Characterizing Non-Consensual Intimate Image Abuse on Telegram Groups and Channels

Mirko Franco*
mifranco@math.unipd.it
Department of Mathematics
University of Padua
Padua, Italy

Ombretta Gaggi
gaggi@math.unipd.it
Department of Mathematics
University of Padua
Padua, Italy

Claudio E. Palazzi
cpalazzi@math.unipd.it
Department of Mathematics
University of Padua
Padua, Italy

Abstract

The non-consensual spread of intimate images and videos is a problematic phenomenon exacerbated by the rise of unmoderated instant messaging platforms like Telegram, where anonymity guarantees meet a loose regulatory framework. The popularity of Telegram groups, channels, and bots where intimate material is shared, along with the severe health consequences associated with this abuse, requires urgent responses and solutions. In this context, we discuss a tool aimed at characterizing the intricate network of Telegram online spaces related to non-consensual pornography and to locate (even slightly edited) copies of images shared across channels and groups. We also discuss the ethical issues associated with our proposal.

CCS Concepts

• **Social and professional topics** → **Computer crime**; **Pornography**; • **Information systems** → **Social networking sites**.

Keywords

Non-Consensual Pornography, Telegram, NCII, Revenge Porn

ACM Reference Format:

Mirko Franco, Ombretta Gaggi, and Claudio E. Palazzi. 2024. Characterizing Non-Consensual Intimate Image Abuse on Telegram Groups and Channels. In *4th International Workshop on OPEN CHALLENGES IN ONLINE SOCIAL NETWORKS (OASIS '24), September 10–13, 2024, Poznan, Poland*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3677117.3685008

1 Introduction

Non-consensual pornography - the dissemination of intimate images and videos without the depicted subject's consent - has received a boost from the rising diffusion of the Internet and instant messaging applications (e.g., WhatsApp, Telegram, Instagram Direct, etc.) [26]. The intimate material can have different origins. For example, the perpetrator might share stolen intimate material (e.g., after having taken photos of unaware people in a changing/fitting room, etc.) or content depicting minors (e.g., of a family members, etc.). Images and videos might also have been stolen from private cloud spaces or unencrypted hard disks. Moreover, intimate content might also be part of datasets related to medical examinations, such as mammography or urological examination. Finally, this phenomenon is also one of the negative consequences of sexting, i.e., the practice of sharing self-generated sexual content through technological mediums[1] (e.g., instant messaging applications, etc.).

The terms "*non-consensual pornography*" and "*revenge porn*" have been used interchangeably by researchers and major press for a long time. However, scholars have recently started to consider the latter as problematic. Indeed, the idea of revenge raises the risk of second victimization, and the research community deems that shifting the focus to the non-consensual nature of the sharing rather than to the pornographic one is necessary. Moreover, intimate material is not always shared to seek revenge, but the perpetrator might disseminate that content just for the pleasure of doing so or to obtain other erotic material.

The frequency of the phenomenon is difficult to assess. However, studies conducted in Australia and the US estimated that a percentage between 10% and 25% of participants had experienced non-consensual pornography in their life [19, 27, 34]. These percentages are very high if we consider the number of users using OSNs and the severe health consequences associated with non-consensual pornography, such as psychological disorders, self-harm, and even suicide [2, 24, 32]. In this context, we must also consider that messaging applications do not protect users from non-consensual intimate image abuse due to the possibility of sending any content to anyone without relevant limitations [10–12]. This fact is also due to the closed nature of messaging platforms compared to traditional social media like Facebook and Twitter.

Despite the increasing research efforts (and in response to them) to enhance and better understand content moderation on messaging systems [10–12, 22, 29, 33], alternative platforms have emerged, offering an unmoderated environment where users can freely share content and discuss without restrictions, where accessing the enormous amount of exchanged information is complex, and so even its analysis. One representative and famous yet controversial example is Telegram, a messaging application similar to WhatsApp, increasingly used by malicious actors, such as white supremacists [13], terrorists [38], crypto investors [25], and so on, to spread misinformation and illegal content, thanks to the anonymity guaranteed by the platform and the flexible regulatory framework[2]. Unfortunately, Telegram has become famous even for the spreading of non-consensual pornographic (i.e., erotic) images across its groups and channels [24, 35].

*Corresponding author.

OASIS '24, September 10–13, 2024, Poznan, Poland

ACM ISBN 979-8-4007-1082-7/24/09
https://doi.org/10.1145/3677117.3685008

[1] For a review of sexting definitions, see Barrense-Dias *et al.* [1]

[2] For more information, see https://telegram.org/faq

In addition to the presence of controversial content and borderline (if not illegal) activities, those groups are organized in complicated structures, where there are several copies of the same content and backup clones of some groups and channels, so even in case of ban, their activities do not come to an end [23, 30, 31]. Moreover, the spread of material and misinformation does not always happen in public groups but also in private (even huge) ones, requiring users to join the group before seeing the content; to join some of them, users have to explicitly ask for permission which has to be approved by an administrator. In some cases, users must start a Telegram bot to obtain the link to join a group. In other cases, the link is provided by the group administrator after having received proof of required payment, even though this is clearly illegal. Therefore, the structure (i.e., the topology) of these groups and channels is complex and not fully known, making control over the exchanged content, including its deletion, not possible.

In this context, inspired by the work of Franco *et al.* [10–12] and grounded on the work of Semenzin *et al.* [35], we discuss a possible tool capable of exploring and analyzing the structure of non-consensual pornography groups and channels on Telegram, to locate copies of images sent without the owner's consent (even in case of slight editing), if any, and to reconstruct their path within the network, if possible. Considering the closed nature of Telegram (and other instant messaging applications) and the consequent difficulties in moderating content and tracing cases of intimate image abuse, this tool can help shed light on this phenomenon, providing a comprehensive and real-time picture of the current landscape, and facilitating the search of potential non-consensual pornography cases. Moreover, our proposal is also useful for content creators whose content is often sent by malicious users outside the platform where they were originally posted, representing a case of copyright infringement, among other violations. For example, consider the case of OnlyFans - the famous subscription-based social media platform containing mainly pornographic content - where the content is often leaked on other OSNs (e.g., on Telegram), representing a case of non-consensual pornography [36]. To the best of our knowledge, this is the first attempt to analyze the topology of Telegram's groups and channels and to develop tools to characterize and better understand the famous yet unsolved problem of non-consensual pornography on this platform.

The remainder of this paper is organized as follows. Section 2 presents a review of the relevant literature. Section 3 provides some background information on Telegram. Section 4 presents and discusses an approach to characterize and better understand the phenomenon of non-consensual pornography on Telegram groups and channels, as well as to search material shared across them. Section 5 discusses the ethical issues associated with the development of the tool proposed in this work and its limitations. Finally, we draw our conclusion and present some future research directions in Section 6.

2 Related Work

In this section, we provide an overview of the relevant literature about the analysis of the topology and characteristics of OSNs, as well as of recent research efforts on contrasting non-consensual pornography.

2.1 Analysis of Topology and Characteristics of Online Social Networks

Several studies analyzed the characteristics and the structure of OSNs. For example, Chang *et al.* [3] presented a comprehensive statistical overview of Tumblr - one of the most famous microblogging platforms - and compared it to other popular social networking services like Facebook and Twitter. Guidi *et al.* [16] investigated and modeled the interaction of users within 18 heterogeneous groups using the concept of Member Network, defined as the network of users' active relationships with the other group members. Their results suggested that each member network presented a hierarchical structure coherent with Dunbar's Circles. De Salve *et al.* [7] proposed a general framework to predict the most influential users within Facebook groups.

Focusing on instant messaging applications, Melo *et al.* [28, 29] investigated the circulation of misinformation across WhatsApp groups dedicated to political discussion in Brazil by analyzing 10 million messages from 1101 public groups. Their results showed several flaws in managing viral content on WhatsApp, in particular regarding the feature "*Forwarded Many Times*", and suggested that misinformation campaigns rely on these flaws to reach a broader audience. Instead, Hoseini *et al.* [21] characterized public groups from Discord, Telegram, and WhatsApp, whose URL (or invitation link) had been shared on Twitter. In particular, they figured out that a consistent number of the analyzed Telegram groups were about pornography and sex, as well as that the URLs were ephemeral, showing how these groups have a limited lifespan. Moreover, they discovered the possibility of obtaining Personally Identifiable Information (PII) such as phone numbers, highlighting the need to design safer messaging applications and improve users' awareness on this topic. Júnior *et al.* [22] developed a web-based tool to monitor the political debate on Telegram's groups and channels during the 2022 Brazilian elections.

Considering the topic of intimate image abuse, Semenzin *et al.* [35] analyzed the role of Telegram in the unauthorized sharing of intimate images and how this is associated with the dynamics of gender inequality, focusing on the Italian case. However, no previous work analyzed the structure of Telegram's non-consensual pornography groups and channels. In this context, our research advances the current state of the art.

2.2 Contrasting Non-Consensual Pornography

The topic of sexting and its consequences has been extensively addressed by the Human-Computer Interaction (HCI) and Computer-Supported Cooperative Work (CSCW) research communities. For example, Razi *et al.* [32] analyzed 4180 posts on an online peer support platform to understand how adolescents seek support about sexting and the potential consequential issues, such as unwanted sexual solicitation or the unauthorized sharing of intimate content. Following the same direction, Hartikainen *et al* [18] examined how adolescents respond and support their peers about the aforementioned topics and how teenagers tend to agree on a set of rules around safe sexting. Coduto *et al.* [4] investigated the how people manage shared sexual content after a relationship breakup and provided some design suggestions to build safer systems for sexting while keeping the breakeup in mind.

The issue of non-consensual pornography has also been addressed from a technological point of view. For example, Franco *et al.* proposed some guidelines for developers to build messaging systems safe by design for sexting in [11] and described the proposed platform, named *SafeSext*, in [12]. Moreover, considering the rising decentralization of social services [5, 14, 15], Franco *et al.* [10] also presented two decentralized solutions to contrast the unauthorized sharing of private content, including non-consensual pornography. Instead, Falduti *et al.* [9] introduced a flow-based chatbot to support victims in reporting cases of intimate image abuse. Following this direction, De Angeli *et al.* [6] evaluated different interaction styles with user interfaces for reporting non-consensual pornography.

However, no prior research focused on contrasting and better understanding intimate image abuse in real and popular messaging platforms like Telegram. In this sense, our contribution advances the state-of-the-art, offering tools for law enforcement and to protect users more effectively and promptly.

3 Background: Telegram

Released in 2013, Telegram is an instant messaging platform with around 800 million active users monthly [37]. In particular, the number of active users has seen a rise in 2021, when many of them moved from WhatsApp to Telegram after the update of the privacy policy of WhatsApp [20].

On Telegram, users can share text messages, images, videos, audio, stickers, files weighing up to 2 GB, contacts, and their real-time position. Users can also make audio and video calls, without sharing the phone number or other private information. Besides the traditional one-to-one chats, Telegram also offers:

- **Groups**: collaborative spaces where the communication is many-to-many, i.e., users can communicate simultaneously, containing up to 200.000 members. Administrators can manage the groups settings, including adding or removing members, setting permission for posting content, pinning important messages, and more. Groups can be either public or private. Public groups are accessible to anyone and can be found through search, while private groups require an invitation to join, like an invitation link.
- **Channels**: spaces designed for the broadcasting of messages that can have an unlimited number of subscribers. Unlike groups, channels are typically used for one-way communication from the administrators to the subscribers. Similarly to groups, channels can be either public or private. Public channels can be searched and joined by anyone, while private channels require an invitation link.
- **Bots**: specialized automated accounts designed to interact with users and groups and perform a variety of tasks, from providing information and notifications to managing groups activities, through programmed commands and responses. Developers can build Telegram's bots by leveraging the Telegram Bot API.

Unfortunately, as mentioned above, these groups, channels, and bots are used for several harmful or even illegal activities, including the non-consensual sharing of intimate images, by exploiting an intricate network where access and detection are not always straightforward.

The dimensions of these spaces (groups and channels) are not predictable but range from a few tens to 30,000 participants, with peaks up to 60,000 members for those aimed at spread content made with hidden cameras [35]. Considering these numbers, characterizing the phenomenon and developing tools to track the unauthorized sharing of intimate material is more than urgent to safeguard people's psychophysical integrity and guarantee safer and more enjoyable online environments.

4 An Approach to Analyze Non-Consensual Pornography on Telegram

To shed light on the phenomenon of non-consensual pornography on Telegram groups and channels, we design and propose to develop a comprehensive tool to reconstruct the intricate network and relationships of groups, channels and bots and to search material shared across these (closed) online spaces, leveraging the Telegram API and/or TDLib. More specifically, we envision the development of a customized web client for Telegram, accessible only to a limited set of authorized users (e.g., Internet police).

Algorithm 1 Algorithm for building the graph starting from some seed groups, channels, or bots (online spaces)

```
function BUILD-GRAPH-TELEGRAM(seedSpaces)
    Stack ← []
    push(Stack, seedSpaces)
    graph ← []
    while Stack is not empty do
        space ← pop(Stack)
        if space not visited then
            space.visited = True
            URLs ← space.URLs
            for all URL in URLS do
                if URL not reachable then
                    space.remove(URL)
                else
                    destinationSpace ← URL.destinationSpace
                    push(Stack, destinationSpace)
                end if
            end for
            append(graph, space)
        end if
    end while
    return graph
end function
```

To reconstruct the complex network of groups, channels, and bots and better understand its structure and characteristics, such as the influential spreaders, we must represent it as a graph $G = (V, E)$, where the vertices V are the aforementioned online spaces while the edges E represents the relationships among them. The nodes are of thee different types, each representing one kind of space. The edges can represent different relationships. For example, the most obvious is that if there is an edge between v_1 and v_2, then v_1 has a link (i.e., an URL) pointing to v_2.

To create the graph, we must visit the various nodes (i.e., groups, channels, etc.) starting from some seed nodes, using Depth-First or

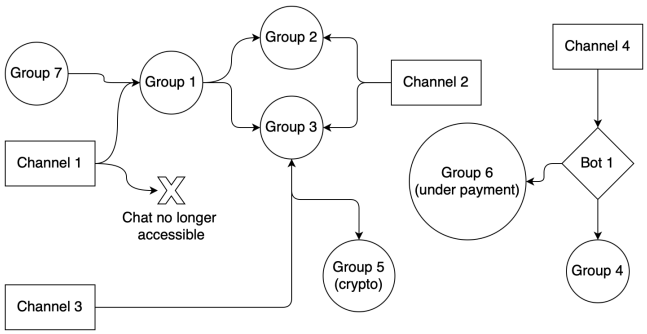

Figure 1: Example of possible structure of the non-consensual pornography network on Telegram

Breadth-First strategies. We report in Algorithm 1 the pseudocode of a (multi-source) DFS adapted for our purposes. We assume that all the nodes are initially not visited, as they are not known in the real scenario. The function returns the graph represented in the adjacency-list form, which consists of an array Adj of $|V|$ lists, one for each vertex. For each $u \in V$, the adjacency list $Adj[u]$ includes all the vertices v such that there is an edge $(u, v) \in E$.

This algorithm provides a graph representation of the structure created by these different groups. Figure 1 shows an example of this complex set of groups, channels, and bots. This representation allows further analyses, such as the computation of measures to identify nodes that influence the network (e.g., closeness centrality, etc.), to count the connected components of the graph, to understand the flow of information, and so on.

To detect cases of intimate image non-consensual sharing abuse within this network, we need first to be able compare images efficiently and define when two pictures can be considered the same. First of all, we cannot compare images directly for efficiency reasons, but we must compute more concise representations, like hash values, and compare them. Moreover, messaging platforms usually apply some form of compression before sending pictures to the recipient, or malicious users can edit them to avoid detection by automated systems, thus modifying the bit-level representation while keeping (quite) unaltered the visualization. If interested in detecting only bit-level identical copies of an image, we could use one of the cryptographic hashing functions, such as MD5 or SHA-1, which map different pictures (even just for one bit) to diverse hash values. The probability of error (i.e., computing the same hash values for two different images) is equal to the likelihood of collision of the hash function, which is nearly zero. As already mentioned, the characteristic (and the problem) of this type of hashing functions is that a single bit change in the picture will result in a significantly diverse hash value. This means that by slightly editing an image, a malicious user would be able to avoid the image to be detected as corresponding to the original one.

Therefore, as we need to detect even edited copies of an image, we must use the so-called perceptual hashing, as also mentioned and done in other recent works [10–12, 23, 30]. Perceptual hashing is a mapping of similar images to similar hash values and different pictures to different fingerprints [8]. More formally, perceptual hashing functions respect the following properties:

(1) Uniform distribution of hash values

$$P[H(X) = \alpha] = \frac{1}{2^L}, \forall \alpha \in \{0,1\}^L \quad (1)$$

(2) Pairwise independence of visually distinct pictures X and Y

$$P[H(X) = \alpha | H(Y) = \beta] \approx P[H(X) = \alpha], \forall \alpha, \beta \in \{0,1\}^L \quad (2)$$

(3) Invariance for visually similar pictures X and $\hat{X}$

$$P[H(X) = H(\hat{X})] \approx 1 \quad (3)$$

(4) Dissimilarity for visually different pictures X and Y

$$P[H(X) = H(Y)] \approx 0 \quad (4)$$

where P represents probability, X, $\hat{X}$, and Y are pictures, α and β are hash values, H is the hashing function, and {0,1} denotes binary strings of length L. Considering the last two properties, once we have the hash values of two images, we can easily compute a distance measure (e.g., the Euclidean distance) and use a prefixed threshold for comparison (e.g., if the computed distance is below the threshold, then the two pictures are the same).

Algorithm 2 Algorithm to locate even (slightly) edited copies of images shared across groups and channels

```
function SEARCH-IMAGE(graph, currentImage)
    nodes ← graph.vertices
    hashValue ← getHashValue(currentImage)
    occurencies ← []
    for all node in nodes do
        listOfImages ← node.sentImages
        for all image in listOfImages do
            if IsTheSame(currentImage, image) = True then
                add(occurencies, node)
            end if
        end for
    end for
    return occurencies
end function
```

Once we have decided when two pictures have to be considered the same, to search for copies of an image within the graph, we need to iterate over all the nodes (i.e., the groups and channels). Then, for each node of the network, we must check whether any of its images is equal to the considered picture (the one we are looking for), as shown in Algorithm 2, using the hashing function. The result is the list of nodes, equivalent to groups and channels, where an occurrence has been found. A possible example of visualization is shown in Figure 2. The user (e.g., law enforcement) can upload an image through an input field. The system executes Algorithm 2, possibly discovering groups and channels where the considered picture has been shared without the owner's consent. The system visualizes each occurrence along with the group/channel's name, the number of copies, and the sender's username on a protected webpage.

Unfortunately, the topology of the Telegram non-consensual pornography groups, channels, and bots is not fixed and stable over time. Conversely, groups are continuously ended and recreated, and the flow of messages and multimedia content across them is

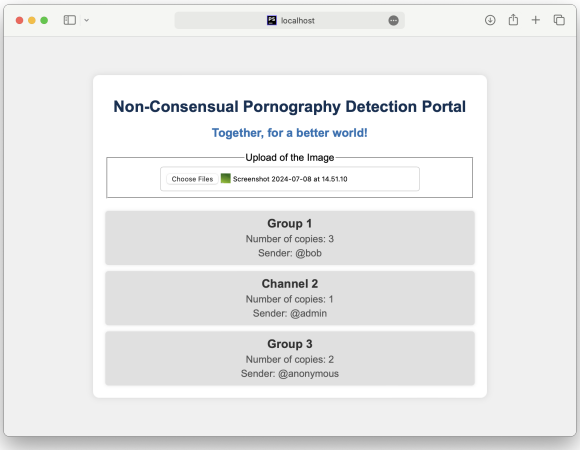

Figure 2: Possible visualization of the search results of an image across groups and channels

constant and enormous, especially in large groups. Therefore, the proposed tool should periodically update its knowledge about the structure of the underlying set of groups and channels, also opening the possibility of performing temporal analyses on the graph to understand how the structure of those spaces changes over time.

5 Limitations and Ethical Issues

Several ethical concerns need to be addressed before developing the proposed system. First and foremost, the development of the tool proposed in this work requires having access to Telegram's non-consensual pornography groups and channels, including their members and content. Although these data are already available on Telegram, there is no consensus yet on how to manage research on closed groups, as demonstrated by the case of the T3 research team [39]. While we agree on the importance of obtaining users' informed consent and protecting their privacy, we cannot reveal our purpose and identities to the members of groups and channels without undermining our research's and tool's aim. This methodology is considered ethical when no other options are available, and it was also used in [35]. We believe that the public relevance of the problem of non-consensual pornography on Telegram and the damages to the victims of this phenomenon, as well as the lack of awareness and knowledge around it, justify this research and its methodology. Nonetheless, we need approval from an Institutional Review Baord (IRB) before accessing Telegram's groups and developing the tool. To further preserve users' privacy, the tool must be deployed on a private server with a strict access management policy.

Moreover, preserving researchers' well-being is imperative, considering the sensitive nature of the topic and the chance for them to come into contact with objectionable content, as usual in the management of human moderators workforce [17]. For this reason, implementing proper training on how to conduct research on these sensitive topics and providing access to psychological support to the research team would be helpful.

Training is also essential for the legal aspects of this research. Indeed, while developing the aforementioned tool is technically feasible, we must comply with Telegram's terms of service and national and international regulations. In particular, these groups and channels might contain illegal content, such as pornographic material depicting underaged people. Child pornography is prohibited in most countries; understanding how to manage even these aspects is essential before undertaking the development.

Finally, despite the efforts to cover and reconstruct the largest part of the network, some groups and channels might not be discovered (e.g., if they are not connected with other groups). In addition, payment through PayPal or similar methods might be required to access some groups, even if it is illegal. Accessing those groups might not be possible due to institutional and legal constraints, so analyzing the content shared within those spaces would not be possible.

6 Conclusion

Non-consensual pornography - the non-consensual sharing of intimate content (e.g., images, videos, etc.) without the depicted subject's consent - has been amplified with the diffusion of the Internet and OSNs while being considered a criminal offense (e.g., in Italy since April 2019). The anonymity and the loose regulatory framework offered by unmoderated platforms like Telegram have been the ideal context for the rise of a dense and intricate network of groups, channels, and bots with up to 60,000 members aimed at the diffusion of intimate material, also becoming an issue of public debate in some famous cases. The size of the phenomenon and the severe health consequences of non-consensual pornography require us to act urgently to protect people's well-being and build safer online communities, especially for the most fragile part of the population.

In this context, we have proposed the development of a comprehensive tool to characterize and analyze the structure of the set of Telegram groups, channels, and bots aimed at disseminating intimate content, as well as to locale (even slightly edited) copies of intimate images and videos. Our envisioned tool is composed of a web client, accessible only to authorized people, that leverages the Telegram API and/or TDLib to communicate with Telegram, and can reconstruct the graph representing the structure of the various channels, groups, and bots starting from some seeds. Moreover, the proposed approach can also be applied to other messaging platforms if those applications provide the necessary APIs and the possibility to access their online spaces through URLs or other equivalent ways.

Our research endeavors are poised to expand in several directions. Primarily, we would like to address the ethical issues associated with the development of the proposed system, as well as to involve potential stakeholders, such as law enforcement and the Agency for Digital Italy (AgID)[3], to discuss the foreseen impact of the tool on society. Moreover, we plan to evaluate the compliance of the proposed tool with Telegram's terms of service and national and international regulations. Finally, we would like to extend the proposed approach to other illegal, inappropriate or problematic content.

[3]https://www.agid.gov.it/it

References

[1] Yara Barrense-Dias, André Berchtold, Joan-Carles Surís, and Christina Akre. 2017. Sexting and the Definition Issue. *Journal of Adolescent Health* 61, 5 (2017), 544–554. https://doi.org/10.1016/j.jadohealth.2017.05.009

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

[3] Yi Chang, Lei Tang, Yoshiyuki Inagaki, and Yan Liu. 2014. What is Tumblr: a statistical overview and comparison. *SIGKDD Explor. Newsl.* 16, 1 (sep 2014), 21–29. https://doi.org/10.1145/2674026.2674030

[4] Kathryn D Coduto and Allison McDonald. 2024. "Delete it and Move On": Digital Management of Shared Sexual Content after a Breakup. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 918, 16 pages. https://doi.org/10.1145/3613904.3642722

[5] Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, and Krzysztof Rzadca. 2010. *Decentralized Online Social Networks.* Springer US, New York, NY, 349–378. https://doi.org/10.1007/978-1-4419-7142-5_17

[6] Antonella De Angeli, Mattia Falduti, Maria Menendez-Blanco, and Sergio Tessaris. 2023. Reporting non-consensual pornography: clarity, efficiency and distress. *Multimedia Tools and Applications* 82, 9 (2023), 12829 – 12858. https://doi.org/10.1007/s11042-022-14291-z

[7] Andrea De Salve, Paolo Mori, Barbara Guidi, Laura Ricci, and Roberto Di Pietro. 2021. Predicting Influential Users in Online Social Network Groups. *ACM Trans. Knowl. Discov. Data* 15, 3, Article 35 (apr 2021), 50 pages. https://doi.org/10.1145/3441447

[8] Ling Du, Anthony T.S. Ho, and Runmin Cong. 2020. Perceptual hashing for image authentication: A survey. *Signal Processing: Image Communication* 81 (2020), 115713. https://doi.org/10.1016/j.image.2019.115713

[9] Mattia Falduti and Sergio Tessaris. 2022. On the Use of Chatbots to Report Non-consensual Intimate Images Abuses: the Legal Expert Perspective. In *Proceedings of the 2022 ACM Conference on Information Technology for Social Good* (Limassol, Cyprus) *(GoodIT '22)*. Association for Computing Machinery, New York, NY, USA, 96–102. https://doi.org/10.1145/3524458.3547247

[10] Mirko Franco, Ombretta Gaggi, Barbara Guidi, Andrea Michienzi, and Claudio E. Palazzi. 2023. A decentralised messaging system robust against the unauthorised forwarding of private content. *Future Generation Computer Systems* 145 (2023), 211 – 222. https://doi.org/10.1016/j.future.2023.03.025

[11] Mirko Franco, Ombretta Gaggi, and Claudio E. Palazzi. 2022. Improving Sexting Safety through Media Forwarding Control. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. 1–6. https://doi.org/10.1109/CCNC49033.2022.9700555

[12] Mirko Franco, Ombretta Gaggi, and Claudio Enrico Palazzi. 2024. Can Messaging Applications Prevent Sexting Abuse? A Technology Analysis. *IEEE Transactions on Mobile Computing* 23, 2 (2024), 1613 – 1626. https://doi.org/10.1109/TMC.2023.3238189

[13] David Gildert. 2023. White Supremacist Active Clubs Are Breeding on Telegram. https://www.wired.com/story/active-clubs-telegram/. Accessed 28th June 2024.

[14] Barbara Guidi. 2020. When Blockchain meets Online Social Networks. *Pervasive and Mobile Computing* 62 (2020), 101131. https://doi.org/10.1016/j.pmcj.2020.101131

[15] Barbara Guidi, Andrea Michienzi, and Laura Ricci. 2021. A Graph-Based Socioeconomic Analysis of Steemit. *IEEE Transactions on Computational Social Systems* 8, 2 (2021), 365–376. https://doi.org/10.1109/TCSS.2020.3042745

[16] Barbara Guidi, Andrea Michienzi, Laura Ricci, and Vincenzo Ambriola. 2021. Analysing Dunbar Circles in Facebook Groups. In *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. 1–6. https://doi.org/10.1109/CCNC49032.2021.9369495

[17] Alon Halevy, Cristian Canton-Ferrer, Hao Ma, Umut Ozertem, Patrick Pantel, Marzieh Saeidi, Fabrizio Silvestri, and Ves Stoyanov. 2022. Preserving integrity in online social networks. *Commun. ACM* 65, 2 (jan 2022), 92–98. https://doi.org/10.1145/3462671

[18] Heidi Hartikainen, Afsaneh Razi, and Pamela Wisniewski. 2021. Safe Sexting: The Advice and Support Adolescents Receive from Peers regarding Online Sexual Risks. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 42 (apr 2021), 31 pages. https://doi.org/10.1145/3449116

[19] Nicola Henry, Anastasia Powell, and Asher Leigh Gevaux Flynn. 2017. *Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse: A Summary Report.* RMIT University.

[20] Alex Hern. 2021. WhatsApp loses millions of users after terms update. https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update. Accessed 2nd July 2024.

[21] Mohamad Hoseini, Philipe Melo, Manoel Júnior, Fabrício Benevenuto, Balakrishnan Chandrasekaran, Anja Feldmann, and Savvas Zannettou. 2020. Demystifying the Messaging Platforms' Ecosystem Through the Lens of Twitter. In *Proceedings of the ACM Internet Measurement Conference* (Virtual Event, USA) *(IMC '20)*. Association for Computing Machinery, New York, NY, USA, 345–359. https://doi.org/10.1145/3419394.3423651

[22] Manoel Júnior, Philipe Melo, Ana Paula Couto da Silva, Fabrício Benevenuto, and Jussara Almeida. 2021. Towards Understanding the Use of Telegram by Political Groups in Brazil. In *Proceedings of the Brazilian Symposium on Multimedia and the Web* (Belo Horizonte, Minas Gerais, Brazil) *(WebMedia '21)*. Association for Computing Machinery, New York, NY, USA, 237–244. https://doi.org/10.1145/3470482.3479640

[23] Manoel Júnior, Philipe Melo, Daniel Kansaon, Vitor Mafra, Kaio Sa, and Fabricio Benevenuto. 2022. Telegram Monitor: Monitoring Brazilian Political Groups and Channels on Telegram. In *Proceedings of the 33rd ACM Conference on Hypertext and Social Media* (Barcelona, Spain) *(HT '22)*. Association for Computing Machinery, New York, NY, USA, 228–231. https://doi.org/10.1145/3511095.3536375

[24] Rachel Kraus. 2020. Telegram's massive revenge porn problem has made these women's lives hell. https://mashable.com/article/nudes-revenge-porn-crime-telegram. Accessed 30th June 2024.

[25] Massimo La Morgia, Alessandro Mei, Francesco Sassi, and Julinda Stefa. 2020. Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations. In *2020 29th International Conference on Computer Communications and Networks (ICCCN)*. 1–9. https://doi.org/10.1109/ICCCN49398.2020.9209660

[26] Sophie Maddocks. 2018. From Non-consensual Pornography to Image-based Sexual Abuse: Charting the Course of a Problem with Many Names. *Australian Feminist Studies* 33, 97 (2018), 345 – 361. https://doi.org/10.1080/08164649.2018.1542592

[27] Sheri Madigan, Anh Ly, Christina L. Rash, Joris Van Ouytsel, and Jeff R. Temple. 2018. Prevalence of multiple forms of sexting behavior among youth: A systematic review and meta-analysis. *JAMA Pediatrics* 172, 4 (2018), 327 – 335. https://doi.org/10.1001/jamapediatrics.2017.5314

[28] Philipe de Freitas Melo, Mohamad Hoseini, Savvas Zannettou, and Fabrício Benevenuto. 2024. Don't Break the Chain: Measuring Message Forwarding on WhatsApp. *Proceedings of the International AAAI Conference on Web and Social Media* 18, 1 (May 2024), 1054–1067. https://doi.org/10.1609/icwsm.v18i1.31372

[29] Philipe de Freitas Melo, Carolina Coimbra Vieira, Kiran Garimella, Pedro O. S. Vaz de Melo, and Fabrício Benevenuto. 2020. Can WhatsApp Counter Misinformation by Limiting Message Forwarding?. In *Complex Networks and Their Applications VIII*, Hocine Cherifi, Sabrina Gaito, José Fernendo Mendes, Esteban Moro, and Luis Mateus Rocha (Eds.). Springer International Publishing, Cham, 372–384.

[30] Massimo La Morgia, Alessandro Mei, and Alberto Maria Mongardini. 2023. TGDataset: a Collection of Over One Hundred Thousand Telegram Channels. arXiv:2303.05345 [cs.CY] https://arxiv.org/abs/2303.05345

[31] Massimo La Morgia, Alessandro Mei, Alberto Maria Mongardini, and Jie Wu. 2021. Uncovering the Dark Side of Telegram: Fakes, Clones, Scams, and Conspiracy Movements. arXiv:2111.13530 [cs.CY] https://arxiv.org/abs/2111.13530

[32] Afsaneh Razi, Karla Badillo-Urquiola, and Pamela J. Wisniewski. 2020. Let's Talk about Sext: How Adolescents Seek Support and Advice about Their Online Sexual Experiences. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376400

[33] Gustavo Resende, Philipe Melo, Hugo Sousa, Johnnatan Messias, Marisa Vasconcelos, Jussara Almeida, and Fabrício Benevenuto. 2019. (Mis)Information Dissemination in WhatsApp: Gathering, Analyzing and Countermeasures. In *The World Wide Web Conference* (San Francisco, CA, USA) *(WWW '19)*. Association for Computing Machinery, New York, NY, USA, 818–828. https://doi.org/10.1145/3308558.3313688

[34] Yanet Ruvalcaba and Asia A. Eaton. 2020. Nonconsensual pornography among U.S. adults: A sexual scripts framework on victimization, perpetration, and health correlates for women and men. *Psychology of Violence* 10, 1 (2020), 68 – 78. https://doi.org/10.1037/vio0000233

[35] Silvia Semenzin and Lucia Bainotti. 2020. The Use of Telegram for Non-Consensual Dissemination of Intimate Images: Gendered Affordances and the Construction of Masculinities. *Social Media and Society* 6, 4 (2020). https://doi.org/10.1177/2056305120984453

[36] Ananta Soneji, Vaughn Hamilton, Adam Doupé, Allison McDonald, and Elissa M. Redmiles. 2024. "I feel phisically safe but not politically safe": Understanding the Digital Threats and Safety Practices of OnlyFans Creators. In *Proceedings of the 33rd USENIX Conference on Security Symposium* (Philadelphia, PA, USA) *(SEC '24)*. USENIX Association, USA.

[37] Statista. 2024. Number of monthly active Telegram users worldwide from March 2014 to July 2023. https://www.statista.com/statistics/234038/telegram-messenger-mau-users/. Accessed 2nd July 2024.

[38] Rebecca Tan. 2017. Terrorists' love for Telegram, explained. https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter. Accessed 28th June 2024.

[39] Michael Zimmer. 2010. "But the data is already public": On the ethics of research in Facebook. *Ethics and Information Technology* 12, 4 (2010), 313 – 325. https://doi.org/10.1007/s10676-010-9227-5