Feminist Interaction Techniques: Deterring Non-Consensual Screenshots with Interaction Techniques

Li Qiwei, Francesca Lameiro, Shefali Patel, Cristi Isaula-Reyes,
Eytan Adar, Eric Gilbert, Sarita Schoenebeck
University of Michigan
Ann Arbor, USA



Figure 1: Performing interlace and binoculars gestures in Hands-Off to deter non-consensual mobile screenshots.

ABSTRACT

Non-consensual Intimate Media (NCIM) refers to the distribution of sexual or intimate content without consent. NCIM is common and causes significant emotional, financial, and reputational harm. We developed Hands-Off, an interaction technique for messaging applications that deters non-consensual screenshots. Hands-Off requires recipients to perform a hand gesture in the air, above the device, to unlock media—which makes simultaneous screenshotting difficult. A lab study shows that Hands-Off gestures are easy to perform and reduce non-consensual screenshots by 67%. We conclude by generalizing this approach and introduce the idea of *Feminist Interaction Techniques (FIT)*, interaction techniques that encode feminist values and speak to societal problems, and reflect on FIT's opportunities and limitations.

CCS CONCEPTS

• **Human-centered computing** → **Interactive systems and tools**; **Collaborative and social computing**.

Authors emails: rrll,flameiro,shefalip,cisaula,eadar,eegg,yardi@umich.edu

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
UIST '24, October 13–16, 2024, Pittsburgh, PA, USA
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0628-8/24/10
https://doi.org/10.1145/3654777.3676380

KEYWORDS

feminism, interaction techniques, social computing, consent

ACM Reference Format:
Li Qiwei, Francesca Lameiro, Shefali Patel, Cristi Isaula-Reyes,, Eytan Adar, Eric Gilbert, Sarita Schoenebeck. 2024. Feminist Interaction Techniques: Deterring Non-Consensual Screenshots with Interaction Techniques. In *The 37th Annual ACM Symposium on User Interface Software and Technology (UIST '24), October 13–16, 2024, Pittsburgh, PA, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3654777.3676380

1 INTRODUCTION

Can interaction techniques be feminist? Feminist values such as agency, consent, and boundaries seek to create a more just and equitable society. Could low-level interaction techniques–at the boundary between people and machines–embody them?

Serious societal problems live at this boundary. For example, non-consensual intimate media (NCIM) refers to the distribution of sexual or intimate content without consent. NCIM is prevalent and causes significant emotional, financial, and reputational harm [7, 9, 15, 28, 32, 41, 45, 49, 63]. A common NCIM case is when sexual content shared during romantic relationships is duplicated and re-shared without permission.[1] If an image gets to a recipient's screen, it can always be captured in some way. An image can likely be saved directly, but if it cannot be saved, it can likely be screenshotted [54], and if it cannot be screenshotted, it can be captured using an external camera.

Offline, learned social rules help govern access to our bodies; in mediated contexts, however, few if any tools exist to express,

[1]This is sometimes referred to as "revenge porn", though the term is not appropriate because NCIM does not conform to the definition of pornography.

grant, or revoke consent [37]. Most existing systems to combat NCIM require reporting the content and then following a set of steps to try to have it taken down, which is reactive and often ineffective [41]. A motivating question for us is: Is it possible to deter non-consensual screenshots with interaction techniques?

To address this issue, and as part of our broader project addressing NCIM, we developed Hands-Off, an interaction technique for messaging applications that deters non-consensual screenshots (see Fig. 1). After a formative study, we built Hands-Off to require recipients to perform a hand gesture in the air, above the device, to unlock media. Borrowing from the social meaning of gestures (e.g., handshakes) [43, 71], Hands-Off uses gestures as design friction to convey a user's consent preferences, and acts as a deterrent against screenshots. We built a set of four hand-gesture-based deterrence features. If a sender wishes to share a photo, but only wants the receiver to have controlled, momentary access to it, they can require that the receiver perform a gesture. The media will only reveal itself while the hand-gesture is being performed. We also describe a threat model and design space for how gestures can be used with different content types, relationships, and locations.

Our lab study (N=13) shows Hands-Off reduces non-consensual screenshots by 67% across all gestures—and by 77% among the top-performing three. The experimental procedure asked participants to view images with Hands-Off, and then try to "break it" by obtaining a screenshot of the image. Afterward, we conducted interviews and a usability survey. Participants found the Hands-Off gestures easy to perform, but difficult or "impossible" to take a screenshot. Participants resorted to using their feet in some cases (see Fig. 6). Critically, participants also reported that Hands-Off establishes social norms about what content the sender wishes to remain transient—setting important social expectations around when duplication is allowed and when it is not.

Finally, we move toward generalizing the conceptual approach of Hands-Off and introduce the idea of *Feminist Interaction Techniques (FIT)*—interaction techniques that encode feminist values and speak to societal problems. FIT draws on feminism as a set of generative concepts for computing—such as agency, boundaries, and consent [3]. It aims to translate feminism's values—and its goal of a more just and equitable society through them—into lower-level, technical HCI concepts. However, problems like NCIM are complex, deeply-rooted societal issues; technical approaches such as FIT can help, but not "solve them." The oppression of women and gender minorities is not a problem that technology alone can fix. To conclude, we reflect on both FIT's opportunities and limitations.

In summary, the major contributions of this work are:

- ***The Hands-Off interaction technique*** for messaging applications that deter NCIM.
- ***An evaluation of Hands-Off***. Hands-Off deterred non-consensual screenshots and may create a constructive cycle that establishes social norms around consent.
- ***The concept of Feminist Interaction Techniques (FIT)***—interaction techniques that encode feminist values and speak to societal problems.
- ***A discussion of the strengths and limitations of FIT***. NCIM is a deeply entrenched societal problem. Approaches such as FIT can ameliorate NCIM, but not solve it.

2 RELATED WORK

We review prior work on how values are built into systems. We then summarize prior research systems for visual privacy, placing Hands-Off within a related threat model. Finally, we consider design friction and its potential to shape Hands-Off outcomes.

2.1 Embedding values in systems

Values are principles or standards that have some influence over behaviors or decision-making. Within technology, a value refers to the underlying ethics and beliefs that shape the design process and the functions of the technology. These values are not just about aesthetics or usability, but about how the system may impact users and society [3, 10, 18]. Human-centered computing has sought to design technologies with certain values instilled, and a rich body of work has critically examined values within computing. For example, Costanza-Chock critiqued the implicit gender and body assumptions in modern airport TSA systems [10], Friedman applied Value Sensitive Design principles for the redesign of the Mozilla browser for cookie awareness [19, 53], and Fiesler et. al noted feminist values in the redesign of a web page [14].

The concept and practice of feminism has a long and storied history, but has typically prioritized values of empowerment, agency, autonomy, and consent. Bardzell argued in 2010 that the field of feminism had much to contribute to interaction design and called for a deeper engagement with feminist ideas in the field of human-computer interaction [3]. That call has been taken up in subsequent work that explores the values embedded in consentful technology, such as control over bodies and affirmative consent in interactions [31, 37].

However, building a complex principle like consent into systems is challenging. The "sociotechnical gap" describes the gap between the social goals we might have for a system, and what the system is actually able to do in practice [1]. These challenges are especially felt at the top of the software "stack", where human behaviors and interactions create rich, messy social contexts, which computers cannot easily model or build abstractions from. That is, while systems might be pretty effective at collecting and protecting user values at lower layers of the stack, such as operating system level access controls, they struggle with application layer levels, such as content that is shared between people. As Ackerman notes, "social activity is fluid and nuanced, and this makes systems technically difficult to construct properly" [1]. Yet, he continues, we can "augment technical mechanisms with social mechanisms to control, regulate, or encourage behavior." This work takes up the charge of augmenting interaction techniques in support of feminist values.

2.2 Visual privacy

It has never been easier to take and share photos online. While photo-sharing offers social value to society (e.g. sending a baby photo to grandparents), photo-sharing via wearable devices, ubiquitous surveillance, and facial recognition technologies creates privacy risks. Privacy-inspired systems address this concern by focusing primarily in three areas: physical photography, online photo access, and photo recapture. Prior work includes systems to prevent unwanted photography in public spaces, such as Privacy.tag's QR codes that can be placed on clothing to enact

privacy protections [5] or using smart LED lighting design in physical spaces to prevent photography [72]. The second area of research focuses on limiting users' access to photos. This includes asking individuals depicted in a photo for preferences regarding obfuscation [44, 55, 56] and drawing cartoons over video streams to protect bystanders' privacy [27], or only showing the faces to friends on social media [29]. A final thread of research includes systems to prevent recapture of a mobile screen, such as preventing second screen capture by changing the lighting and display on a screen [70] and digital watermarking systems that collect metadata of the device making screenshots [2, 24, 34], and photos that fade with time [46].

Although screenshots are useful for collecting and sharing information [11], their misuse can also have serious consequences. Screenshots play a role in making temporal sharing into a permanent privacy violation [13, 54]. Illicit duplication and dissemination of screenshots have contributed to mass online harassment, misinformation via decontextualization of content, and revealing personal information that leads to stalking, surveillance, and even kidnapping of both adults and children [6, 38, 45]. While ephemeral social network sites such as Snapchat are often used for temporal and casual communication, they are not ideal for preserving privacy [46]. Snapchat still allows screenshots and users have discovered additional methods of saving photos and messages sent on the platform [36, 46].

This work is motivated by NCIM, a specific form of privacy leakage harm. The illicit distribution of another individual's intimate content impacts women disproportionately and exemplifies a form of privacy violation that impacts everyone [7, 9]. The harms of NCIM are severe and lasting. According to a survey conducted by the Cyber Civil Rights Initiative, of 361 victims of NCIM, 93% suffered significant emotional distress, 82% suffered significant impairment in social and occupational areas, 42% sought out psychological services, and 51% experienced suicidal ideation [32]. NCIM can have many causes, including fabrication with deepfakes and recordings during sexual assault. A common occurrence is the non-consensual distribution of intimate content that was initially sent with consent, common in break-ups between romantic couples [7, 15, 41, 64]. Another form of violation occurs in commercial activities, often involving sex work or the creation of sexual content [40, 49], when such content is redistributed or shared without the creator's consent. This can be through copying existing content to a different platform or by sharing privately commissioned work publicly. NCIM is part of a broad class of problems where gender inequalities are perpetuated online, including the creation and dissemination of NCIM [7–9, 15, 17, 22, 41, 48, 49], our data bodies [37], acts of intimate partner violence [16, 17, 60, 73], and other forms of online harms. These problems go far beyond privacy breaches, causing emotional, reputational, and economic harm.

2.3 Design friction

HCI has historically focused on making systems that are intuitive, unburdensome, and that prioritize performance for the end-user. Introducing friction at the cost of lessening performance may increase desired behaviors, similarly to how a stop sign slows driving but increases safety. Design friction is the concept of deliberately making some interactions more difficult, in order to make them more purposeful, safe, and thoughtful [23].

Design friction has been implemented in social media platforms to avoid unsafe or undesired actions, particularly ones that have downstream harms on other users. Wang et. al deployed a countdown timer on Facebook to ensure the user waits 20 seconds before making a post in order to minimize regrettable posts [65]. Gould et. al notes several design friction choices on Twitter's platform to warn users against potential misinformation in some posts, as well as asking users to confirm they have read an article themselves before re-tweeting [23].

Friction can also be a tool towards meaningful reflection and intention. It is common for functionally opposing design approaches to remove key aspects of their function in order to highlight their values. This includes works in critical design, counter-functional design, slow design, reflective design, and lucid design [20, 47, 53]. Physical friction can also be designed to induce user reflection. For example, "Crank That" is a physical hand-crank intervention to increase friction and awareness of passive consumption in Twitter content feeds [57]. Users are required to continuously turn a hand crank in order to power a screen to use social media, allowing users to "question how they value various interactions on social media by transforming their usage into an embodied one in which they have to physically work for their experience" [57].

Our work applies design friction to encourage users to think about consent when taking screenshots in online conversations. We leverage intentional design barriers to promote responsible use. We also shift the burden from those who are the victims of consent violations towards those who might be the perpetrators of consent violations. That is, instead of responding to non-consensual sharing reactively (e.g. requesting a takedown), we intervene in it proactively (e.g. deterring from violations).

An effective proactive mechanism should prevent or deter unwanted behavior. Currently, only a few messaging platforms allow users to prevent screenshots altogether.[2] StopNCII, a hashing-based system developed by multiple stakeholders including Meta, allows users to upload photos to a server before these photos are ever posted by someone else, and then block subsequent attempts by someone else to upload these photos.[3] However, even then there are many drawbacks. Transformed images may evade the hash algorithm. When these images continue to be reposted, platforms may overly rely on StopNCII and invest less effort in removals. And of course, users must trust the third party–in this case, Meta. Our work aims to make the burden more equitable, placing "the work" on a potential perpetrator rather than the potential victim.

3 FORMATIVE STUDY

We conducted a formative interview study to develop design requirements for a technological intervention. The formative study aimed to augment prior qualitative and survey research on NCIM [7–9, 15, 17, 22, 41, 48, 49]. The first portion of the interview focused on participants' existing screenshot experiences and practices. The second portion asked participants for their thoughts about using a

[2]https://www.safedigitalintimacy.org/state-of-the-industry
[3]https://stopncii.org/

screenshot deterrence system. In our conception of Hands-Off, we believed that a gestural interface–one that prevented viewers from using the screenshot features by occupying their hands–could be an effective deterrent. We used the formative study as an opportunity to test this idea. Thus, in the second part of the interview, we had participants explore how they would use a screenshot deterrence feature. We described the design of a gesture-based approach and solicited reflection and feedback feedback. Our university's IRB approved the study.

3.1 Participants

Eight participants were recruited from two undergrad courses at a large university, consisting of 4 women and 4 men. We specifically recruited participants who were able and willing to share their own or other peoples' experiences about screenshots. We wanted to capture not only NCIM-specific experiences but also wider patterns of unauthorized screenshot sharing so that Hands-Off may be a system used for messaging broadly. We gave participants the option of either 1:1 solo interviews or paired interviews in which the participant brought a friend, who often acted as a confidante, to encourage more conversation. Each interview session took between 45 to 60 minutes. Each participant was compensated $15 for a pair interview or $20 for a solo interview. In the paired interview, both participants were paid and both generated information used for the study.

3.2 Interview results

Two authors analyzed the interview data. We annotated interview transcripts and used open coding to find themes across all sessions. Below are high-level themes from our formative study.

3.2.1 Theme 1: The need for screenshot prevention. Participants wanted enhanced privacy measures in mobile messaging platforms, especially in scenarios where sensitive content is exchanged. The dissemination of sensitive content without the sender's knowledge can have far-reaching consequences. A participant shared an incident that exposed a critical gap in notification systems, leaving the victim unaware of unauthorized sharing.

> *"A girl was sexting to a friend of mine. And one of my friends sends those pictures to, like, half of the group or whatever. And then I think someone inside the group sent it to another person. It went through most of our grades. I don't know if the girl knew who did that. I mean, there was like, no notification. So she just came into the situation where those photos were running through the class." –P4*

Furthermore, harm can arise from uncontrolled text message re-sharing. Participant 2 recounted a personal experience of sharing a screenshot of a conversation with a professor, only to have it forwarded to the entire class.

> *"I had shared my conversation with a professor with someone, and I didn't really want everyone to know about it. But that person forwarded it to the entire class. And after I found out ... I was angry. The effects of that incident continued till the day I graduated. People in that group forwarded it to their friends and spoke about me. Not just my department, but other people also would come up to me and ask me about it." —P2*

Axis	Design Considerations
Content	Serious content→serious gesture Silly content→silly gesture
Relationship	Close→simple, less protective gesture Not close→more protective gesture
Location	Public→socially acceptable gesture Private→any gesture

Table 1: Design considerations from formative study. The type of gesture matters for of content sent, the relationship between sender and recipient, and the location for viewing the content.

3.2.2 Theme 2: Perceived security of gesture-based screenshot prevention. We presented participants with a possible gesture-based approach, using hand gestures to both indicate preferences about and deter unwanted screenshots. Participants expressed a strong preference for gesture-based security features within mobile messaging applications. Their feedback shed light on the underlying motivations and practical benefits. Gesture-based security provides a tangible barrier, making it significantly harder for the recipient to share content.

One participant conveyed the importance of a physical safeguard that actively prevents sharing, especially in scenarios involving acquaintances and friends.

> *"Even if there was just a feature that said, this person doesn't want to share with an acquaintance, I wouldn't necessarily trust them to actually do that. And so I would want them to do something that physically prevented them from doing that." —P4*

Participants noted that gesture-based deterrence could reduce the potential awkwardness associated with directly requesting confidentiality through written or spoken messages. This suggests that a gestural approach may enhance privacy while streamlining communication.

3.2.3 Theme 3: Gesture should depend on context. All participants believed that there should be a variety of gestures to choose from to account for various usage contexts. Specifically, context depends on three axes: the type of content sent, the relationship with the recipient, and the recipient's location of viewing. Table 1 maps the connection between the axis and its design considerations.

Type of content sent. Participants emphasized the importance of tailoring gestures to the nature of the content being shared. For instance, for lighthearted or silly content, a corresponding playful or casual gesture was suggested. In contrast, when sharing serious or sensitive information, participants favored a more solemn and meaningful gesture that aligned with the gravity of the content:

> *"What you're doing with your body elicits of obviously different emotions ... so it would be really hard for me to engage with a serious text effectively if I had to do something silly." –P5*

Relationship with recipient. The relationship with the recipient mattered in determining the appropriateness and

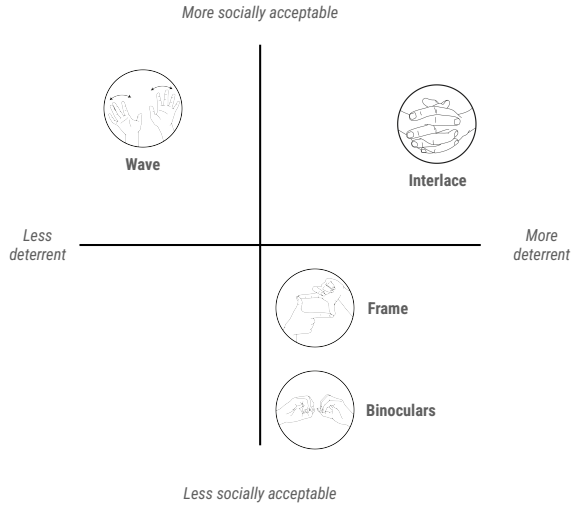


Figure 2: A priori, designer-view of deterrence vs social acceptability for Hands-Off gestures.

complexity of the gesture. For close relationships, a simpler, less protective gesture was suitable. Conversely, for interactions with acquaintances or less familiar contacts, participants leaned towards employing a more intricate and potentially challenging gesture to enhance security.

Location of viewing. Participants thought the viewing environment was a crucial factor in gesture design. In public spaces, there was a preference for gestures that blended seamlessly with everyday actions. This choice was motivated by the desire for subtlety and to avoid drawing attention. In private settings, however, participants felt more at liberty to employ a wider range of gestures.

4 SYSTEM DESIGN

Hands-Off gestures are designed around principles of deterrence and social acceptability, with each usage context leading to the design requirements of a particular gesture. We describe a set of design goals (see Fig. 2) and threat model (see Fig. 3) for Hands-Off gestures. We then illustrate how this design space maps to specific use cases and conclude with implementation details for Hands-Off.

4.1 Threats and design goals

4.1.1 Threat model. The threat model for Hands-Off is unwanted photo duplication in online sharing [4] (see Fig. 3). The system should deter general unauthorized duplication, which would take media out of its original context. We borrow from prior visual privacy systems and "assume that the adversaries are the users, the online services and third parties (e.g., external observers)" [44]. The paradigm begins with a sender who sends a piece of original content to a recipient. From there, the recipient may download the file, screen record, screenshot, capture it using a second device themselves, or utilize an accomplice to capture on a different device.

Hands-Off goals include *preventing* screenshots, and *deterring* second device capture by the same individual. Some portions of the threat model are accounted for in prior work. In-app downloads and screen recording may be disabled by the system developer, and second device capture may be deterred with a system such as Kaleido that uses lighting patterns to disrupt outside cameras [70]. Screenshots on the device may also be prevented within the operating system of mobile devices, but this is rarely implemented in popular mobile messaging applications. As we have observed, there is no approach that can absolutely *guarantee* that an image not be captured and reshared. However, it is worth considering which approaches raise the cost of different types of "attacks".

4.1.2 Design goals. Hands-Off functions by occupying both hands to prevent individuals from engaging the screenshot features on the device. As the hands are occupied, this may further deter second device capture.[4] However, our analysis of themes in the formative study reveals additional specific design constraints:

- **D1:** Gestures should be easy to perform and detectable.
- **D2:** Gestures should, at minimum, deter screenshot capture.
- **D3:** Gestures should suit different viewing contexts, content types, and receiver-sender relationships.

Because our focus is on using the hands as *deterrence* rather than the traditional *input*, our design space for hand gestures is distinct from those defined in prior work [66, 68]. For this reason, we chose to create our own inclusion criteria. The design guidelines allow us to focus on specific gesture types while eliminating others. For example, an alternative approach is to use multi-touch detection on the screen itself. This can engage the hands in a way that prevents screenshots. However, these may be harder to execute and detect, requiring contortion of the hands on the device (violation of D1); may be less secure as the hands are close to the buttons (violation of D2); and because the hands are on the device, they may function *too well* across all contexts (violation of D3). Dynamic gestures (e.g., waving, clapping, etc.) may be easy to perform but harder to detect and may limit the contexts in which they are applied (e.g., are less suitable in a public setting).

In addition to the explicit guidelines above, we have opted to focus on abstract gestures with relatively little cultural significance. Some gestures are culturally dependent in meaning (e.g., palms touching in a prayer gesture) whereas others have existing iconic or metaphoric roles (e.g., hands making a heart symbol). By relying on more abstract gestures, we hope that their meaning may be more flexible. This allows some degree of communicable understanding through gestures, while still allowing flexibility for how users choose to interpret them. That said, depending on context, gestures with existing meaning may be desirable for certain applications. These are possible with Hands-Off, but are left to future work.

4.2 Design space

Hands-Off gestures are shaped with two key factors in mind: preventing misuse and fitting within societal norms. Like a

[4]Clearly, this is just a deterrent. A particularly motivated attacker could position a second device, record a video, clip frames, and recover a fairly good representation.

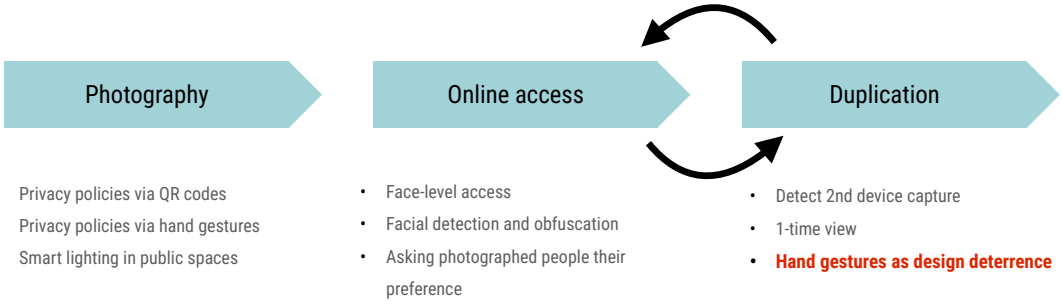


Figure 3: Threat model of possible methods of screen duplication after content is sent. Duplicated content may be posted online repeatedly, continuing this cycle. HANDS-OFF contributes to deterrence against screenshotting content. Also listed is prior work and where it fits in this threat model: preventing photography([5, 72]), preventing online access([27, 30, 39, 62]), and preventing duplication([46, 70]).

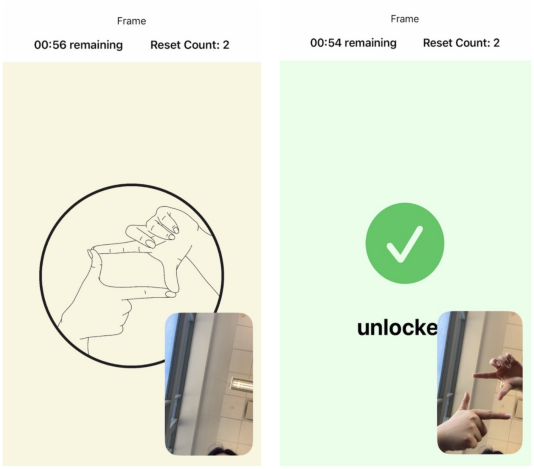


Figure 4: HANDS-OFF interface we use in the usability study. The left screen shows users what gesture to perform, and the right screen shows a successfully unlocked screen after the gesture is detected by the model.



Figure 5: Participants performing the HANDS-OFF gestures.

literary symbol, social gestures are imbued with meaning. They communicate through physicalization of language or ceremony [35, 52]. A wave goodbye between friends, a handshake after a negotiation, or a raised hand in a court of law are all means of communicating between parties but also to observers. They have semantic meaning [69], which may be learned, innate [33], or inferred (e.g., hands with palms outward to represent a 'wall') [43]. Even a gesture made in private can embody a sentiment or belief or serve a regulatory function [51]. Using a gesture, even an abstract one, can physicalize an affirmation, whether observed by someone else or not: "I understand that the image was shared with me and is not intended for sharing with others." The friction imposed by the physical nature of the gesture further acts to reinforce the meaning and, thus, a broader value system of consent, autonomy, and agency. It is not a button to be clicked away.

As a form of body language, the choice of gestures in interaction must take into account likely social interpretation. This is key as HANDS-OFF exists within two overlapping, but distinct, design spaces: bodily friction and social friction. Bodily friction is the invisible but physical restraint. The constrained space is the gap between the user when performing the necessary gesture, and the physical location of the two phone buttons that need to be pressed simultaneously to screenshot. In HANDS-OFF, the gap is maintained by the system's detection of a hand gesture and the distance between reaching over and pressing the two buttons. Along the social dimension, someone using their phone in a public space will consider their social appearance in doing so. Prior work has shown that people generally want to avoid making social blunders in the presence of others, and subtle movements and movements that look and feel like everyday actions are preferred over uncommon movements [50].

4.2.1 HANDS-OFF gestures. HANDS-OFF's gestures map to different locations along hypothetical deterrence and social acceptability

Gesture	False Positives	False Negatives	Precision	Recall	F_1
Wave	3	1	98%	99%	0.98
Frame	6	9	97%	95%	0.96
Interlace	32	2	86%	99%	0.92
Binoculars	4	6	97%	96%	0.96

Table 2: Model shows high precision across 3 of the 4 gestures. Interlace was an exception because the model had difficulty recognizing interlaced fingers as two hands instead of one.

axes (see Fig. 2). *Wave:* Waving two hands at a phone in public is common when we are greeting someone on video chat, and thus blends in as socially acceptable. *Interlace:* Two hands each holding the other with fingers interwoven for additional security, and is also a 'low-key' gesture to do in public settings. *Frame:* Viewing something through frames that the fingers create lends an element of playfulness, and is somewhat silly to do in public. *Binoculars:* This is the strangest and silliest of the four hand gestures, and is likely preferred to be done in private only.

4.3 Use cases

Hands-Off may be used in any scenario when someone may choose to share a message or photo, and does not want the recipient to have permanent access to it. Our interview study shows that users may choose to use Hands-Off to share content such as personal documents, emotionally intimate moments, playful memories, or romantic photos.

Silly moment just for us. Sam is having a good time and wants to share a photo of him out drinking with his long-distance best friend Ray. However, Sam doesn't want Ray to send this photo to anyone else. He chooses Hands-Off and selects the *binoculars* option to match the silliness of the photo with the gesture, and also to imply Ray should not reshare this photo. When Ray receives the message, he is prompted to perform the hand gesture and then sees the photo Sam has shared.

Romantic intimacy. Anna met Jordan on a dating app recently and they have been chatting online. They begin sexting and Anna wants to send some photos. However, she doesn't know Jordan well and wants to take protective measures before doing so. She only wants Jordan to see these photos, not anyone in Jordan's group chat. She chooses the *frame* option to send a photo to Jordan.

Office gossip. Ali and Jo are best friends at work. Today, Jo heard some very interesting gossip that she wants to share with Ali. It's somewhat sensitive and she wants to ensure he can't pass on the information – at least not with proof that she had shared it. Jo selects *interlace* because it matches the nature of the topic.

4.4 Implementation details

We built Hands-Off using SwiftUI for iOS devices. We chose the iPhone for its consistent button placement and hardware design. We rely on pose detection using a custom CoreML hand pose detection model trained with a custom corpus we built. We defined a multi-class neural-network classification model with 20 convolution layers for interlace, wave, frame, binoculars, and a background class for when none of the above gestures are detected. Training data consisted of 120 to 200 photos of hands performing each gesture per class. We collected the vast majority of the data ourselves by taking photos of the hands of participants. We account for high and low lighting, light and dark skin tones, and different photography angles. The remaining photos are copyright-free images of hands from the internet. The model was trained to recognize the hands through the positions of the fingertips and the locations of the joints. See Table 2 for model performance. Facial data was not used to train the model.

Gesture detection in the Hands-Off system initially shows a screen with the hand gesture that the user is prompted to perform as in Figure 4. The system can detect hands while the phone is on a flat surface or propped up (e.g., with a phone stand). Once the model detects the hand gesture successfully, the underlying photo is revealed. The camera feed is continuous, and the photo is covered again as soon as the hand gesture stops being detected. To decrease the times that the image flickers between covered and uncovered, we add an adjustable confidence level for the gesture detection model's predictions with a default set at 90%. The rest of the user interface is composed of a front-camera view at the bottom right corner similar to those found in common video chat software.

4.5 Hands-Off limitations

4.5.1 System limitations. One limitation of using the CoreML model is it consistently recognized interlaced hands as one hand instead of two, which impacted precision for interlace (see Table 2). For each other hand gesture, Hands-Off required two hands detected as well as gesture detected to display the photo. However, we had to silently change this two-hands criterion for the interlace option. This limitation tells us the CoreML vision model works well for detected separated hands or poses, but may be limited for gestures when the hands stack or otherwise overlay each other.

We note several limitations in Hands-Off. First, Hands-Off is based on assumptions and modes of interactions specific to the iPhone. Screenshot deterrence is built on top of one static assumption of the double button press on the left and right sides of the phone body. The methods of screenshots can vary in other designs of mobile phones. As future work progresses, limitations may also arise in securing hand gesture-based consent in AR, VR, and XR spaces due to the possibility of certain gestures already being used as input by the specific system. Second, this study tackles just one aspect of many potential privacy concerns in the threat model. Screen recording can still be used to capture the screen if that feature is not disabled in the application. Future research in gesture-based deterrence should consider allowing users to create their own custom hand gestures. This personalization would add a uniquely intimate layer to the interaction, similar to how secret handshakes signify closeness between two people or some in-group status.

4.5.2 Accessibility limitations. Currently, Hands-Off is limited in accommodating all abilities (e.g., people with mobility impairments and those with blindness or low vision). Feminism should acknowledge intersectionality, and that includes building for various abilities. Expanding the range of gesture-based methods to accommodate users with different abilities, needs, and various

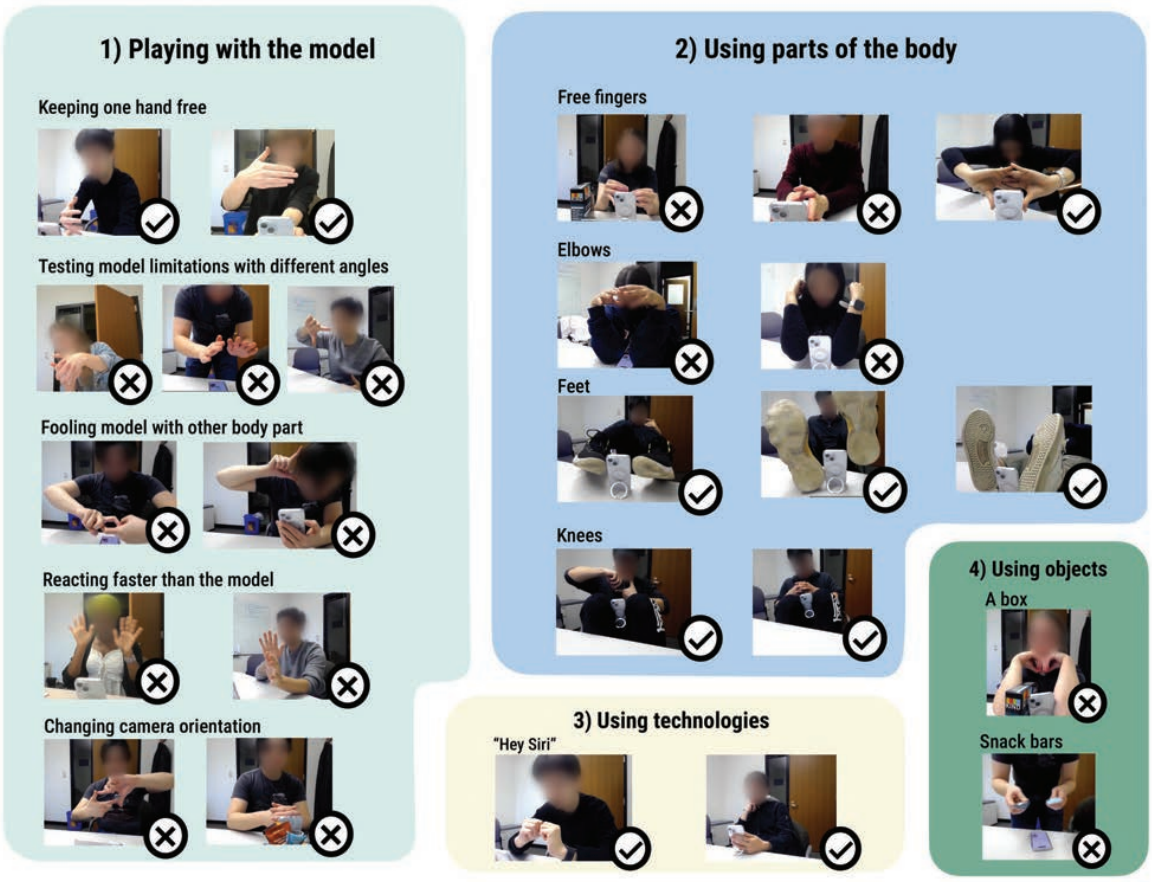


Figure 6: Attempts to break Hands-Off surfaced many creative methods, including playing with model boundaries, using body parts, voice-based technologies, and prop objects.

device models is crucial. For individuals with limited hand dexterity or those who may not be able to perform certain gestures, providing customizable gestures or alternative input methods, such as voice commands or facial expressions, could enhance usability. For users with visual impairments, integrating haptic feedback or audio cues to guide and confirm interactions can make the system more accessible. Compatibility with screen readers and providing clear, descriptive labels and instructions for all gestures and functions would also be important. Accessibility testing with diverse user groups may be a continuous part of the development process to identify and address any barriers that may arise. By prioritizing inclusive design, Hands-Off can better serve a broader range of users and embody principles of intersectional feminism.

5 STUDY

Following our design goals outlined in Section 4.1.2, we set out to answer these questions:

RQ1. Can hand gestures be completed & recognized successfully?
RQ2. Can hand gestures deter screenshots?
RQ3. What are peoples' preferences for hand gestures under different situations?

RQ1 draws from **D1** to evaluate the effectiveness of the gesture recognition model and whether participants are able to perform the gestures. RQ2 speaks to **D2** to focus on the deterrence ability. RQ3 assesses participant preferences for **D3**. RQs 1 and 2 are evaluated via in-lab usability tasks, and we answer RQ3 through interviews with the same participants. Our university's IRB approved the study.

5.1 Materials and procedure

We designed an experiment using two tasks to answer our research questions. Participants first received a 3-minute demonstration of Hands-Off to ensure that they were physically able to perform each gesture. The first task focused on participants' ability to execute the gestures. The second task focused on participants' ability to circumvent the Hands-Off system.

For the first task, an iPhone running the Hands-Off iOS app was placed in front of the participant. The gestures were shown in random order and participants had up to one minute to perform each gesture to have it recognized by the model *once*. After a gesture is detected, Hands-Off will move on to the next gesture. We recorded videos of participants while using Hands-Off and

documented for each gesture the seconds that it took for the gesture to be detected by the system.

The second task asked the participant to try to take a screenshot of the unlocked screen to the best of their ability. We instructed them to take screenshots by pressing two buttons on the iPhone. Naturally, it is difficult to hold a hand gesture and also take a screenshot at the same time, so we instructed the participants to use whatever method they can to "break" the system and try to take the photo. The participants received no additional hints or instructions beyond this. For each gesture, participants are given up to 3 minutes or until they choose to give up and move on to the next gesture. We again recorded videos of the participants, and for each gesture, we documented the number of attempts.

Participant results for the screenshot deterrence task can be broken up into the following categories:

- **Successful** screenshot capturing an unlocked screen.
- **Failed** can be defined in two ways:
  Attempted screenshot but the screen became locked due to the gesture not being detected when a screenshot was taken.
  Skipped the trial without making an attempt; participant believed it was "impossible" to take the screenshot.

After each task, we asked participants to complete the NASA Task Load Index (NASA-TLX) to compare the difficulty between the two tasks. NASA-TLX is a long-standing measurement of mental workload with 21 questions on the mental and physical demands of the activity, temporal demand, performance, effort, and frustration experienced in the task [25, 26].

At the end of the evaluation, we asked each participant the following open-ended interview questions to assess how well gestures satisfy the varying suitability guideline (**D3**):

- Imagine you were messaging a friend and they sent a message that you had to unlock with a hand gesture. Would you assume they would be okay for you to screenshot it?
- Which hand gesture are you most likely to use to send:
  …something funny to a close friend?
  …something personal you don't want to be opened in public?
  …something serious?
  …something to someone you're not close with?

The evaluation was performed in a private, mostly empty office set up for the experiment design. The participants sat at a desk and used a provided iPhone 15 (iOS 17.6) on which Hands-Off was installed. A stand attached to the case supports the phone, but the phone can also be laid flat on a table. We recorded video in two different ways: (a) a screen recording captured the exact on-screen interaction between the participant and Hands-Off; and, (b) a camera on a separate laptop captured the broader physical interaction of the participant and the device.

5.2 Participants

We invited 13 participants to attempt to take screenshots while using Hands-Off. We selected participants who currently own and use an iPhone as their main mobile device. The participants consisted of undergraduate and graduate students whose ages ranged from 18 to 30 years old (μ = 23.8 years). We did not specifically restrict participation based on physical abilities or limitations (though individuals may have self-selected to participate). All 13 were able to successfully perform the hand gestures without assistance. Each participant was compensated $20 following the study.

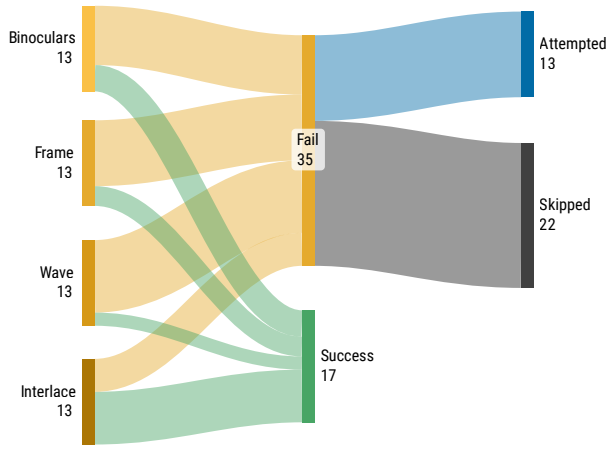


Figure 7: Of all attempts, 33% succeeded in making a screenshot, 25% attempted without success, 42% gave up early on believing the task to be impossible.

5.3 Results

5.3.1 *Gestures as deterrence.*

Using Hands-Off deterred 67% of all screenshot attempts. The success rate increases to 77% when we take out the interlace gesture. Figure 7 shows the results across all usability tasks. On average, participants took between 1 and 11 seconds ($\mu = 2.78$ sec) to perform a hand gesture and to have it detected by the system. In contrast, when attempting to screenshot while performing a hand gesture, the mean time spent across all hand gestures was 74.4 seconds and up to the full time allotment of 180 seconds. Notably, in 7 trials participants chose to skip a gesture when they felt it was impossible to "break" and decided to give up and move on to the next gesture without making an attempt.

Participants were able to perform the hand gestures on their own easily, but found it very difficult to take a screenshot. Even when we exclude participants who chose to give up early, Figure 8 displays the dramatic difference between time spent on the first and second tasks. The time spent screenshotting was, on average, 27 times longer than that doing hand gestures only. The majority of successful screenshots were using interlace due to the aforementioned loophole. Similarly, the self-reported usability metrics in Figure 10 suggest that participants found that performing the gestures was easy, but that attempting screenshots was difficult.

5.3.2 *Getting around Hands-Off.*

Playing with the model. Participants prodded, poked, and pushed the gesture recognition model to find its working boundaries. Participants attempted different angles and camera

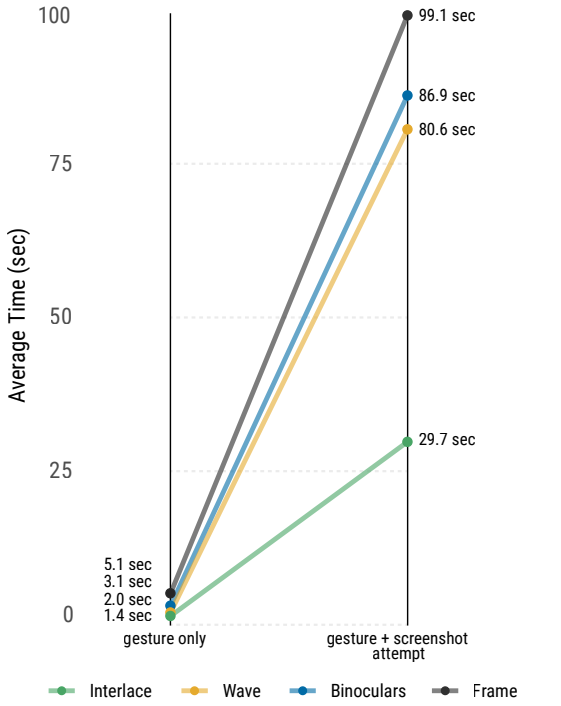


Figure 8: Completion times for the two evaluation tasks. Performing gestures was easy (left), but trying to screenshot while performing gestures was difficult (right).

orientations to find the limits of the model. One participant creatively attempted to "trick" the model with his index finger joints posing as a frame (without success). We also witnessed attempts to make the gesture to unlock the phone and then quickly try to screenshot. We found that the interlace gesture was a special case. With the exception of interlace, no other attempts to push the boundaries of the model resulted in successful screenshots.

Using parts of the body. With the hands engaged in performing the gesture, some participants tested alternative parts of the body to press the two side buttons on the iPhone. This included elbows, knees, and even feet. The use of feet and knees was successful because the hands could be free to perform the gesture. Some gestures, such as interlace and binoculars, did not engage all fingers (e.g., free pinkies or thumbs), which one participant was able to use to screenshot.

Using technologies. For the purposes of the usability testing, we did not disable voice interactions (i.e., Siri). A few savvy participants used this to take a screenshot, resulting in some of the fastest successful times. We note that this feature could be blocked in the application.

Using other objects. The usability laboratory contained a few quotidian items, including snack bars and small empty cardboard boxes. Participants were told they could use any method they could think of to attempt to screenshot. Using a box to press the button was unsuccessful, as was usage of the snack bars.

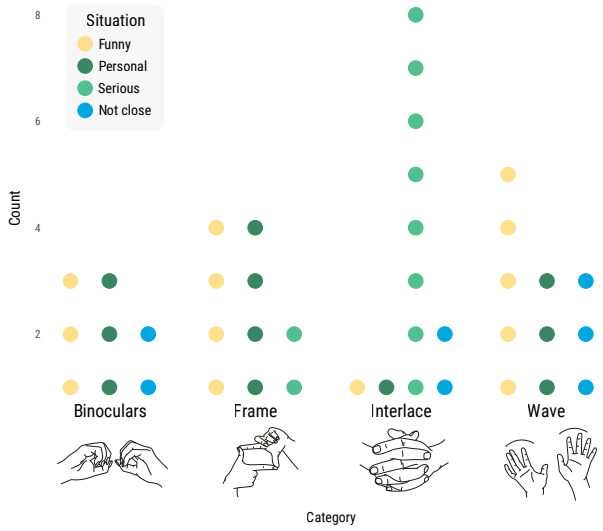


Figure 9: Strong preferences for using interlace in "serious" situations and mixed preferences for other situations.

5.3.3 *Gestures as social signals.*

Sent with gestures == don't screenshot me! Nearly all participants noted the social significance of a message sent with a hand gesture. The additional friction of performing hand gestures pushed participants to consider the context in which the exchange was taking place. In their statement, P13 considered the sender's desired permanence and understood the use of gestures to be "*something similar to the concept of invisible ink. If it's something you have to do another task to see, I'm assuming that it's something super private, and it's probably not meant to be kept for a long time.*". While taking a screenshot is not entirely impossible, the difficulty of the task is effective for starting a discussion about the appropriateness of taking a screenshot. P1 says, "*there's a social presumption of safety and privacy. To take a screenshot is to go against the social mores of the technology. It feels bad to do it, so any kind of buffering you can do to force people into a social more is a good idea. It forces you to think about something before you do it.*"

Hand gestures as an emotional language. We asked participants to select the gesture they believed to be most appropriate under different social contexts (see Fig. 9). Responses showed clear patterns to the appropriateness of gestures in different situations.

We note some flexibility in interpretations because there are often multiple interpretations of the emotional value of a gesture.

One approach to choosing the best gesture for sending a funny photo to a close friend was to take into account the context in which the photo is being sent, the sender, and the media. P12 chose the frame gesture because it mirrored "*taking a picture, and you get to see my funny photos when using the picture.*" A different approach more heavily considered which gesture would be the simplest for the recipient to complete, considering that a funny photo to a close friend calls for a low-security measure. Due to the underlying hand recognition loophole that allowed *interlace* to be screenshotable

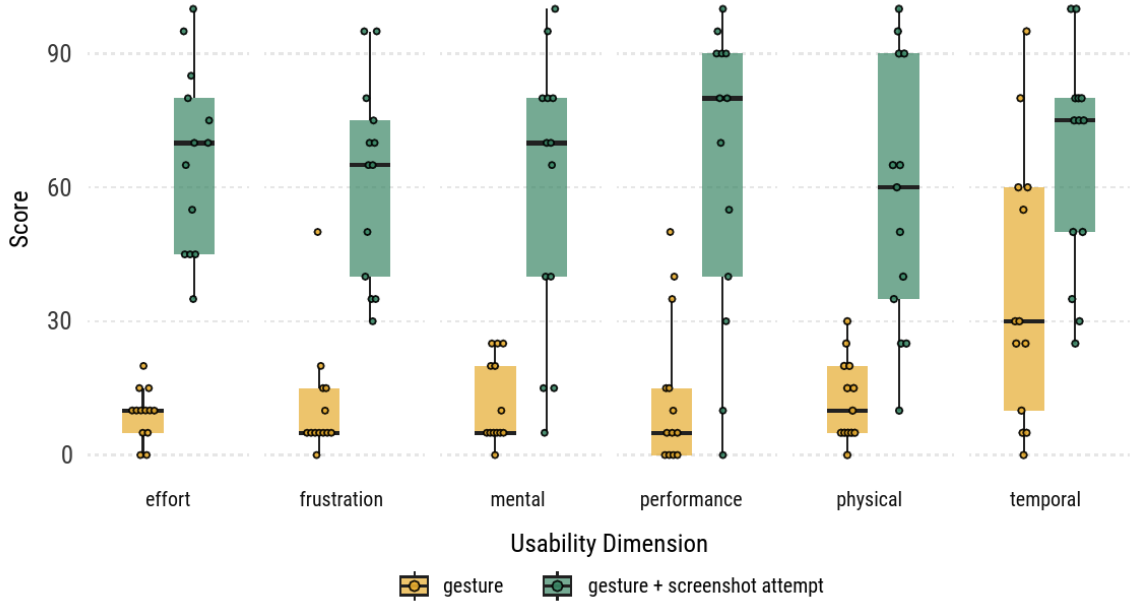


Figure 10: Participants' self-reported NASA-TLX usability results show it is easy to perform Hands-Off gestures on their own, but difficult do gestures and attempt to screenshot at the same time.

with one hand, P10 believed interlace "*was easy enough to only have to use one hand to do it. That's the best preferred, only because you can trick the system with that one.*"

Interlace and frame were top choices for gestures when participants would not want the recipient to open the message in public, but for possibly different reasons. The physical gestures of interlace implied seriousness. P1 supports this by saying that *"interlaced fingers would be the one that I would pick, just because it is stern and it's closed...It's almost like you're holding something, cradling something that you wouldn't want seen."* In contrast, P11 selected frame to deter the recipient from opening the message in public spaces: *"If it's in public, I would want it to be a gesture that would be weird to do in public, so I feel the frame is pretty strange with doing it to your phone. You might wave at your phone or you might set up your phone on a little stand or something and lace your fingers in front of it. Both those things seem more natural, so they're easier to do in public."*

For serious content, some participants preferred interlace. P13 believes *"because interlace is the easiest one to maintain while also still staying focused on what you're looking at."* Participant 1 noted that interlace had a serious nature to it: *"This is what I would do with a job interview, at something serious like a stern meeting. If I'm arrested, I put my hands like this."*

Although most of the participants had clear gesture preferences for defined situations, others such as P2 believed all gestures were fine for any situation: *"All of these gestures don't seem overly silly, where it'd be weird if you had to make a weird face or something, but since it's just a gesture to open a message, I feel like they're all appropriate in that way."*

5.4 Summary

To recap, we summarize the answers to our evaluation questions.

RQ1. Can the hand gestures be completed and recognized successfully? Yes, on average it took fewer than 3 seconds for a model to recognize a hand gesture. See Figure 8.

RQ2. Can hand gestures deter screenshots? Two-thirds, or 67% of screenshot attempts, resulted in failure. Restricting to the top-performing three gestures (e.g., eliminating interlace), the deterrence rate was 77%. Among successful attempts, we see interesting (and socially unlikely) methods of trying to screenshot. See Figures 7 and 6.

RQ3. What are peoples' preferences for hand gestures under different situations? Many considered the emotions the gestures evoked and the practicality of using certain gestures in different situations. For example, interlace is largely preferred in serious situations. See Figure 9.

6 DISCUSSION

Hands-Off reduced non-consensual screenshots, and represents a type of feminist interaction technique. To conclude, we attempt a conceptual contribution, and move toward generalizing the approach of Hands-Off. We discuss how interaction techniques can be feminist, and the opportunities and constraints associated with such an aim.

6.1 Feminist Interaction Techniques

This paper introduces the concept of *Feminist Interaction Techniques (FIT)*—interaction techniques that embody feminist values and speak to societal problems (see Fig. 11). While some subdomains

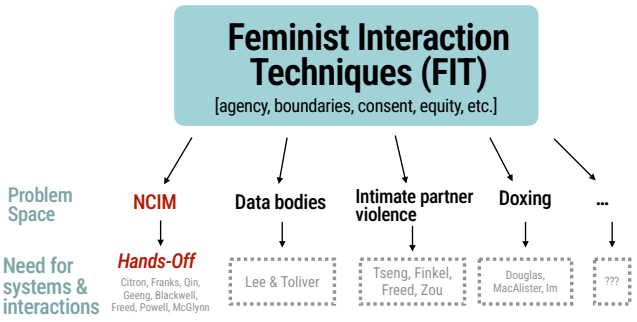


Figure 11: A conceptual framework of FIT, incorporating other scholars who have called for systems and interaction techniques in domains such as data bodies (e.g, [37]), intimate partner violence (e.g., [16, 60, 73]), and doxing (e.g., [31]).

of computing (e.g. the field of Social Computing [59]) have been receptive to the idea of feminism-inspired designs, systems built with such values are few and far between. Part of the problem is the inherent difficulty in mapping high-level concepts to concrete system interactions. With FIT, we aim to bridge the gap between what values systems should have and how they can be built into interactive technologies. We address calls to make feminism concrete in systems:"...while feminism is generally known as a critical strategy, which too often suggests that feminism is only applicable after the fact ...[we] stress the potential for feminism to contribute to an action-based design agenda" [3].

Our application of FIT to the NCIM space demonstrates a way to overcome the limitations of existing solutions. Current NCIM solutions rely primarily on reporting violations; however, reporting is burdensome for users. It requires interacting with an unknown third party (whoever reviews the report for a platform), and can even require submitting *more* photos of oneself and photos of IDs for identification or matching purposes [12, 21, 41]. These approaches are 'state-of-the-art' in deployed systems, but they are not particularly feminist. The Hands-Off system puts the power to establish boundaries in the hands of the photo owner rather than the recipient. It also shifts how we think about *who* should bear the burden of consent from the victim to the potential violator. Finally, it adopts a proactive, rather than reactive, approach, allowing people to establish boundaries rather than reacting to harms.

6.2 FIT values

Feminism is a multi-faceted movement and discipline that has evolved through different waves and phases (see a review within the computing context in [3]). However, many of its core values are durable, including consent, boundaries, equity, bodily autonomy, economic justice, and racial justice. In the case of NCIM, an overarching value is first that NCIM is a problem worth addressing– it affects millions or billions of people daily and degrades social life online and offline. In focusing on NCIM, we also embrace the values that people should have control over their likeness online. Sharing content of someone's likeness without their consent can be a violation of their bodily rights and autonomy, and the field of computing bears some responsibility for addressing the problem of non-consensual sharing of content.

While outside the scope of this paper to exhaustively list values, FIT can leverage feminist values to create new interaction techniques. Critically, our user study suggests that we can effectively design systems that communicate these values to users. As one participant said after using Hands-Off, "There's a social presumption of safety and privacy ...It forces you to think about something before you do it." We could also co-create values with users. In this study, we pre-selected the four hand gestures for participants, which is appropriate for early exploration [67]. However, as shown in 2, the hand gestures bore social meaning, e.g. a wave is more socially acceptable than a binoculars gesture.

Future work could run gesture elicitation studies [61], allowing people to create gestures aligned with their own values. There could also be libraries of consent-based gestures by aggregating preferences across many users [42]

6.3 Application spaces for FIT

Feminist interaction techniques have many use cases. Anywhere there are societal problems that introduce threats to safety and well-being, we can bring a feminist-inspired lens to the problem. The decision to do so does not introduce bias to the design space, but instead recognizes that many social problems are themselves rooted in bias. The power of feminist interaction techniques is that it does not take away from one group in order to design for another; a rising tide lifts all boats.

Digital safety, and other problem spaces with interpersonal and social harms, are natural fits for FIT; however, FIT is not limited to these contexts. There has been much demand for systems and mechanisms that make online interactions safer, more inclusive, and more participatory. It is possible to think of many different vectors for applying FIT to common social interaction paradigms. How to do this in different domains remains an open question—and an opportunity for creative technical HCI research.

A generative approach may be to apply a feminist value to an interaction technique of interest and ask, "How are assumptions about this value 'baked into' it?" In the case of Hands-Off, we targeted the consent assumptions built into the idea that once an image is sent to someone, they have immediate and irrevocable access to it. How are concepts of bodily autonomy (or lack thereof) baked into the context of meeting someone's VR avatar? How is racial justice encoded in the techniques we use to explore spaces in AR—given that the history of many locations and spaces are contested (e.g., Indigenous lands)? What assumptions about consent does deepfake technology make?

6.4 Limitations and precautions

The computing community has a role to play and a responsibility to bear to address digital harms. Problems like NCIM would not exist without decades of computing work that put cameras and mobile devices into nearly everyone's hands, with few safeguards on their use. However, it is important to interrogate the limits of FIT—and any technical approach—in important societal problems. FIT cannot solve gender-based violence. No technology can. Problems like NCIM are technologically-mediated, but the social

and societal contexts in which they exist have been around for millennia. The oppression of women and gender minorities, how the law treats these harms, how society treats survivor-victims, etc., are problems that technology cannot single-handedly "fix." For computing communities with techno-solutionist norms, it is important to note that no technology—no matter how clever and well-intentioned—will completely solve complex societal problems. Additionally, feminism itself, like any set of values or principles, has flaws and limitations (e.g., early feminism prioritized gender while overlooking race, a pattern that was also observed with social technologies [58]).

We began the paper with the question: can interaction techniques be feminist? Our Hands-Off system demonstrates how they can be, but we should proceed with caution in this goal. System design seeks to abstract and concretize outcomes, but consent is a practice not an outcome. To realize the goal of feminist values in interaction techniques, we should not overfit to a design space of solving an interaction problem, but instead to the goal of augmenting an interaction process aligned with desired values.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grants 1763297 and 2311102.

REFERENCES

[1] 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.

[2] 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.

[3] Shaowen Bardzell. 2010. Feminist HCI: taking stock and outlining an agenda for design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Atlanta Georgia USA, 1301–1310. https://doi.org/10.1145/1753326.1753521

[4] Punam Bedi, Vandana Gandotra, Archana Singhal, Himanshi Narang, and Sumit Sharma. 2013. Threat-oriented security framework in risk management using multiagent system. *Software: Practice and Experience* 43, 9 (2013), 1013–1038.

[5] 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

[6] Anna Brosch. 2018. Sharenting–Why do parents violate their children's privacy? *The New Educational Review* 54 (2018), 75–85.

[7] Danielle Keats Citron. 2018. Sexual privacy. *Yale LJ* 128 (2018), 1870.

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

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

[10] Sasha Costanza-Chock. 2020. *Design justice: Community-led practices to build the worlds we need*. The MIT Press.

[11] Emily M Cramer, Yoonmo Sang, and Sunyoung Park. [n. d.]. Uses and Gratifications of the Screenshot in Human Communication: An Exploratory Study [1]. ([n. d.]).

[12] 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

[13] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New media & society* 21, 8 (2019), 1824–1839.

[14] Casey Fiesler, Shannon Morrison, and Amy S. Bruckman. 2016. An Archive of Their Own: A Case Study of Feminist HCI and Values in Design. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, San Jose California USA, 2574–2585. https://doi.org/10.1145/2858036.2858409

[15] 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

[16] 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.

[17] 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

[18] Batya Friedman. 1996. Value-sensitive design. *interactions* 3, 6 (1996), 16–23.

[19] Batya Friedman, Daniel C Howe, and Edward Felten. 2002. Informed consent in the Mozilla browser: Implementing value-sensitive design. In *Proceedings of the 35th annual hawaii international conference on system sciences*. IEEE, 10–pp.

[20] Bill Gaver and Heather Martin. 2000. Alternatives: exploring information appliances through conceptual design proposals. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 209–216.

[21] Christine Geeng. [n. d.]. Usable Sexurity: Studying People's Concerns and Strategies When Sexting. ([n. d.]).

[22] 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.

[23] Sandy J. J. Gould, Lewis L. Chuang, Ioanna Iacovides, Diego Garaialde, Marta E. Cecchinato, Benjamin R. Cowan, and Anna L. Cox. 2021. A Special Interest Group on Designed and Engineered Friction in Interaction. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–4. https://doi.org/10.1145/3411763.3450404

[24] 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

[25] Sandra G Hart. 2006. NASA-task load index (NASA-TLX); 20 years later. In *Proceedings of the human factors and ergonomics society annual meeting*, Vol. 50. Sage publications Sage CA: Los Angeles, CA, 904–908.

[26] Sandra G Hart and Lowell E Staveland. 1988. Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. In *Advances in psychology*. Vol. 52. Elsevier, 139–183.

[27] Eman T. Hassan, Rakibul Hasan, Patrick Shaffer, David Crandall, and Apu Kapadia. 2017. Cartooning for Enhanced Privacy in Lifelogging and Streaming Videos. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE, Honolulu, HI, USA, 1333–1342. https://doi.org/10.1109/CVPRW.2017.175

[28] Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, and Adrian J Scott. 2020. *Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery*. Routledge.

[29] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/off: Preventing privacy leakage from photos in social networks. In *Proceedings of the 22nd ACM SIGSAC Conference on computer and communications security*. 781–792.

[30] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/Off: Preventing Privacy Leakage From Photos in Social Networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, Denver Colorado USA, 781–792. https://doi.org/10.1145/2810103.2813603

[31] 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*. ACM, Yokohama Japan, 1–18. https://doi.org/10.1145/3411764.3445778

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

[33] Jana M Iverson and Susan Goldin-Meadow. 1997. What's communication got to do with it? Gesture in children blind from birth. *Developmental psychology* 33, 3 (1997), 453.

[34] 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.]).

[35] Seokmin Kang and Barbara Tversky. 2016. From hands to minds: Gestures promote understanding. *Cognitive Research: Principles and Implications* 1 (2016), 1–15.

[36] Zubeida Casmod Khan, Thulani Mashiane, and Nobubele A Shozi. 2015. Snapchat media retrieval for novice device users. In *Proceedings of the 10th International Conference on Cyber Warfare and Security*. 162–169.

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

[38] Jacqueline D Lipton. 2009. We, the Paparazzi: Developing a Privacy Paradigm for Digital Video. *Iowa L. Rev.* 95 (2009), 919.

[39] Suyuan Liu, Lan Zhang, Haikuo Yu, Jiahui Hou, Kaiwen Guo, and Xiang-Yang Li. 2022. HideSeeker: Uncover the Hidden Gems in Obfuscated Images. In *Proceedings*

of the Twentieth ACM Conference on Embedded Networked Sensor Systems. ACM, Boston Massachusetts, 682–695. https://doi.org/10.1145/3560905.3568514

[40] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. 2021. " It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *30th USENIX Security Symposium (USENIX Security 21)*. 375–392.

[41] 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.

[42] Meredith Ringel Morris, Jacob O Wobbrock, and Andrew D Wilson. 2010. Understanding users' preferences for surface gestures. In *Proceedings of graphics interface 2010*. 261–268.

[43] Cornelia Müller, Alan Cienki, Ellen Fricke, Silva Ladewig, David McNeill, and Sedinha Tessendorf. 2013. *Body-Language-Communication. Volume 1*. Walter de Gruyter.

[44] 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

[45] 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.

[46] Sabid Bin Habib Pias, Imtiaz Ahmad, Taslima Akter, Apu Kapadia, and Adam J Lee. 2022. Decaying Photos for Enhanced Privacy: User Perceptions Towards Temporal Redactions and'Trusted'Platforms. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–30.

[47] James Pierce and Eric Paulos. 2014. Counterfunctional things: exploring possibilities in designing digital limitations. In *Proceedings of the 2014 conference on Designing interactive systems*. ACM, Vancouver BC Canada, 375–384. https://doi.org/10.1145/2598510.2598522

[48] Anastasia Powell, Nicola Henry, Asher Flynn, and Adrian J. Scott. 2019. Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. *Computers in Human Behavior* 92 (March 2019), 393–402. https://doi.org/10.1016/j.chb.2018.11.009

[49] 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).

[50] Julie Rico and Stephen Brewster. 2010. Usable gestures for mobile interfaces: evaluating social acceptability. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 887–896.

[51] Cintia Rodríguez and Pedro Palacios. 2007. Do private gestures have a self-regulatory function?: A case study. *Infant behavior and development* 30, 2 (2007), 180–194.

[52] Deborah Schiffrin. 1974. Handwork as ceremony: The case of the handshake. (1974).

[53] Phoebe Sengers, Kirsten Boehner, Shay David, and Joseph 'Jofish' Kaye. 2005. Reflective design. In *Proceedings of the 4th decennial conference on Critical computing: between sense and sensibility*. ACM, Aarhus Denmark, 49–58. https://doi.org/10.1145/1094562.1094569

[54] 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.

[55] Jiayu Shu, Rui Zheng, and Pan Hui. 2017. Your privacy is in your hand: Interactive visual privacy control with tags and gestures. In *Communication Systems and Networks: 9th International Conference, COMSNETS 2017, Bengaluru, India, January 4–8, 2017, Revised Selected Papers and Invited Papers 9*. Springer, 24–43.

[56] Jiayu Shu, Rui Zheng, and Pan Hui. 2018. Cardea: Context-aware visual privacy protection for photo taking and sharing. In *Proceedings of the 9th ACM Multimedia Systems Conference*. 304–315.

[57] Katherine W Song, Janaki Vivrekar, Lynn Yeom, Eric Paulos, and Niloufar Salehi. 2021. Crank That Feed: A Physical Intervention for Active Twitter Users. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–6. https://doi.org/10.1145/3411763.3451817

[58] Catherine Knight Steele. 2021. Digital black feminism. In *Digital Black Feminism*. New York University Press.

[59] Stephanie B Steinhardt, Amanda Menking, Ingrid Erickson, Andrea Marshall, Asta Zelenkauskaite, and Jennifer Rode. 2015. Feminism and feminist approaches in social computing. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing*. 303–308.

[60] 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.

[61] Santiago Villarreal-Narvaez, Arthur Sluÿters, Jean Vanderdonckt, and Radu-Daniel Vatavu. 2024. Brave New GES World: A Systematic Literature Review of Gestures and Referents in Gesture Elicitation Studies. *Comput. Surveys* 56, 5 (2024), 1–55.

[62] Nishant Vishwamitra, Yifang Li, Hongxin Hu, Kelly Caine, Long Cheng, Ziming Zhao, and Gail-Joon Ahn. 2022. Towards automated content-based photo privacy control in user-centered social networks. In *Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy*. 65–76.

[63] 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

[64] 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

[65] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A field trial of privacy nudges for facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Toronto Ontario Canada, 2367–2376. https://doi.org/10.1145/2556288.2557413

[66] Jacob O. Wobbrock, Meredith Ringel Morris, and Andrew D. Wilson. 2009. User-defined gestures for surface computing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Boston MA USA, 1083–1092. https://doi.org/10.1145/1518701.1518866

[67] Jacob O Wobbrock, Meredith Ringel Morris, and Andrew D Wilson. 2009. User-defined gestures for surface computing. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1083–1092.

[68] Jacob O. Wobbrock, Andrew D. Wilson, and Yang Li. 2007. Gestures without libraries, toolkits or training: a $1 recognizer for user interface prototypes. In *Proceedings of the 20th annual ACM symposium on User interface software and technology*. ACM, Newport Rhode Island USA, 159–168. https://doi.org/10.1145/1294211.1294238

[69] Jiang Xu, Patrick J Gannon, Karen Emmorey, Jason F Smith, and Allen R Braun. 2009. Symbolic gestures and spoken language are processed by a common neural system. *Proceedings of the National Academy of Sciences* 106, 49 (2009), 20664–20669.

[70] 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

[71] Hui Zhou and Tingqin Zhang. 2008. Body language in business negotiation. *International Journal of Business and Management* 3, 2 (2008), 90–96.

[72] 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

[73] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. 2021. The role of computer security customer support in helping survivors of intimate partner violence. In *30th USENIX Security Symposium (USENIX Security 21)*. 429–446.