

## Defining Intimacy, Consent, and Harm in the Digital Age

On 25 August 2026, the [SVRI TFGBV Community of Practice](#) hosted a webinar on 'Defining Intimacy, Consent and Harm in the Digital Age'. This second TFGBV CoP event emerged as a proposal by the Policy and Advocacy Working Group.

The event brought together legal experts, technologists, and survivor advocates to examine evolving definitions of intimacy and the challenges of enforcing consent in an era of synthetic media and borderless digital platforms. The panel was particularly interested in the tensions between freedom of expression and digital consent, and justice and practical enforcement.

Future CoP events will continue to reflect on evidence from the field, including insights emerging from the SVRI Forum in October.

### What does meaningful consent actually look like in online spaces?

Digital technologies have fundamentally altered the landscape of intimacy, often leaving legal and platform governance systems struggling to keep pace. A core tension lies between the rigid, act-based definitions of the law and the fluid, contextual experiences of survivors around the world.

From a legal perspective, Dr [Olga Marques](#) highlighted that the law often fails to capture the 'digital layer' of sexual harm. In Canada, for instance, Section 162.1 of the Criminal Code makes it an offence to share an intimate image without consent, but applying these definitions in digital environments can be complex. Drawing on her work, she also referred to the idea of 'permanent remembering', as images can be stored and redistributed indefinitely. Survivors may not know whether an image will circulate again, who has it, or how to respond legally despite existing frameworks.

*"An image can continue to exist long after the original distribution (...) in my own research that's what a lot of frontline professionals were talking about. We really don't know how to act legally to the fact that this is a permanent remembering. We don't know what's going to happen, who has it, who's copied it." - Olga Marques*

There are also concerns about how privacy is defined contextually within legal frameworks. The Supreme Court of Canada (*R v Jarvis*, 2019) ruled that being visible in public does not mean forfeiting the right to a reasonable expectation of privacy. But even with these legal protections, there are limitations. The law does not always map neatly onto what people experience as harmful. Legal questions may instead become: does this fit within a specific definition? Was there a reasonable expectation of privacy? How should harm be defined in online spaces?

*"This is not as simple as privacy on one side and freedom of expression on the other, because the challenge right now is figuring out how to protect people from non-consensual sexual harm*

*and digital harm... How do we protect people without enveloping every single type of communication as harmful, particularly when content from LGBTQ+ communities, sexual health content, and images of breast cancer survivors can be caught up in these crossroads?" - Olga Marques*

People's experiences do not fit neatly within fixed definitions of intimacy, harm and consent.

### **Intimacy is not the same as nudity**

[Rohini Lakshane](#) also problematised the significant gap between what is 'legally' considered intimate, usually centred on nudity, and what is experienced as intimate in practice. Harm can occur when an image, even a non-sexualised one, is used to violate religious or cultural norms around modesty. Given that this content does not necessarily include nudity, it flies under the radar of automated content moderation systems, and continues to be monetised. It can also give perpetrators more room to contest reports against their content. This reflects similar findings from [Chayn's report](#) in Pakistan, which raises the need to discuss whether and how an image can become a weapon, and how the harm can extend beyond the person directly targeted.

[Hyra Basit](#) from the [Digital Rights Foundation](#) expanded the discussion with insights from their work with survivors in Pakistan. The rise of AI-generated content, including deepfakes, has introduced a new dimension of harm that traditional laws are often ill-equipped to address. In her experience, the psychological consequences and the fear felt by survivors of non-sexualized intimate abuse are just as significant as those caused by explicitly sexual imagery. If a person's likeness is recognisable, it can damage a survivor's professional reputation or personal safety. Sometimes an explicit image is not even necessary: an ordinary photograph combined with music, emojis or other elements can be used against someone, with consequences equivalent to those associated with nude images.

*"The consequences that they fear (...) from those images being shared or put online are the same as another person would fear (...) if it was just a nude." - Hyra Basit*

Drawing on ten years of case data and advocacy work, Hyra noted that Meta introduced a specific policy on sensitive imagery. She also highlighted how abusers can use synthetic media to 'digitally sexualise' bodies without the person's participation. This loss of control over one's own likeness can itself be a profound form of harm, regardless of whether viewers believe the image to be authentic. Content can also be created in one jurisdiction, hosted in another, and viewed globally, making enforcement extremely difficult for national legal systems.

### **Safety Features and Innovations**

Technology platforms are at the front line of defining and enforcing digital consent. [Kenya Fairley](#) from the dating app Bumble outlined how platform architecture can proactively protect users by engaging experts and GBV organisations to inform their work. Bumble uses several layers of Safety by Design intended to return agency to users.

*“In order for people to really build those meaningful relationships online, they need to feel safe. They need to feel that they can be vulnerable and be within a respected community.” - Kenya Fairley*

She shared some of the features included in Bumble’s apps to prevent and respond to harm.

| Feature                          | Functionality                                                                                                                                            |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Private Detector</a> | An AI tool that detects and blurs lewd images. Users choose whether to unblur or report them. This tool is open source on GitHub.                        |
| Deception Detector               | Automatically identifies and removes spam, scams and fake profiles before members are exposed to them.                                                   |
| Review Before Send               | Uses AI to detect inappropriate text. Forty per cent of users choose to edit their messages after receiving an alert that their language may be harmful. |
| Bloom Programme                  | An online trauma-support initiative offering resources and one-to-one therapy for survivors of digital and physical abuse.                               |

For prevention, Bumble aims to reduce interactions with bad actors and suspicious behaviour using machine learning. It also works to reduce and remove harmful content, respond empathetically and reliably, and promote prosocial behaviour and healthy interpersonal conduct both online and offline.

### **Survivor-Centred Perspectives and Global South Realities**

The experience of Technology-Facilitated Gender-Based Violence (TFGBV) is not monolithic. Survivor advocacy, particularly in LMIC contexts, reveals deep systemic barriers to justice, while also reinforcing the importance of allowing survivors to identify what they need as part of recovering their agency.

Hyra Basit underscores that reporting mechanisms on major platforms such as Meta, TikTok and X are often hidden or too complex for people with low digital literacy or limited financial independence to navigate. In Pakistan, there are only 15 cybercrime wings for the entire country. Survivors may have to travel for hours to file a complaint, which may be impossible for those without financial independence or permission to travel.

According to data from the [Digital Rights Foundation’s helpline](#), another difficulty in reporting is that survivors often prioritise immediate removal of content over long-term legal prosecution. However, without legal action, there is no guarantee that the perpetrator will not resurface the content later from private storage.

Some final reflections also pointed out that some safety features can create additional risks. Survivors may need to preserve evidence, even when their immediate priority is content removal, because that evidence may later be necessary to file a police complaint. At the same time, some safety features can introduce surveillance through mandatory identity checks, face matching, or systems that may silence women reporting violence or discussing gender minorities.

### **What to take from this panel**

- Non-consensual harm can occur through non-sexualised images that fall outside current legal and platform definitions of sexual or intimate content.
- Technology can compound the original act of violence through “permanent remembering,” as content can be stored, copied and resurfaced years later, creating ongoing uncertainty for survivors.
- Consent is layered: consent to create an image is not blanket consent for its retention, distribution, or algorithmic manipulation.
- Some platforms are increasingly using proactive tools (some using AI) to detect harmful content and provide trauma-informed resources through established programmes. However, survivors still face significant barriers, including limited local cybercrime infrastructure, financial dependency, and victim-blaming cultural norms.