will be referred to by their icons and will be used in subsequent analysis in Sections 6 and 7. Technology interactions are highlighted in the vignettes through underlining to emphasize these elements. Quotes in subsequent sections will provide more direct mappings to *specific* layers of the sociotechnical stack.

✉ "She and her ex-boyfriend had exchanged intimate photos throughout their three-year relationship, but she had never thought that he would use them to destroy her life . . . her pictures were on over 200 websites and she had been inundated with unwelcome sexual propositions from men who

had seen them. The pictures had also been <u>sent to her boss and a co-worker</u>. [She] spent the next few months trying to explain the situation to her employer, her family, her friends, and colleagues, and to <u>plead with porn sites and search engines to remove her material</u>. Even after removing the photos, <u>within two weeks her material was up on 300 websites</u>. At that point, [she] gave up trying to change her search results, and started the process to change her name. She couldn't see any other way to escape the material that was <u>following her everywhere</u>, jeopardizing her career, her psychological health, and her relationship." [36]

◾️ "Her ex-husband brought her to a hotel room and drugged her. She had no memory of what happened, but later found out that he and another man had raped her. She divorced him shortly after, and seven months later he <u>sent a video containing footage of the rape</u> to the school board where she worked. She was fired from her job as a school superintendent immediately after the <u>video was sent to her colleagues</u>, and the police were still investigating the rape at the time of the interview." [5]

🌐 "[She] found <u>deepfake videos</u> of herself on various <u>4chan threads</u>, alongside <u>information about her college, name, and local area</u> ... At first [she] started receiving a bunch of <u>Snapchat notifications from people adding me</u> ...and someone replied that <u>someone posted my Snapchat on 4chan</u>." [26]

6 NCIM Along the sociotechnical stack

This section examines how each layer of the sociotechnical stack enables NCIM harms and shapes the experiences of victim-survivors. To illustrate the complex interactions and downstream social consequences at each layer, we incorporate victim-survivor quotes and vignettes from sources mentioned in Section 5.

Interactions within the sociotechnical stack require all layers to work in concert, much like how searching an online catalog involves the user interface, network instruction delivery, and database queries. Similarly, harms facilitated by the sociotechnical stack are distributed across its multiple layers. Thus, the focus of our analysis is not to isolate harms to a specific layer but to *identify key technical components* within each layer that lead to specific social outcomes. We aim to highlight how changes at any single layer can influence the entire system, potentially mitigating or exacerbating NCIM harms. This approach allows us to provide a comprehensive view of the sociotechnical dynamics at play, offering insights into how technological design and implementation can be altered to reduce the incidence and impact of NCIM.

6.1 User interface

The user interface (UI), as the top level of the technical stack, enables direct interaction and manipulation by users. It encompasses the visible elements of applications and includes features and settings that users can adjust. Crucially, the UI can facilitate NCIM harms by enabling loss of control over intimate media once sent, setting social media profiles to public by default, and allowing visible social networks to be used for malicious purposes.

6.1.1 Loss of control over content after sent. Online sharing of media results in the transfer of possession to the recipient, who can permanently save the content through various methods such as screenshots or screen recordings [78, 79, 88]. Sharing intimate media, however, requires careful consideration of trust and reciprocity, as senders must navigate intimacy and negotiate trust [41]. This aspect of UI design often lacks mechanisms to prevent the unauthorized sharing of intimate media, despite the trust placed by the sender. A poignant example is provided by a victim-survivor's testimony:

> *"I sent this photo of my breast to this particular person. And they asked for more and more and more. I sent these pictures ... to this guy who I'd been seeing for months and months ... That's when he told me that he showed three of his friends what I'd sent him."* [50]

This quote underscores the ease with which trust can be violated and the profound impacts of such breaches, highlighting the need for enhanced protections.

6.1.2 Visible social networks. Victim-survivors often see their social networks used against them. On many platforms, social networks are publicly visible. Perpetrators exploit these visible connections, using publicly available information to tarnish reputations. The following account illustrates the misuse of visible social networks for intimidation and harassment:

> *"He told me he would take what [intimate photos] he had and show all my friends and put them on MySpace and all that and send them to other people in town."* [102]

This narrative not only highlights the direct threats faced by victim-survivors but also reflects a broader theme of exploitation that permeates many NCIM incidents, where personal and professional networks are abused to extend harm. Similarly, the perpetrator in ✉ emailed her intimate photos to numerous contacts within her social and professional networks; 🎥 had videos sent to her work colleagues.

6.1.3 Default publicness. Default publicness in social media design privileges "a heteronormative assumptive posture of public expression" [18]. This makes personal information easily accessible and users readily reachable, sometimes directly enabling harassment. Online abuse among NCIM victim-survivors is prevalent and widespread; forty-nine percent report being harassed or stalked online by users who have seen their material [53]. As a result, many victim-survivors are compelled to create new online identities to escape harassment and feel safe [50]. The public display of even basic personal information poses a safety threat [10, 66, 67]. This exposure often leads to anxiety among victim-survivors, who fear unsolicited contact such as *"Getting messages on Facebook from people I'd never met, telling me I had a nice body"* [50]. Many view subsequent online experiences as threatening, further isolating NCIM victim-survivors [66]. The anxiety about being contacted via social media is profound, leading some to withdraw completely:

> *"I don't really have an online presence anymore because I'm just so terrified of ... people contacting me because they've seen these pictures."* [66].

These accounts highlight the need for a critical re-evaluation of privacy and consent mechanisms within UI design to better protect individuals from the far-reaching consequences of NCIM.

6.2 Applications

The application layer of the sociotechnical stack includes video hosting sites, social media platforms, mobile applications, and online forums. It consists of the rules, policies, and code that enable these platforms [63]. This layer can facilitate NCIM harms through mechanisms such as impersonation and by providing a space for knowingly hosting non-consensual content.

6.2.1 Impersonation. The lack of stringent account verification on platforms facilitates abuse, including the creation of fake accounts, impersonation, and falsified posts. These tactics can be used maliciously to harm others, as illustrated by the following case:

> *"They were a couple and she sent him photos, and then when they split up he set up a Facebook account with her name and he uploaded the photos to screw with her ... from here and from the surrounding towns, it always tends to become public knowledge."* [75]

This quote highlights how social media platforms can be exploited to falsify identities, leading to significant social damage and public humiliation.

6.2.2 Abusive platforms. Platforms such as Reddit, Discord, 4chan, and Telegram are known to host forums and groups that are notorious for creating and sharing non-consensual sexual content [26]. These platforms often serve as venues for the distribution of NCIM, exploiting their relative anonymity and community features. 🌐 involve these platforms, showcasing how they facilitate the sharing of non-consensual content. Traditional content moderation techniques on larger platforms often prove insufficient, as harmful communities may simply migrate to less moderated platforms to continue their activities unchecked. This migration poses significant challenges in controlling the spread of NCIM and underscores the need for robust moderation practices across all platforms, not just the major ones [95].

6.3 Algorithms

Algorithms include generative AI models for creating new content, recommendation algorithms that inadvertently promote non-consensual content, and search engine algorithms that facilitate access to abusive material.

6.3.1 Deepfakes. 2023 saw more deepfakes created than in all previous years combined [26]. The advent of "nudify" models and their widespread availability have made it easier for perpetrators to generate and disseminate harmful content. The following quote illustrates the profound distress experienced by an individual whose altered images were circulated:

> *"People were messaging me because they found me on a porn website . . . my name and my face were on there . . . my school and my hometown were also on there . . . oh my God, these videos had thousands of views on them. Hearing that the next time someone's in your hometown, they're going to fuck you. It's just terrifying."* [26]

This experience highlights the severe social repercussions of deepfakes, demonstrating how quickly and extensively damaging content can spread, impacting personal security and mental health.

6.3.2 Content recommendation algorithms. Content recommendation algorithms aim to maximize views, likes, and shares. However, without mechanisms to discern consensual from non-consensual content, these algorithms can inadvertently distribute harmful material widely, a frequent issue on both mainstream and adult platforms. No safeguards currently prevent the circulation of content that may constitute sexual abuse. For NCIM victim-survivors, this distinction marks the difference between isolated harm and pervasive abuse.

These algorithms also compromise privacy by recommending accounts. Consider the experience of a sex worker who tried to maintain separate personal and professional:

> *"I wanted a second account with Facebook [for clients to interact with me]. I had a different email address . . . I didn't want my friends to see it at all, but they were suggested to me [by Facebook] immediately . . . [so] I just deleted it right away."* [65]

This quote illustrates the privacy challenges individuals face due to the invasive nature of content recommendation algorithms, which can inadvertently expose sensitive aspects of a person's life to unintended audiences, leading to potential social and professional harm.

6.3.3 Search engine algorithms. In ✉ the victim-survivor had to undertake the laborious process of manually requesting search engines to deindex abusive content featuring her. This example illustrates the critical need for more proactive and victim-centered approaches in search engines to prevent the easy accessibility and perpetuation of abusive material online.

6.4 Networking and the internet

Networks connect devices, making online content potentially permanent due to widespread duplication.

6.4.1 Near-infinite replication and spread. Online content is duplicated for reasons both malicious and benign. Websites are often archived or automatically cached. Data scrapers harvest content from sites such as Reddit to boost traffic. Such practices underscore the challenge of online permanency: once posted, content may never be fully removable.

The internet is involved in most NCIM cases, as images are distributed one-to-one on messaging applications or broadcast to a wide audience [5]. Completely removing content from the internet is nearly impossible, a fact of which victim-survivors are painfully aware. These statements poignantly capture the enduring nature of online content:

> *"There will never be a day in my entire lifetime that all the images of me could ever be deleted . . . It's a crime that doesn't just happen and then that's done. It's something that is continual, and this could continue for I don't know how long."* [66]

While victim-survivors strive to control the spread of NCIM, they also grapple with the reality of the internet's permanence. A significant 54% fear discovery of the material by their children or future descendants [53], leading to profound emotional distress and ongoing trauma.

> *"[It's become] a hidden obsession to always check my phone...and that's kind of become the way that I've coped with it, constantly checking my phone, to the detriment of my work."* [50]

6.4.2 Broadcasting. Websites facilitate the broadcasting of abusive materials. For instance, a perpetrator created new websites specifically to harm his ex-girlfriend.

> *"Her ex-boyfriend posted an eBay auction for a disc containing naked photos of her, which she successfully had taken down from eBay. However, a year later, he created a porn website with the naked photos of her, which included her full name, the name of her town, the name of the college she taught at."* [5]

Despite efforts by victim-survivors to remove content, media is frequently re-uploaded. Even with some measures in place on eBay to address abuse, the victim-survivor could prevent neither doxxing nor the public display of the content she attempted to remove. The inherent capabilities of the internet make it a challenging domain to control [63]. Victim-survivors often feel helpless and trapped, tormented by the knowledge that their images are "out of [their] control" and "hanging over" them [66].

6.4.3 Data provenance. Data provenance concerns the origin, migration, and current location of data, posing critical questions for victim-survivors addressing privacy violations. Individuals often find themselves involuntarily playing a "guessing game," forced to construct complex mental models to discern which social interactions might be safe. This necessity arises from their need to manage potential negative perceptions among those who may have seen their sexual images, as they "hyper-analyze all of their social interactions" [66]. The misuse of data extends into the realm of AI models, where non-consensual media are included in the training sets. This misuse initiates a new cycle of victimization, with these images being repurposed to develop deepfake models that facilitate further abuse.

6.5 Storage and OS

6.5.1 Files. A fundamental challenge with digital privacy begins at the level of file design and storage systems, which currently do not support the revocation of consent. Sexting lacks the privacy

typically associated with physical intimacy. Despite agreements to keep shared photos private, digital systems facilitate their unauthorized circulation and duplication. Many people desire their ex-partners to delete intimate content post-breakup, yet there's no foolproof method to enforce such deletion [25].

> "I guess it was the thing to do, like you share nudes with your partner or boyfriend, and we broke up …We didn't end on very good terms …he [sent the photos around the school] and everyone kind of got my photo during class." [50]

This quote from a victim-survivor illustrates the lack of control over digital content once shared, even within trusted relationships. The inability to enforce digital privacy after a relationship sours shows a critical vulnerability in digital consent, exacerbating the risk of NCIM when intimate photos are misused. In broader social interactions, consent is often implicitly negotiated and nuanced, subtleties that current files fail to protect [2, 62].

6.5.2 Price of storage. Perpetrators of NCIM exploit cheap storage for blackmail and abuse [5, 66]. The cost of storing digital content, such as videos and images, is minimal. This affordability means that once someone obtains a copy of content, they are likely to retain it indefinitely. There are few incentives for deletion. Unlike digital storage, physical storage incurs costs. Storing physical photographs in a photo album will ultimately run out of space.

6.6 Hardware

Cameras play a crucial role in NCIM. NCIM may arise from recordings initially made with consent (intended to remain private) or during acts of sexual assault, as depicted in ◼. In other situations, recordings are made surreptitiously, without the person's awareness and without other crimes being committed. For instance, one ex-boyfriend set up covert cameras around the victim-survivor's home to film her [5]. Nonetheless, individuals do not consent to the recording because they are not aware of it. Other times, victim-survivors consented to sexual acts but did not consent to recording:

> "I didn't realize there was another friend who had managed to video me …peeked in the door, stuck a phone or something. He filmed me performing a sexual act on the person and then put it on Facebook." [50]

These document violations of consent and the illicit usage of recording devices on a vulnerable and unaware person.

7 Roadmap for NCIM Research

As the final contribution of this paper, we present a research roadmap for NCIM. This roadmap builds directly on the gaps identified in our previous analysis, particularly the need for more computing research. It draws on insights derived from the sociotechnical stack and the narratives captured in victim-survivor quotes.

We use the sociotechnical stack as a framework to identify and explore potential research areas to reduce the harms associated with NCIM. By systematically examining each layer of the sociotechnical stack, we propose targeted interventions that could diminish the technical capabilities that currently facilitate NCIM. This includes innovating privacy safeguards, enhancing content moderation frameworks, and developing more robust consent mechanisms within digital platforms. This research agenda aims to bridge the gap between technical potential and social necessity, focusing on transforming how social computing and related fields can respond more effectively to the challenges of NCIM. No technology will eliminate the harms of NCIM; rather, the intent here is to significantly reduce harms using sociotechnical approaches.

7.1 Research in user interfaces

7.1.1 Communicating consent. The process of intimate sharing online often lacks explicit, codified expressions of preferences regarding the handling of content after the fact. More critically, even when senders stipulate that materials remain private between partners, these preferences are frequently disregarded. A novel approach could allow senders to specify their preferences at the interface layer and incorporate protective mechanisms down the stack to enforce preferences at the recipient's end. How could people communicate those preferences, and how could they stay with the media as it moves through various systems?

Possible methods for designing this elicitation include participatory design, which centers on the needs and desires of the communities involved in the design process, and speculative design, which promotes creative and radical thinking [3, 80]. Studies at the intersection of human-centered computing and sexual health have explored how interactions can be designed to support sexual well-being [11], the mediation of consent through technology [52, 107], and the effects of social media on sex work and sex-positivity.[3] Future research can consider the flexibility and contextual constraints of preference elicitation features. For example, once a privacy preference has been expressed at the UI level and is implemented in the application, how can a *possible revocation* of prior consent be designed?

7.1.2 Limiting the attack surface. Security research [41, 71] indicates that people use various strategies to limit the exposure of personally identifiable information during intimate sharing. There is a need to integrate these insights into the design of platforms to better support privacy. In the development of messaging platforms, designers may consider elements important to intimate sharing, such as fostering trust and enabling the creation of private channels [2, 76]. Additionally, introducing new social sharing modalities can provide users with more flexible, controlled, and secure options for both sending and receiving content.

7.2 Research in applications

7.2.1 Content moderation and takedowns. Content moderation encompasses a wide range of activities aimed at mitigating harmful content on platforms, including harassment and misinformation [43, 94]. Key questions at the intersection of NCIM and content moderation involve identifying non-consensually shared content, supporting victims in requesting content takedowns, and establishing regulatory requirements for companies to manage NCIM effectively. While many websites have community guidelines that regulate user behavior, not all have specific policies addressing non-consensual content sharing, and even those that do may lack enforcement procedures [28]. The process for victim-survivors requesting takedowns of NCIM content lacks transparency, leaving many unsure of the outcomes.

Further research may study how content circulates through online communities. Misogyny and toxic masculinity are prevalent online and may intensify when combined with graphic and traumatic imagery [56]. Techniques such as nudging have shown effectiveness in fostering healthier behaviors in online settings, suggesting potential applications for deterring the spread of NCIM. However, research also indicates that awareness of the non-consensual nature of sexual content may *heighten* toxic masculine behaviors and motivate further consumption [29, 30]. This area demands careful consideration of the balance between social and antisocial behavior.

7.2.2 Trauma-informed social computing. Those impacted by NCIM may be seeking recovery in a complex emotional state, requiring support that is trauma-informed [16]. Online experiences that were previously mundane may now become traumatizing. Research may explore how to design

---

[3]https://sexpositivesocialmedia.org

interfaces that minimize triggering experiences following trauma. This problem is not limited to NCIM victim-survivors, but extends to individuals who experienced a variety of traumatic events online, including but not limited to stalking, doxxing, intimate partner violence, and blackmailing [39, 90]. Tseng et al. note that continuity is an important principle for designing interventions to address IPV; information, relationships, and approaches should be consistent when caring for IPV victims [98]. This, combined with other types of internet-related trauma, suggests that design ought to account for usage after traumatic events [16, 87].

7.3 Research in algorithms

7.3.1 Hashing. Hashing algorithms are essential in preventing the spread of NCIM. However, this is not without limitations. Platform participation is entirely optional, it may be challenging to detect altered images, and requiring victim-survivors to verify their identity as part of the process can further infringe on their privacy. Research should strive for more comprehensive solutions that are effective regardless of platform policies, while accounting for the very real possibility of such systems being misused themselves, e.g., by perpetrators of intimate partner violence wishing to eliminate evidence of abuse [38].

7.3.2 Deepfakes. The emergence of sexually explicit AI-generated content presents another dimension of NCIM harm. Studies indicate that deepfake sexual abuse constitutes a significant portion, accounting for 96 to 98% of all deepfake content [26, 59, 60]. This alarming prevalence, coupled with existing inadequacies in legal protections, underscores the urgent need for policy interventions. Deepfakes pose unique challenges that redefine the boundaries of consent in the creation of media. Unlike traditional forms of NCIM, deepfakes eliminate the need for physical proximity or explicit recordings, as perpetrators need only easily accessible benign images or videos from the victim's social media profiles. Exploiting default publicness and leveraging advancements in generative AI to produce nude images, deepfakes facilitate the creation and dissemination of NCIM without consent or awareness. The distinction between consent and violation in deepfake technology is stark. Unlike cases where intimate media was initially shared consensually with a partner, deepfakes leave little room for ambiguity. While not inherently limited to non-consensual content, the most prevalent uses of deepfake technology are harmful, and necessitate a critical reassessment of its legal status and the protections afforded to individuals.

7.4 Research in networks

7.4.1 CDNs. Content Delivery Networks (CDNs), such as CloudFlare, have the potential to recognize and refuse hosting NCIM. For example, CDNs may ensure that non-consensual material is not propagated across their servers. Given the central role of hosts in the online ecosystem—where a single host can support numerous websites—their influence is pivotal. This power necessitates caution; it grants hosts substantial control over decisions concerning platform content, potentially affecting how content is moderated or censored. It is important to prevent censorship of legitimate expressions while curbing the spread of harmful material.

7.4.2 Consent protocols. Could protocols be utilized to enforce consensual data transmission? Could we then affirm that the transmission of data—particularly intimate content—is consensual? This approach could significantly reduce NCIM harms which primarily stem from unauthorized sharing over networks. However, implementing such a system requires careful governance to balance the deterrence of non-consensual sharing with the need to maintain the free flow of knowledge and other beneficial data. Developing media protocols including licensing agreements could help deter unauthorized use. One challenge here is applying these solutions to emerging decentralized platforms, where control and enforcement mechanisms are not as straightforward

as in centralized systems. Research in this area may consider innovative approaches to protocol design that can operate effectively within different topologies.

7.5 Research in storage and OS

7.5.1 Deterring duplication. Unauthorized duplication of content is a central issue in many NCIM cases. There are several forms of unauthorized duplication of content, including screenshots replicating intimate details. This prompts the question: could files themselves be designed to embed mechanisms that verify and protect user consent, akin to how institutions manage document access on cloud services? Future research in protocols may address duplication prevention measures. Although it is impossible to *fully* prevent duplication, introducing barriers and restrictions may mitigate some harmful practices: even if protections don't prevent *all* harms, barriers may sufficiently deter a *portion* of non-consensual screenshots or recordings. Deterrence may even communicate senders' privacy preferences.

7.6 Research in hardware

7.6.1 Consensual cameras. Is it feasible to ensure consent is respected by recording devices? For example, the MacBook webcam is designed with a green light that is hardwired to turn on whenever the camera is on.[4] This design helps prevent unauthorized recordings by malware and mitigates concerns about secret recordings. Meta Ray-Bans are designed with a continuously blinking capture LED light to signal when the camera is active. If the LED is obscured, the glasses will stop recording, prompting the user to clear the obstruction.[5] The LED serves as a transparent indicator to ensure that people are aware when recording is taking place. Similarly, camera-equipped phones sold in Japan have a shutter sound that, by industry convention, is not possible to disable.[6] This privacy protection was established to avoid surreptitious photos and filming.

The direct wiring of the webcam light ensures the feature cannot be bypassed. Could the camera's hardware be programmed to interact with the application layer to ensure consent is obtained? Could future recording devices be designed to actively seek and respect the consent of the subjects before recording begins? Hardware solutions like this are particularly impactful because they operate at the lowest level of the technical stack, embedding privacy protections directly into the device itself. By implementing these features at a fundamental level, just as data flows up the technical stack, the benefits may flow up the sociotechnical stack.

8 Conclusion

NCIM is both a technical and sociotechnical challenge, interacting deeply with many social and computing elements. The roots of sexual abuse and the misogyny that drive NCIM are historical and pre-date the internet. The sociotechnical approach presented in this paper cannot *fully solve* the underlying issues of abuse, nor fully address the shaming and gendered imbalances experienced by victim-survivors, it offers strategies to reduce the widespread proliferation of harmful content. This paper addresses the critical gap in how technologies not only facilitate but also generate NCIM at scale. Through the sociotechnical stack framework, we analyze the interplay between social impacts and technical elements, highlighting the role of features such as generative AI models in creating non-consensual content. Our approach demonstrated the practical application of the sociotechnical stack to dissect the complexities of NCIM, revealing how these technologies influence the creation, obtainment, and dissemination of content. We present our findings and outline a research roadmap

---

[4]https://support.apple.com/en-us/102177
[5]https://about.meta.com/ray-ban-stories-privacy/#built-for-your-privacy
[6]https://www.engadget.com/2016-09-30-japans-noisy-iphone-problem.html

of sociotechnical research in NCIM to support victim-survivors, deter perpetrators, and foster consent in digital interactions.

Acknowledgments

References

[1] [n. d.]. Safe Digital Intimacy. https://www.safedigitalintimacy.org/. Accessed: April 28, 2024.

[2] Mark S Ackerman. 2000. The intellectual challenge of CSCW: the gap between social requirements and technical feasibility. *Human–Computer Interaction* 15, 2-3 (2000), 179–203.

[3] James Auger. 2013. Speculative design: crafting the speculation. *Digital Creativity* 24, 1 (2013), 11–35.

[4] Yu Bai, Li Li, Shanqing Zhang, Jianfeng Lu, and Mahmoud Emam. 2023. Fast Frequency Domain Screen-Shooting Watermarking Algorithm Based on ORB Feature Points. *Mathematics* 11, 7 (Jan. 2023), 1730. https://doi.org/10.3390/math11071730 Number: 7 Publisher: Multidisciplinary Digital Publishing Institute.

[5] Samantha Bates. 2017. Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors. *Feminist Criminology* 12, 1 (Jan. 2017), 22–42. https://doi.org/10.1177/1557085116654565 Publisher: SAGE Publications.

[6] Lindsay Blackwell, Jill Dimond, Sarita Schoenebeck, and Cliff Lampe. 2017. Classification and Its Consequences for Online Harassment: Design Insights from HeartMob. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW (Dec. 2017), 24:1–24:19. https://doi.org/10.1145/3134659

[7] Sarah Bloom. 2014. No vengeance for revenge porn victims: Unraveling why this latest female-centric, intimate-partner offense is still legal, and why we should criminalize it. *Fordham Urb. LJ* 42 (2014), 233.

[8] Danielle Blunt, Ariel Wolf, Emily Coombes, and Shanelle Mullin. 2020. Posting into the void: Studying the impact of shadowbanning on sex workers and activists. *Hacking/Hustling* (2020), 1–87.

[9] Cheng Bo, Guobin Shen, Jie Liu, Xiang-Yang Li, YongGuang Zhang, and Feng Zhao. 2014. Privacy.tag: privacy concern expressed and respected. In *Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems*. ACM, Memphis Tennessee, 163–176. https://doi.org/10.1145/2668332.2668339

[10] Danah Boyd. 2010. Social network sites as networked publics: Affordances, dynamics, and implications. In *A networked self*. Routledge, 47–66.

[11] Johanna Brewer, Joseph'Jofish' Kaye, Amanda Williams, and Susan Wyche. 2006. Sexual interactions: why we should talk about sex in HCI. In *CHI'06 Extended Abstracts on Human Factors in Computing Systems*. 1695–1698.

[12] Alexandra Brodsky. 2021. *Sexual Justice: Supporting Victims, Ensuring Due Process, and Resisting the Conservative Backlash*. Metropolitan Books.

[13] Denise Buiten. 2020. It's "vile" but is it violence? A case study analysis of news media representations of non-consensual sexual image-sharing. *Feminist Media Studies* 20, 8 (2020), 1177–1194.

[14] Emma Burnett. 2023. CRIMINALIZING NONCONSENSUAL PORNOGRAPHY. *Boston University Law Review* 103, 6 (2023).

[15] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, 441–458. https://doi.org/10.1109/SP.2018.00061

[16] Janet X Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *CHI Conference on Human Factors in Computing Systems*. 1–20.

[17] Michelle Chen. 2016. One More Way the Courts Aren't Working for the Poor. https://www.thenation.com/article/archive/one-more-way-the-courts-arent-working-for-the-poor/.

[18] Alexander Cho. 2018. Default publicness: Queer youth of color, social media, and being outed by the machine. *New Media & Society* 20, 9 (2018), 3183–3200.

[19] Danielle Keats Citron. 2014. *Hate crimes in cyberspace*. Harvard University Press.

[20] Danielle Keats Citron. 2020. A New Compact for Sexual Privacy. *William & Mary Law Review* (2020).

[21] Danielle Keats Citron. 2022. *The Fight for Privacy: Protecting Dignity, Identity and Love in our Digital Age*. W.W. Norton & Company.

[22] Danielle Keats Citron and Mary Anne Franks. 2014. Criminalizing revenge porn. *Wake Forest L. Rev.* 49 (2014), 345.

[23] Danielle Keats Citron and Mary Anne Franks. 2020. The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform. *U. Chi. Legal F.* (2020), 45.

[24] Elizabeth M. Clancy, Bianca Klettke, and David J. Hallford. 2019. The dark side of sexting – Factors predicting the dissemination of sexts. *Computers in Human Behavior* 92 (March 2019), 266–272. https://doi.org/10.1016/j.chb.2018.11.023

[25] Kathryn D Coduto and Allison McDonald. 2024. "Delete it and Move On": Digital Management of Shared Sexual Content after a Breakup. (2024).

[26] Sophie Compton and Marina Hunt. 2024. *Deepfake Abuse: Landscape Analysis*. Technical Report. My Image My Choice Coalition. Available online: www.myimagemychoice.org.

[27] Maddy Coy. 2024. *Violence Against Women in the US: Theory, Research and Policy*. Taylor & Francis.

[28] Antonella De Angeli, Mattia Falduti, Maria Menendez-Blanco, and Sergio Tessaris. 2023. Reporting non-consensual pornography: clarity, efficiency and distress. *Multimedia Tools and Applications* (Jan. 2023). https://doi.org/10.1007/s11042-022-14291-z

[29] Walter S DeKeseredy and Martin D Schwartz. 1993. Male peer support and woman abuse: An expansion of DeKeseredy's model. *Sociological Spectrum* 13, 4 (1993), 393–413.

[30] Walter S DeKeseredy and Martin D Schwartz. 2016. Thinking sociologically about image-based sexual abuse: The contribution of male peer support theory. *Sexualization, Media, & Society* 2, 4 (2016), 2374623816684692.

[31] Arne Dekker, Frederike Wenzlaff, Anne Daubmann, Hans O Pinnschmidt, and Peer Briken. 2019. (Don't) look at me! How the assumed consensual or non-consensual distribution affects perception and evaluation of sexting images. *Journal of clinical medicine* 8, 5 (2019), 706.

[32] Alexa Dodge. 2019. Nudes are Forever: Judicial Interpretations of Digital Technology's Impact on "Revenge Porn". *Canadian Journal of Law and Society* (April 2019). https://doi.org/10.1017/cls.2019.4

[33] Asia Eaton, Holly Jacobs, and Yanet Ruvalcaba. 2017. 2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration. (2017).

[34] Hany Farid. 2018. Reining in online abuses. *Technology & Innovation* 19, 3 (2018), 593–599.

[35] Mary Anne Franks. 2014. Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators. *SSRN Electronic Journal* (2014). https://doi.org/10.2139/ssrn.2468823

[36] Mary Anne Franks. 2015. Drafting an effective'revenge porn'law: A guide for legislators. *Available at SSRN 2468823* (2015).

[37] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 202:1–202:24. https://doi.org/10.1145/3359304

[38] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.

[39] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 1–22. https://doi.org/10.1145/3134681

[40] Deen Freelon and Chris Wells. 2020. Disinformation as political communication. , 145–156 pages.

[41] Christine Geeng, Jevan Hutson, and Franziska Roesner. 2020. Usable Sexurity: Studying {People's} Concerns and Strategies When Sexting. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 127–144.

[42] R. Stuart Geiger. 2016. Bot-based collective blocklists in Twitter: the counterpublic moderation of harassment in a networked public space. *Information, Communication & Society* 19, 6 (June 2016), 787–803. https://doi.org/10.1080/1369118X.2016.1153700 Publisher: Routledge _eprint: https://doi.org/10.1080/1369118X.2016.1153700.

[43] Tarleton Gillespie. 2018. *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

[44] Chiara Gius. 2022. Addressing the Blurred question of 'responsibility': insights from online news comments on a case of nonconsensual pornography. *Journal of Gender Studies* 31, 2 (2022), 193–203.

[45] Eric Goldman. 2020. How Section 230 Enhances the First Amendment. https://papers.ssrn.com/abstract=3662475.

[46] Wei Gu, Ching-Chun Chang, Yu Bai, Yunyuan Fan, Liang Tao, and Li Li. 2023. Anti-Screenshot Watermarking Algorithm for Archival Image Based on Deep Learning Model. *Entropy* 25, 2 (Feb. 2023), 288. https://doi.org/10.3390/e25020288

[47] Janet Halley. 2016. The Move to Affirmative Consent. *Signs: Journal of Women in Culture and Society* 42, 1 (Sept. 2016), 257–279. https://doi.org/10.1086/686904

[48] Vaughn Hamilton, Gabriel Kaptchuk, Allison McDonald, and Elissa M. Redmiles. 2024. Safer Digital Intimacy for Sex Workers and Beyond: A Technical Research Agenda. *IEEE Security & Privacy* 22, 2 (2024), 17–28. https://doi.org/10.1109/MSEC.2023.3324615

[49] Jeff Hearn and Matthew Hall. 2019. 'This is my cheating ex': Gender and sexuality in revenge porn. *Sexualities* 22, 5-6 (2019), 860–882.

[50] Nicola Henry and Asher Flynn. 2019. Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support. *Violence Against Women* 25, 16 (Dec. 2019), 1932–1955. https://doi.org/10.1177/1077801219863881 Publisher: SAGE Publications Inc.

[51] Nicola Henry and Anastasia Powell. 2015. Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology* 48, 1 (March 2015), 104–118. https://doi.org/10.1177/0004865814524218

[52] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S Ackerman, and Eric Gilbert. 2021. Yes: Affirmative consent as a theoretical framework for understanding and imagining social platforms. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–18.

[53] Cyber Civil Rights Initiative. 2014. Revenge Porn Statistics. (2014). https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf

[54] Shagun Jhaver, Sucheta Ghoshal, Amy Bruckman, and Eric Gilbert. 2018. Online Harassment and Content Moderation: The Case of Blocklists. *ACM Trans. Comput.-Hum. Interact.* 25, 2 (March 2018), 12:1–12:33. https://doi.org/10.1145/3185593

[55] Xiao-Dan Jiang, Shi-Ming Yu, De-Feng He, Yong-Liang Liu, and Zhe-Ming Lu. [n. d.]. Information Leakage Source Tracing Based on Robust Image Watermarking Against Mobile Instant Messaging. ([n. d.]).

[56] Callum Jones, Verity Trott, and Scott Wright. 2020. Sluts and soyboys: MGTOW and the production of misogynistic online harassment. *New media & society* 22, 10 (2020), 1903–1921.

[57] Kristen N Jozkowski. 2015. Barriers to affirmative consent policies and the need for affirmative sexuality. *U. of Pac. L. Rev.* 47 (2015), 741.

[58] Gopinaath Kannabiran, Alex A Ahmed, Matthew Wood, Madeline Balaam, Theresa Jean Tanenbaum, Shaowen Bardzell, and Jeffrey Bardzell. 2018. Design for sexual wellbeing in HCI. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–7.

[59] Vasileia Karasavva and Aalia Noorbhai. 2021. The Real Threat of Deepfake Pornography: A Review of Canadian Policy. *Cyberpsychology, Behavior, and Social Networking* 24, 3 (March 2021), 203–209. https://doi.org/10.1089/cyber.2020.0272

[60] Andrei O. J. Kwok and Sharon G. M. Koh. 2021. Deepfake: a social construction of technology perspective. *Current Issues in Tourism* 24, 13 (July 2021), 1798–1802. https://doi.org/10.1080/13683500.2020.1738357

[61] Jin Ree Lee and Steven Downing. 2019. An exploratory perception analysis of consensual and nonconsensual image sharing. *International Journal of Cybersecurity Intelligence & Cybercrime* 2, 2 (2019), 23–43.

[62] Una Lee and Dann Toliver. 2017. *Building Consentful Tech.* Technical Report. http://www.consentfultech.io/wp-content/uploads/2019/10/Building-Consentful-Tech.pdf

[63] Lawrence Lessig. 2009. *Code: And other laws of cyberspace.* ReadHowYouWant. com.

[64] J. Nathan Matias. 2019. Preventing harassment and increasing group participation through social norms in 2,190 online science discussions. *Proceedings of the National Academy of Sciences* 116, 20 (May 2019), 9785–9789. https://doi.org/10.1073/pnas.1813486116

[65] Allison McDonald, Florian Schaub, Catherine Barwulor, Michelle L Mazurek, and Elissa M Redmiles. [n. d.]. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. ([n. d.]).

[66] Clare McGlynn, Kelly Johnson, Erika Rackley, Nicola Henry, Nicola Gavey, Asher Flynn, and Anastasia Powell. 2021. 'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse. *Social & Legal Studies* 30, 4 (Aug. 2021), 541–562. https://doi.org/10.1177/0964663920947791 Publisher: SAGE Publications Ltd.

[67] Clare McGlynn and Erika Rackley. 2017. Image-Based Sexual Abuse. *Oxford Journal of Legal Studies* 37, 3 (2017), 534–561. https://doi.org/10.1093/ojls/gqw033

[68] Colten Meisner. 2023. Networked Responses to Networked Harassment? Creators' Coordinated Management of "Hate Raids" on Twitch. *Social Media + Society* 9, 2 (April 2023), 20563051231179696. https://doi.org/10.1177/20563051231179696 Publisher: SAGE Publications Ltd.

[69] Marijke Naezer and Lotte van Oosterhout. 2021. Only sluts love sexting: Youth, sexual norms and non-consensual sharing of digital sexual images. *Journal of Gender Studies* 30, 1 (2021), 79–90.

[70] Josef Nguyen and Bonnie Ruberg. 2020. Challenges of Designing Consent: Consent Mechanics in Video Games as Models for Interactive User Agency. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376827

[71] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[72] Alexandra-Mihaela Olteanu, Kevin Huguenin, Italo Dacosta, and Jean-Pierre Hubaux. 2018. Consensual and Privacy-Preserving Sharing of Multi-Subject and Interdependent Data. In *Proceedings 2018 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2018.23002

[73] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 83–102. https://www.usenix.org/conference/soups2018/presentation/park

[74] Unnati Patel and Ronald Roesch. 2022. The Prevalence of Technology-Facilitated Sexual Violence: A Meta-Analysis and Systematic Review. *Trauma, Violence, & Abuse* 23, 2 (April 2022), 428–443. https://doi.org/10.1177/1524838020958057 Publisher: SAGE Publications.

[75] Laura Pavón-Benítez, Nuria Romo-Avilés, and Pilar Tarancón Gómez. 2022. "In my village everything is known": sexting and revenge porn in young people from rural Spain. *Feminist Media Studies* 22, 8 (Nov. 2022), 2020–2036. https://doi.org/10.1080/14680777.2021.1935290

[76] Anastasia Powell and Nicola Henry. 2014. Blurred lines? Responding to 'sexting'and gender-based violence among young people. *Children Australia* 39, 2 (2014), 119–124. Publisher: Cambridge University Press.

[77] Anastasia Powell, Adrian J Scott, Asher Flynn, and Sarah McCook. 2024. A multi-country study of image-based sexual abuse: Extent, relational nature and correlates of victimisation experiences. *Journal of Sexual Aggression* 30, 1 (2024), 25–40.

[78] Lucy Qin, Vaughn Hamilton, Sharon Wang, Yigit Aydinalp, Marin Scarlett, and Elissa M Redmiles. 2024. " Did They Consent to That?": Safer Digital Intimacy via Proactive Protection Against Image-Based Sexual Abuse. *arXiv preprint arXiv:2403.04659* (2024).

[79] Li Qiwei, Francesca Lameiro, Shefali Patel, Cristi-Isaula-Reyes, Eytan Adar, Eric Gilbert, and Sarita Schoenebeck. 2024. Feminist Interaction Techniques: Deterring Non-Consensual Screenshots with Interaction Techniques. arXiv:2404.18867 [cs.HC]

[80] Toni Robertson and Jesper Simonsen. 2012. Participatory Design: an introduction. In *Routledge international handbook of participatory design*. Routledge, 1–17.

[81] Yanet Ruvalcaba and Asia A Eaton. 2020. Nonconsensual pornography among US adults: a sexual scripts framework on victimization, perpetration, and health correlates for women and men. *Psychology of violence* 10, 1 (2020), 68.

[82] Nithya Sambasivan, Nova Ahmed, Amna Batool, Elie Bursztein, Elizabeth Churchill, Laura Sanely Gaytan-Lugo, Tara Matthews, David Nemar, Kurt Thomas, and Sunny Consolvo. 2019. Toward Gender-Equitable Privacy and Security in South Asia. *IEEE Security & Privacy* 17, 4 (2019), 71–77.

[83] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 2019. " They Don't Leave Us Alone Anywhere We Go" Gender and Digital Abuse in South Asia. In *proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–14.

[84] Sarita Schoenebeck, Oliver L Haimson, and Lisa Nakamura. 2021. Drawing from justice theories to support targets of online harassment. *New Media & Society* 23, 5 (May 2021), 1278–1300. https://doi.org/10.1177/1461444820913122 Publisher: SAGE Publications.

[85] Sarita Schoenebeck, Carol F. Scott, Emma Grace Hurley, Tammy Chang, and Ellen Selkie. 2021. Youth Trust in Social Media Companies and Expectations of Justice: Accountability and Repair After Online Harassment. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (April 2021), 2:1–2:18. https://doi.org/10.1145/3449076

[86] Janneke M. Schokkenbroek, Koen Ponnet, Joris Van Ouytsel, Michel Walrave, and Wim Hardyns. 2023. Receive, forward, repeat: The link between sexting intention, sexting attitudes, and non-consensual sexting behaviours. *Telematics and Informatics* 84 (Oct. 2023), 102036. https://doi.org/10.1016/j.tele.2023.102036

[87] Carol F Scott, Gabriela Marcu, Riana Elyse Anderson, Mark W Newman, and Sarita Schoenebeck. 2023. Trauma-Informed Social Media: Towards Solutions for Reducing and Healing Online Harm. *arXiv preprint arXiv:2302.05312* (2023).

[88] Alexis Shore and Kelsey Prena. 2023. Platform rules as privacy tools: The influence of screenshot accountability and trust on privacy management. *New Media & Society* (July 2023), 14614448231188929. https://doi.org/10.1177/14614448231188929 Publisher: SAGE Publications.

[89] Carly Parnitzke Smith and Jennifer J Freyd. 2014. Institutional betrayal. *American Psychologist* 69, 6 (2014), 575.

[90] Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. 2007. Intimate partner violence, technology, and stalking. *Violence against women* 13, 8 (2007), 842–856.

[91] Jackie Speier. 2022. Speier, Katko, Klobuchar, Burr Reintroduce Bipartisan Bill to Address Online Exploitation of Private Images on International Women's Day. https://speier.house.gov/2022/3/speier-and-katko-reintroduce-bipartisan-bill-to-address-online-exploitation-of-private-images-on-international-women-s-day

[92] Amia Srinivasan. 2021. *The right to sex: Feminism in the twenty-first century*. Farrar, Straus and Giroux.

[93] Yolande Strengers, Jathan Sadowski, Zhuying Li, Anna Shimshak, and Florian 'Floyd' Mueller. 2021. What Can HCI Learn from Sexual Consent? A Feminist Process of Embodied Consent for Interactions with Emerging Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3411764.3445107

[94] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. 2021. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*. 247–267. https://doi.org/10.1109/SP40001.2021.00028

[95] Brian Timmerman, Pulak Mehta, Progga Deb, Kevin Gallagher, Brendan Dolan-Gavitt, Siddharth Garg, and Rachel Greenstadt. 2023. Studying the Online Deepfake Community. *Journal of Online Trust and Safety* 2, 1 (Sept. 2023). https://doi.org/10.54501/jots.v2i1.126

[96] Rona Torenz. 2021. The politics of affirmative consent: Considerations from a gender and sexuality studies perspective. *German Law Journal* 22, 5 (2021), 718–733.

[97] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2020. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th USENIX security symposium (USENIX Security 20)*. 1893–1909.

[98] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care infrastructures for digital security in intimate partner violence. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–20.

[99] Deborah Tuerkheimer. 2015. Affirmative consent. *Ohio St. J. Crim. L.* 13 (2015), 441.

[100] Jirassaya Uttarapong, Jie Cai, and Donghee Wohn. 2021. Harassment Experiences of Women and LGBTQ Live Streamers and How They Handled Negativity. In *Proceedings of IMX '21*. https://doi.org/10.1145/3452918.3458794

[101] Kate Walker and Emma Sleath. 2017. A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and Violent Behavior* 36 (Sept. 2017), 9–24. https://doi.org/10.1016/j.avb.2017.06.010

[102] Wendy A. Walsh and Dafna Tener. 2022. "If you don't send me five other pictures I am going to post the photo online": A qualitative analysis of experiences of survivors of sextortion. *Journal of Child Sexual Abuse* 31, 4 (May 2022), 447–465. https://doi.org/10.1080/10538712.2022.2067093

[103] Tom Wilson and Kate Starbird. 2020. Cross-platform disinformation campaigns: lessons learned and next steps. *Harvard Kennedy School Misinformation Review* 1, 1 (2020).

[104] Lan Zhang, Cheng Bo, Jiahui Hou, Xiang-Yang Li, Yu Wang, Kebin Liu, and Yunhao Liu. 2015. Kaleido: You Can Watch It But Cannot Record It. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, Paris France, 372–385. https://doi.org/10.1145/2789168.2790106

[105] Shilin Zhu, Chi Zhang, and Xinyu Zhang. 2017. Automating Visual Privacy Protection Using a Smart LED. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*. ACM, Snowbird Utah USA, 329–342. https://doi.org/10.1145/3117811.3117820

[106] Douglas Zytko and Nicholas Furlo. 2023. Online Dating as Context to Design Sexual Consent Technology with Women and LGBTQ+ Stakeholders. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3544548.3580911

[107] Douglas Zytko, Nicholas Furlo, Bailey Carlin, and Matthew Archer. 2021. Computer-mediated consent to sex: the context of Tinder. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–26.