NON CONSENSUAL PORNOGRAPHY AND INTERMEDIARY LIABILITY

- AKHIL DEO

Introduction

The phrase nonconsensual pornography captures a wide range of conduct such as revenge porn, material obtained by hidden cameras, stolen photos and recordings of sexual violence. Take for example the „celebrity leaks" of 2014, where a website called 4chan.org uploaded nude images of over 100 women, including many well-known celebrities after hacking into private iCloud accounts.[1]

The psychological and emotional toll that such conduct can have on a person is enormous, particularly because dissemination may occur within the social circles of most victims. Often, such events also negatively impact higher education and employment prospects, forcing victims to find new identities and even change residence.

In India, a confusing plethora of legislations criminalize such pornography. [2] However, because online intermediaries are the preferred method of dissemination, it becomes important to address the role they might play in curbing such practices and the liability they might incur for failing to do so.

The limitations of intermediary liability

The current understanding on intermediaries is that they are neutral communications platforms with little or no control over the material that passes through them and are therefore immune from liability for any illegal conduct on their platform.[3] In the US, this shield extends to intermediaries who refuse to remove sexually compromising photographs of victims, even after notice.[4]

Recently however, this understanding has come under increasing scrutiny especially with respect to non consensual pornography. Some advocacy groups have studied the policies of major intermediaries and found that they lacked commitments to human rights apart from free speech and that this position often works to the detriment of women.[5]

In India, Section 79 of the Information Technology Act states that intermediaries will be held liable only under two circumstances: If the intermediary was involved in the commission of the unlawful act or upon receiving actual knowledge of unlawful content, it fails to expeditiously disable access to that material.

Rich McCormick, „Hack leaks hundreds of nude celebrity photos" The Verge, 1 September, 2014.

1 See generally, sections 354A (sexual harassment), 354C (voyeurism), 354D (stalking) and 509 (outraging modesty) of the Indian Penal Code 1857. See also S.67 & S.66E of the IT Act 2000.

2 See generally, Communications Decency Act, 47 USC § 230(c) (1996), Art. 12-15, E-Commerce Directive 2000 (Directive 2000/31/EC), S. 79 of the IT Act 2000.

3 Barnes v Yahoo! Inc., 570 F3d 1096 (9th Circ 2009).

4 Carly Nyst, „End Violence: Internet Intermediaries and Violence against Women Online" (Executive Summary and Findings, Association for Progressive Communications, July 2014) at p. 3.

Further, the list of unlawful content under the Guidelines [6] includes „pornography" and content which is „invasive of another's privacy" and intermediaries are obligated to take down such material within 36 hours of receiving „actual knowledge", which was held to imply an order from a competent authority, usually being a court.[7] While this decision was celebrated in terms of limiting the „chilling effect" that vague intermediary liability laws can have on free speech, it raises a few practical issues in terms of their obligations with respect to pornographic content.

First, the primary victims happen to be women, many of whom find it intimidating to institute legal proceedings and would rather avoid the stigma that comes attached with it, especially in conservative and patriarchal societies like India.[8] Second, while popular intermediaries such as Facebook have set up mechanisms through which victims can seek redress,[9] other websites that actively solicit non consensual pornography[10] are shielded by intermediary liability laws in the US, making them unlikely to comply with Indian Court orders.

Today online conduct relating to child pornography, hate speech and terrorism have forced stakeholders to reassess the role of the intermediaries.[11] Further, tools such as PhotoDNA, which can function across platforms like social media websites and messenger applications such as WhatsApp, have given companies the technological prowess to deal with harmful content such as child pornography in a targeted manner, reducing collateral damage to legitimate expression.[12]

This has lead governments to point out that if intermediaries do have the technological capacity to filter one type of content, this should extend to other harmful conduct as well.[13]

Emerging options

Ultimately such simplistic models of regulating intermediaries will do more harm than good. A useful model must be based on the effectiveness of remedying harm and limiting the financial and social cost incurred by the intermediary because the key justifications for limiting intermediary liability remain strong.

One emerging option is the „right to be forgotten" (RTBF). In 2013, the European Court of Justice ruled that Google and other „data controllers" could be obligated to or de-link personal information

---

6 See generally Information Technology (Intermediary Guidelines) Rules, 2011.

7 Shreya Singhal v. Union of India, 2015 (4) SCALE 1.

8 Neha Dixit, „„Why did you let him shoot that?" An Indian woman"s story of revenge porn", Scroll, 12 February, 2017.

9 See Facebook, Community Standards (2017).

10 Abby Rogers, „The Man Behind a Website That Let You Post Nude Pics of Your Ex is Back with a Brand New Venture", Business Insider, 29 November 2012.

11 Monica Horten, „Liability and responsibility: new challenges for internet intermediaries", LSE Media Policy Project Blog, 20 October 2016.

12 Catharine Smith, „Facebook Adopts Microsoft Photo DNA To Remove Child Pornography", Huffington Post, 20 July 2011.

13 Select Committee on Communications, Social Media and Criminal Offences Inquiry, House of Lords Paper No 37, Session 2014–15 (2014) at p. 84.

of an individual that is „inaccurate, inadequate, irrelevant or excessive".[14] Protection Regulation (GDPR) in fact institutionalizes this right and member states to create RTBF laws.[15]

It is conceivable that this could also extend to de-indexing URL"s which carry non consensual pornographic content. [16] Google already allows users to flag such content, which will then be removed from the search results.[17] Interestingly, a 2014 the Karnataka High Court judgment upheld a request to de-index a certain information from search engines, finding that the right to be forgotten exists as a rule in *'sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned*".[18]

While the RTBF will require a search engine to strike a balance between an individual"s privacy and public interest in accessing information, some forms of conduct should not pose a difficult challenge. For example, a 2014 Google Advisory Report while detailing the types of information that "bias toward an individual"s strong privacy interest", concluded that information on an individual"s intimate or sex life holds increased weight against public interest.[19] Several scholars have similarly concluded that there is a strong case for a RTBF procedure for non consensual pornography because there is no countervailing public interest in such information.[20]

Search engines like Google are primary gateways into the internet, making them the least cost avoider. It follows that if certain content cannot be found on Google, wide spread dissemination becomes difficult. This will remedy much of the harm that victims face.

While the RTBF does present an interesting option for limiting the dissemination of non consensual pornography, it raises proportionality concerns when applied to other expression where the boundaries are less clear. Moreover, it is unclear if this will only apply to search engines, which only de-list content on the search result or if intermediaries like Facebook will also have to comply, which would imply that the content would truly be erased,[21] which might raise additional free speech issues.

---

14 Google Spain SL v Agencia Española de Protección de Datos (C-131/12) [2014] ECJ 317.

15 Daphne Keller, „The final draft of Europe"s "right to be forgotten" law", Media Policy Project Blog, LSE, 18 December 2015.

16 Aidan Forde, „Implications of the Right to Be Forgotten" (2015) 18 Tulane Journal of Technology and Intellectual Property 83, 119.

17 Joanna Walters, „Google to exclude „revenge porn" from internet searches", The Guardian, 21 June, 2015. See also, Google, European Privacy Requests for Search Removals, 20 March 2017.

18 Sri Vasunathan vs The Registrar, General Writ Petition No. 62038 of 2016.

19 Google Advisory Council „Advisory Council Final Report" (2014).

20 N. Suzor et al, „Non-consensual porn and the responsibility of online intermediaries" 40(3) Melbourne University Law Review (Forthcoming, 2017) at p.16.

21 Daphne Keller, „The "Right to Be Forgotten" and National Laws Under the GDPR", Centre for Internet and Society Blog, Stanford, April 27, 2017.

Conclusion

Ultimately, the expansion of „digital lives" and criminal conduct online will force governments and intermediaries to develop public policy options that secure a varied set of digital rights. Making intermediaries liable for harmful conduct will only serve to hamper to the growth of internet based services.

A better model is intermediary responsibility, which must take into account clear identification of harmful conduct, transparent procedures, technological and cost effectiveness. While this is a complex issue, it is increasingly necessary to have this conversation in order to develop effective regulations.

(Word count: 1090)