[PART 1] IMAGE-BASED ABUSE: A PRACTICAL TECHNICAL GUIDE TO CONTROL THE SPREAD OF CONTENT

19th December 2024

Rohini Lakshané

Rohini Lakshané is an interdisciplinary researcher, technologist and Wikimedian. https://about.me/rohini

Read more

Photo by 愚木混株 cdd20 on Unsplash.

This guide offers practical suggestions for victim-survivors of image-based abuse, especially those living in the global majority world, to remove the violative content while safeguarding their privacy and identity online. It may also be useful for those who support or accompany victim-survivors. This guide contains two parts. Access Part 2 here.

Image-based abuse (IBA), commonly known by the misnomer "revenge porn" is an umbrella term that may refer to,

1. the capture, creation, publishing or distribution of nude or sexually explicit images (photos or videos) without the consent of one or more persons in the frame,
2. a threat to do so, or
3. digitally altered images, often created via image-editing tools such as Photoshop and now increasingly through Artificial Intelligence (AI), that make someone appear nude or in a sexually explicit act without their consent.

IBA violates the rights and dignity of the victims and harms them in all aspects of their lives in the immediate and long-term. Much like everything else on the internet, it is important to understand that once the content is posted online, even if it is removed from one source, copies of it can appear on other or the same sources. However, it is also critical to know that despite this "downward distribution" of content,[1] it is possible to have the content removed. This guide discusses various technical and legal ways that exist to assist the victims and survivors of IBA.

The onus of protecting themselves should not be on the victim-survivors or on persons trying to avoid IBA incidents. But there are known issues that hinder timely and adequate relief, along with failure to stop or reduce the perpetration of IBA. Law enforcement and internet platforms are known to thwart reports raised against IBA content, or act inadequately or slower than required. As a result, victim-survivors sometimes

end up going to unscrupulous hackers, lawyers or police personnel who give them ill-informed or adverse suggestions in return for a fee, bribes or other favours. This aggravates harm and distress to the victim-survivor while also leading them away from genuine remedies. In other cases, victim-survivors do not approach anyone at all and thus do not receive timely support. Some consider self-harm in these cases.

As the calls for more and better remedies to IBA grow louder, one hopes that new technical, legal, and social solutions that effectively address this challenge will appear. In the meantime, it is critical for victim-survivors to have access to support that they can take to best protect themselves. Easy and quick access to such information is essential as intrusive technologies such as deepfakes grow, and AI-based tools tread uncharted territories.

This guide comes with a disclaimer that IBA is a sensitive and complex issue that varies for each person. For exact solutions specific to a particular case, victim-survivors should receive direct legal, psychological, and technical support.

REQUESTING CONTENT REMOVAL

IBA content is often posted on pornographic websites, forums, cloud services meant for sharing/hosting images, channels and groups on instant messaging apps, social media, among other places (see infographic titled "Arc of image-based abuse"). There are ways to request the removal of this content.

For those who want to seek legal redressal, it is advisable to keep copies of this content as evidence before requesting removal. The evidence should be stored securely to prevent its loss or exposure. Refer to "Protect Your Sensitive Information" in the Security-in-a-Box guide for instructions..

- ### REMOVAL FROM PORNOGRAPHIC WEBSITES

Major porn websites such as PornHub and Xhamster have non-consensual content policies and a form for requesting removal of content. Once reported, the content is usually removed quickly. This guide serves as an introduction to these policies, and each platform has a different policy pertaining to IBA.

NOTE: *The following links contain NSFW content.*

PornHub policy: https://help.pornhub.com/hc/en-us/articles/4419871787027-Non-Consensual-Content-Policy
Content Removal Form: https://www.pornhub.com/content-removal

› Fill the report under "Abusive or Illegal Content"

Reference article: How to remove non-consensual videos from PornHub
Xhamster policy: https://xhamster.com/info/trust-and-safety
Contact form: https://xhamster.com/info/contact?subject=abuse
File the report under "Subject" › Report violation of our rules/ Content removal
"Type of request": Illegal exposure under non-consensual content

Some lesser known or smaller porn websites as well as IBA content sites that post non-consensual content to generate profit, do not have robust content removal policies. They also do not specify a way to request removal of their content. In such cases, a good approach is to read their privacy policy and terms of use or terms of service and determine how the content can be taken down. Look for these or similar phrases in the Terms of Service documents to determine whether the content violates site's own policies:

- pornography or sexually explicit content, or content that is otherwise obscene or lewd;
- violates any law
- threat to personal safety
- images of physical or sexual assault or abuse that appear to have been captured solely, or principally, for exploitative, prurient, or gratuitous purposes;
- content that is defamatory, abusive, vulgar, harassing
- invasive of a person's privacy/ violation of privacy

This list is indicative and not exhaustive.

Some IBA sites are intended for extortion, defamation or/ and vendetta . They may also display personally identifying information such as the victim's name, location, social media profile alongside their images. Some of these websites are on the dark web, "a part of the internet that lets people hide their identity and location from other people and from law enforcement". The sites may suggest to the viewers to email or text them to remove any content. It is *not advisable* to *directly email or text* them for these reasons:

1. **Reason:** It is possible to extract personal information from emails.
   Work around: To prevent disclosing information such as one's real name and email address, a new, pseudonymous email account can be set up solely for contacting the IBA website/service.
   Catch: It is still possible to extract internet protocol (IP) addresses from these emails. An IP address is a unique address assigned to every device connected to the internet. Using the IP address and geolocation technology, someone's approximate location at the level of the city, region or state can be determined. The IBA site or service already has photos or videos of the victim-survivor. Using a combination of location information, photos/videos and any other information that the site may already have about the victim-survivor, it is possible to gather granular information from social media, online databases, dumps obtained from data breaches, reverse image searches etc. This can pose a direct threat to their safety.

   It is important to understand that nothing on the internet is completely anonymous, and research suggests that even the most anonymised dataset can lead to re-identifying the exact person the information belongs to.
2. Some IBA content services provide their username on a messaging app as the mode to contact them. Depending on the features and security of the app, it may be possible for them to trace anyone who contacts them on the app. Calls (even missed calls) made via the app can potentially reveal IP addresses. Some apps have features that leak or expose the approximate location, phone number or other personally identifying information.

3. The IBA website or service may publicly expose or sell the personal information they gather. They may forward the information to entities such as other IBA sites, extortion gangs, cybercriminals or for advertising across the internet.

- ### REMOVAL FROM PLATFORMS

All major social media sites, search engines and messaging apps such as Telegram, Discord, and WhatsApp, among others have a feature for reporting abuse, usually under the head of "non-consensual intimate images" (NCII) or "pornography" for IBA content. For detailed information about the steps for removal, refer to the section "Takedown requests to platforms" in the paper, "Non-consensual intimate imagery: An overview" and the guide "Removing Sensitive Content from the Internet". Both of these references provide comprehensive information about removal across different platforms. The paper also elucidates on legal remedies, preventive strategies, digital security measures, and resources for victim-survivors.

The Image-Based Abuse Project by the Australian Research Council lists policies, guidelines, community standards and reporting options on 37 different platforms categorised as adult sites, dating apps, search engines and social media.

Microsoft recently announced a partnership with StopNCII.org – a project backed by Meta, "to pilot a victim-centered approach to [NCII] detection,"and tackling sexually explicit deepfakes, in its search engine Bing. StopNCII.org enables users to preventively request takedowns of their own IBA content from participating member platforms, which at the time of writing are Meta, Instagram, PornHub, Playhouse, TikTok, OnlyFans, Snapchat, Redgifs, Reddit, Threads, and Niantic apart from Bing.

Microsoft already has an online mechanism to report digital safety concerns across all its products, while Google Search offers a process to request removal of personal content under its content and product policies. Removal of the images from search results does not remove them from their source, but it limits their discoverability and reach on the public internet.

Recent research has shown that Twitter removes non-consensual nude or sexually explicit images much faster if they are reported as copyright violations than as only "non-consensual intimate images". We have also observed the same pattern of responses from Twitter when we supported some IBA victim-survivors in filing reports on Twitter.

IDENTITY MANAGEMENT

It is recommended that the victim-survivors maintain a separate and secure email account and file storage for all communication pertaining to the removal of the IBA content. The accounts should contain as little personally-identifiable information of the victim-survivor as possible to ensure their identity or communication is not compromised due to the bad security practices of the IBA-enabling websites. This is important as cloud-based services and forums that almost exclusively host IBA content only enable the "report abuse" option to logged-in users.

Some victims change their identities to escape the stigma and relentless harassment arising from IBA. Identity management is important to prevent new identities from being associated with their old identities or IBA content. Security Planner and "Protect the privacy of your online communication" in Security-in-a-Box are among many useful references that offer a starter guide to technical solutions.

Having a separate email account is also desirable from the perspective of wellbeing of the victim-survivor. It compartmentalises the correspondence and documents related to the IBA incidents, away from their everyday activities, and they can choose to visit the IBA-related accounts only when necessary or when they feel ready. It is important to keep records of all communications and requests being sent to websites, platforms and law enforcement, and to use a reliable virtual private network (VPN), or TOR browser, while sending the emails to IBA sites or services so that the victim-survivor's IP address is not compromised. (See Choosing the VPN That's Right for You, What is TOR and is it safe?, How to use TOR on Android and iPhone, How to use TOR for Windows)

- ### SETTING UP ALIAS ACCOUNTS

If it is not possible to set up and maintain a separate account, then,

1. Create and use one or more aliases to an existing secure email account.
    1. What is an alias and how does it improve online security?
    2. Instructions for how to create aliases in some popular email providers:
       Protonmail (Note: refer to "With new usernames" and not "With a plus sign (+).)"
       Outlook, Apple Mail
       Fastmail
       Mail.com
       Tutanota
       Gmail (Note: Refer to #6 below.)

       Some of these are paid services that offer a limited number of free aliases.
2. It is advisable to use a different alias for each site and service you need to contact. This applies even if you create a new email account for correspondence related to IBA incidents. Creating many aliases may sound tedious but there is usually a way to manage aliases within the email account and have identifiers corresponding to each of them.
3. The alias should be chosen such that it does not reveal the username or any other personally-identifiable information such as birth year or location. For example, the aliases of janedoe@example.com could be <randomname>@example.com or lazypineapple@example.com.
4. Create a separate folder for correspondence pertaining to the IBA incident(s).
5. Set up filters in your email account to sort emails addressed to the alias to the folder. Here are the instructions about filters on Gmail (and here), Protonmail, Microsoft Outlook, and Thunderbird.
6. Note that aliases of free Gmail accounts are formatted in a way that reveal the real email address and username. Thus, they are not suitable for this use case. For example, if the username is "janedoe", and the alias is "iba", then the alias address becomes **janedoe+iba@gmail.com** (technically called an "email

subaddress"), which reveals the real email address janedoe@gmail.com.

Similarly, it is possible to filter messages into a separate folder on some instant messaging apps, such as Signal, WhatsApp, Telegram and Facebook Messenger.

SEEKING TECHNICAL SUPPORT

There are various cases where technological support becomes essential for victim-survivors to prevent further harm. These could range from stolen or leaked images from compromised accounts or devices, and AI-generated photos that make the person appear nude or in sexually explicit acts. The repercussions could vary as well, from online or offline abuse, harassment, stalking or violence apart from the harm to reputation, privacy and dignity, which can lead to situations like impersonation or blackmailing for more sexually explicit content and/or money. In these cases, not only is it advised for the victim to not give in to demands of the perpetrator, but also technological remedies are necessary.

Every victim-survivor's risk profile and level of vulnerability to different kinds of threats is different. In some especially sensitive cases it is important to seek experts' help who can assess the situation, provide specific advice and find the best solutions and practices. The expert should carry out all activities while following the principle of do-no-harm. However, it is necessary to be cautious of unethical experts and charlatans, some of whom actively seek out victims.

Access Now Digital Security Helpline is a good resource to reach out to when technological assistance is needed. The Helpline operates 24/7, and responds to all requests within two hours.

USEFUL RESOURCES AND REFERENCES

Umibot, is a chatbot created at RMIT University in Australia, to help with queries related to image based abuse and where to seek help from. It is primarily meant for Australian users, but some of its information may be useful in other parts of the world.

"Resources" section of the paper Non-consensual intimate imagery: An overview.

SeeMe.Hk (Support against IBA in Hong Kong): The website uses the term image-based sexual violence (IBSV).

The author would like to thank Sapni G K for her inputs.

The next part in this guide suggests legal remedies for victim-survivors, especially in India.

[1] Downstream distribution is the re-posting of IBSA content done by entities that did not capture or create the content and did not originally post it on the internet or start its offline distribution. https://factordaily.com/the-crying-shame-of-image-based-abuse/