Content Take Downs on the World Wide Web

A Global Reality

Research Methodology and Past Work

This paper is a legal analysis of five key cases on global take downs from around the world, namely Swami Ramdev v. Facebook Inc. (India, Delhi High Court), Google v. CNIL (France, CJEU), Eva Glawischnig-Piesczek v. Facebook Ireland Ltd. (Austria, CJEU), Google Inc. v. Equustek Solutions Inc. (Canadian Supreme Court), and X v. Twitter Inc. (Australia, Supreme Court of New South Wales). These judgments are the leading case law on the subject of global take downs internationally and the most recent case among these, the Delhi High Court case in Swami Ramdev v. Facebook Inc. discusses and relies on the remaining judgments.

Global take down orders raise questions around free speech and privacy on the Internet and contribute to the changing dynamics of intermediary liability law on the Internet. SFLC.in has published comprehensive work on intermediary liability law which can be downloaded from, here – https://sflc.in/resources.

This paper is an extension of our existing work on intermediary liability law in India and its intersection with international developments. Our analysis in this paper has built upon robust learning from our previous work. We would like to thank all stakeholders who have helped us by attending our public discussions and agreeing to speak to us to supplement our knowledge on the subject of intermediary liability.

Introduction

Around the world, there is general consensus on certain categories of content that should be removed from the Internet, globally – child pornography, child exploitative imagery, and live streaming of terror attacks, are just a few examples. Countries around the world have laws for the expeditious removal of such content and Internet platforms have in-built mechanisms for its disablement. In accordance with different standards of domestic law, courts and governments frequently ask large Internet platforms to remove content from their services. Recently, courts in different countries like Canada, Australia, France, Austria, and India have been asking platforms to take down content globally, in application of their national laws.

The immediate threat of such global take down orders is that they negatively impact global online free speech, digital privacy (in situations where proactive monitoring is imposed on platforms), and the open nature of the world wide web. On a close assessment of some of the key judgments on global take downs from around the world, the subject matter issues range from defamation to stealing of trade secrets. Each case needs to be assessed separately to understand the contextual challenges arising out of the subject matters and the type of removal order imposed on social media platforms. Platforms have been asked by courts to de-list web links (Google), take down content (Facebook), and suspend user accounts (Twitter). Some courts have asked for a one-time content removal, whereas others have demanded proactive monitoring to take down future instances of publication. Each remedy has its own degree of risk posed to free speech and privacy and courts tend to learn from each other, regularly referencing and relying on past judgments.

In all cases, Internet platforms (Facebook, Twitter, and Google) have been considered by courts to be where proliferation of content takes place. Going beyond traditional intermediary liability law, where platforms are not required to interfere with content when it is uploaded, courts have recognized the clout which certain intermediaries exercise on the Internet and have asked them to play a larger role in taking down illegal content. This poses a challenge to existing intermediary liability law and further enhances the power certain intermediaries exercise over information access on the Internet.

Each case on global take downs exposes the courts' struggle in grappling with complicated issues of law and technology. The opaque methods of how Internet platforms operate their services, adds to this confusion and results in judgments which may not be enforceable due to the practical challenges with technology.

At each step, courts must be assisted by platforms, lawyers, civil society and domain experts to explain the complexities of technology and the intersection with law, so that they issue judgments which are not just based on established legal principle but are technologically sound and feasible.

What is a global take down order?

Internet intermediary[1] platforms like Facebook, Twitter, Google, and YouTube frequently take down content from their web services in adherence to their community standards and terms of use. In addition to these, courts and government agencies often ask Internet intermediaries to take down content in accordance with law.[2] Internet intermediaries are not obligated to take-off content from

1 For a definition of the word 'intermediary' according to Indian law, kindly refer to Sec. 2(1)(w) of the Information Technology Act, 2000.

2 For Indian law, see Sec. 79 of the Information Technology Act, 2000 and Shreya Singhal v. Union of India, AIR 2015 SC 1532

their platforms and are accorded a general safe-harbour protection for user-generated/ third party content on their services[3].

Traditionally, when ordered by courts, Internet platforms take down content from the relevant geographical region, in accordance with the territorial jurisdiction of the issuing court. But lately, courts from around the world have been ordering platforms to remove content from their 'global services' exercising long-arm jurisdiction, affecting the visibility of content throughout the world. For ex. courts in Austria have asked Facebook to take down content not just from its Austrian/ EU service, but from all service areas around the world. This has been possible due to the centralized structure of these Internet intermediary platforms and their ubiquitous presence around the world.

If uploaded from India, then take it down globally
Swami Ramdev v. Facebook (India, Delhi High Court)

Though it's not the first time an Indian court has asked an Internet intermediary to take down content globally[4], the judgment of the Delhi High Court in *Swami Ramdev v. Facebook*[5] is the first comprehensive assessment of the legality of global take down orders, where the court found its remit in Indian law.

The dispute in this matter arose from certain videos which contained summaries of a biography of Baba Ramdev[6] titled *'Godman to Tycoon – the Untold Story of Baba Ramdev'* written by journalist Priyanka Pathak-Narain[7]. This book, as part of separate litigation before the Delhi High Court[8], had been held to contain defamatory content on Baba Ramdev and was restrained from being published by the court. Claiming that the videos on social media platforms were defamatory in nature, the petitioners in this case, Baba Ramdev and Patanjali Ayurved Ltd., requested the court to pass a global take down order for the removal of such videos. The petitioners arraigned Facebook, Google, YouTube, Google Plus, Twitter, and Ashok Kumars (John Does – unidentified parties) to the case.

None of the platforms objected to removing the specified content from their India services, but they all contested removing the content from their global services.

The central question before the court was whether, according to prevailing content take down law in India, Internet intermediary platforms could be asked to take down content globally?

The court, after comprehensively discussing the international jurisprudence on global take downs and taking into account Indian content take down law, held in favour of the petitioners and stated that nothing in the Information Technology Act, 2000 ("the IT Act") bars courts from ordering global take down of content from Internet intermediary platforms. The court adopted a graded approach to content take down[9] – a) videos which had been uploaded from Indian IP addresses had

3 Id.
4 YouTube LLC v. Geeta Shroff (Delhi High Court, 2018), FAO 93/2018. In this matter, YouTube had withdrawn its appeal before the Delhi High Court challenging an order to take down content globally.
5 Swami Ramdev v. Facebook Inc., 263 (2019) DLT 689
6 Baba Ramdev is a popular Indian yoga guru and owner of the famous consumer goods company Patanjali Ayurved Ltd. - https://www.bloomberg.com/news/features/2018-03-15/this-multibillion-dollar-corporation-is-controlled-by-a-penniless-yoga-superstar.
7 Review: Godman to Tycoon by Priyanka Pathak-Narain – https://www.hindustantimes.com/books/review-godman-to-tycoon-by-priyanka-pathak-narain/story-AS0MTSOIa135y0R62eNbRJ.html.
8 Swami Ramdev v. Juggernaut Books (Delhi High Court, 2018), CM(M) 556/2018
9 Facebook, Google, and Twitter have filed appeals before a division bench of the Delhi High Court against the single judge order in Swami Ramdev v. Facebook – https://www.livelaw.in/news-updates/delhi-hc-db-admits-facebooks-appeal-against-global-blocking-order—149368 and http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=18408&yr=2020.

to be removed on a global basis; and b) videos which had been uploaded from outside India had to be made inaccessible (blocked) from Indian domains. Interestingly, the court established a new 'notice and take down' regime by allowing the petitioners to directly approach intermediary platforms for future take down of offending content. Though the court did allow intermediaries to object to such requests, this position is incongruent with established take down jurisprudence in India, wherein only courts and governments can ask platforms to take down content.[10] This also amplifies the problem of private determination of legality being delegated by courts to Internet platforms.

Free speech implications and the global network
Analysing the court's rationale

The upload destination argument

The main reasoning of the court to allow for a global take down was based on a literal reading of a few provisions of the IT Act. Sec. 79 of the IT Act obligates Internet intermediaries to expeditiously remove content from the 'computer resource' operated by them, when ordered by a court on government agency. The court interpreted the definition of 'computer resource' to mean a maze or a network of computers which is global in nature.[11] The court stated that, *"79. Thus, the removal and disablement is intricately connected to the information that is uploaded and the system upon which it is uploaded, where it resides."*[12] The court held that once content is uploaded from India and is made available globally, Indian courts have jurisdiction to have it removed on a global basis.

The Internet is an intricate, globally connected network, which has managed to diminish physical boundaries and enabled us to communicate on a real time basis across the world. If we were to reverse the court's logic that since content uploaded from India is immediately available globally, thus removal of such content must be global, then only content which is uploaded from India and is accessible on the Indian Internet would naturally and legally be immune from global take downs. If Internet platforms are encouraged by courts to provide access to information only domestically, then it'll lead to the balkanisation of the Internet, hampering the promise of a free and open world wide web.

Varying standards of free speech

Unfortunately, one glaring gap in the reasoning of the court to arrive at the global take down order, was the lack of analysis of its effect on free speech on the Internet. As was argued by the platforms in this case, the standards of law on free speech varies drastically across nations. Though, the book on Baba Ramdev which was the subject matter of litigation in this matter was considered to be defamatory, the same content might be perfectly legal in other regimes like the US or Germany. Cutting access to perfectly legal content across jurisdictions hampers the protection of free speech on the Internet across the world. If global take downs become the norm around the world, then the Internet will reflect free speech standards of the most regressive country.

10 See supra note 2
11 Kindly refer to Sec. 2(1)(j), (k), and (l) of the Information Technology Act, 2000.
12 Para 79 of the *Swami Ramdev* judgment

Virtual Private Networks (VPNs)

Put in simple terms, a VPN helps Internet users mask certain details of their web activity like IP address and geo-location, which would be otherwise visible to third parties, and helps maintain a certain level of anonymity over the Internet.[13] A VPN may be used by Internet users to mask their IP address and route Internet traffic through a country which is different from their physical location.

The court while granting an order for a global take down stated that such injunctions must be effective and since by using VPN services the offending material could be still accessed, geo-blocking would not be a sufficient remedy. *"92… If geo-blocking alone is permitted in respect of the entire content, there cannot be any dispute that the offending information would still reside in the global platforms of the Defendants, and would be accessible from India, not only through VPN and other mechanisms, but also by accessing the international websites of these platforms. It is not unknown that the Canadian, European and American websites of Google, Facebook, YouTube and Twitter can be accessed in India through various technological means. This would thus result in partial disabling and partial removal."*[14]

The challenge with understanding the flow of data on the Internet from a geographical standpoint is that the location of upload/ download of such data can be easily masked using readily, available technology like VPN services or Tor (Onion Service Protocol)[15]. An Internet users physical location may be distinct from her apparent geo-location on the Internet. Considering the court's judgment in *Swami Ramdev* strongly links the 'upload destination' principle with when the material gets available on Internet platforms, this argument may be erroneous as it's easy to manipulate the upload destination on the Internet.

For illustration purposes – If X wanted to upload the defamatory content (in this case) onto YouTube sitting in India, after the court order (i.e. once the platforms had removed the content from their websites), they could mask their IP address using a VPN service to a country that was not India, say the United States. Once the content had been uploaded onto YouTube from another country, it could then only be blocked for access within India (as per the court's order). Subsequently, when the content gets blocked from access in India, X or any other user from India, could use a similar VPN service, mask its IP and continue to view the content on YouTube.[16]

Another argument to consider, specially in the context of the Indian region is that the percentage of Internet users in India who might be aware or sophisticated enough to use VPN/ Tor services may be negligible.[17] The court did not assess how geo-blocking would be insufficient taking into account the prevailing digital literacy rate in India. Ordering a global take down of content due to the mere possibility of accessing the it using VPN services may be a disproportionate response, as in most cases geo-blocking would be sufficient considering the low awareness levels of technologies like VPN and Tor services in India.

Another anomaly in the court's reasoning is allowing geo-blocking of content uploaded from foreign shores with respect to India. If geo-blocking was considered insufficient for content uploaded from India (due to access to VPN services) then for the same reason, it should have been considered insufficient for content uploaded from foreign shores as well.

13 What is a VPN? - https://www.cloudflare.com/learning/vpn/what-is-a-vpn/.
14 Para 92 of the judgment in *Swami Ramdev* (supra note 5)
15 Tor: Onion Service Protocol – https://2019.www.torproject.org/docs/onion-services.html.en.
16 An Analysis of Swami Ramdev v. Facebook – The Existential Risk of Global Take Down Orders – https://sflc.in/detailed-analysis-swami-ramdev-v-facebook-judgment.
17 Digital Literacy Mission, Digital Empowerment Foundation – https://defindia.org/national-digital-literacy-mission/.

Constant monitoring and risk of future uploads

One of the positive features of *Swami Ramdev* is that the court correctly enunciated that online intermediaries cannot apply their own mind as to which information should be blocked or not[18]. This is the established legal principle of online content take down in India as pronounced in *Shreya Singhal v. Union of India*[19]. The Delhi High Court in prior judgments of *MySpace*[20] and *Kent RO*[21] has clearly stated that monitoring requirements and private determination of legality of content will lead to a chilling effect on speech and unwarranted private censorship. The court has held that intermediaries do not have the prowess to determine complex questions of law on content take downs. Thus the requirement of constant monitoring and private determination of the legality of content has been squarely rejected by the Delhi High Court in its jurisprudence. In terms of enforcement of intellectual property rights, the Delhi High Court has allowed rights holders to directly approach intermediary platforms for take down of illegal content by specially pointing to it.[22] Though, that was a diversion from *Shreya Singhal*, in which the court clarified that take down could only be ordered by courts or governments, *Swami Ramdev* brings a similar relief in law to determination of the legality of online speech.

In *Swami Ramdev*, the court has allowed Baba Ramdev and Patanjali (petitioners) to directly approach Internet platforms in cases of future uploads of the defamatory content, to have such content removed. Though, the court has allowed platforms to object to such take down requests, this type of a notice and take down request where private parties determine the legality of speech goes against established standards of take down law and the court's own understanding that intermediaries could not apply their own mind in determining which content must be blocked or not.

Private determination of legality of speech will not only lead to the risk of over censorship on Internet platforms, but also lead to dilution of safe-harbour protection, as intermediaries will be obligated to monitor content on their platforms more closely as per law. With intermediaries already taking down content of their own volition, such additional legal mandate to take down content will impact free speech on the Internet. The real risk of judgments like *Swami Ramdev*, lies in future courts being empowered to pass global take down orders and requiring private entities to determine the legality of speech, without judicial determination.

Reputation harm, trade secrets, and privacy
The international reality of global take downs

Courts around the world have granted global take downs for a variety of reasons – protection of reputation/ defamation (EU – appeals from France and Austria), protection of trade secrets and other intellectual property rights (Canada), and protection of personal financial data (Australia). These judgments are not only different in their subject matters but also in the mode of their take down orders, ranging from de-referencing on a search engine to complete take downs, including blocking of user accounts. The only instance out of these cases where the court refused to grant a global take down order came from France in a battle between Google and CNIL – the French Data Protection Authority, wherein Google refused to de-reference certain links from its global service and the CJEU sided with Google.

18 This is to be assessed as a position required under law. Intermediaries can and do regularly take content down of their own accord from their services in adherence to their own community guidelines.
19 Supra Note 2
20 MySpace v. Super Cassettes Industries, 236 (2017) DLT 478
21 Kent RO Systems Ltd. v. Amit Kotak, 240 (2017) DLT 3
22 Id.

Finding balance between the RTBF and the right to information
Google v. CNIL (France, CJEU)

In *Google v. CNIL*[23] the CNIL had ordered Google to de-reference/ de-index web links from its service which related to a natural person under the right to be forgotten. Google had refused to remove the relevant links from its global service and had approached the CJEU through formal channels of appeal to decide on the matter. Google had implemented the de-referencing applying geo-blocking, wherein irrespective of which national service an Internet user accesses, Google would show that version of its search engine which corresponded to the location of the Internet user.

The CJEU in *Google v. CNIL* gave a fairly reasoned order, wherein it held that there was no obligation under EU law for search engines to conduct de-referencing of links on their global services on a request received from an EU Member State, under the right to be forgotten. The court, while upholding the principle of proportionality, held that the right to protection of personal data wasn't an absolute right and needed to be balanced with other fundamental rights such as the right to freedom of information. The court recognized the varying legal standards of the right to be forgotten around the world, to conclude that it would not be fit to impose the EU model all across the world, *"59. That being said, it should be emphasised that numerous third States do not recognise the right to de-referencing or have a different approach to that right."*[24]

Despite holding that search engines aren't obligated under EU law to de-reference web links from their global services under a right to be forgotten request, the CJEU did clarify that where appropriate, and after balancing the right to protection of personal data and the right to information, national supervisory and judicial authorities of EU Member States do have the power to order search engines to de-reference web links globally.

The *CNIL* judgment of the CJEU is a well reasoned order which upholds the right to proportionality and acknowledges the varying standards of legal principles around the world, which might get affected due to a global take down order. As a comparison with India's *Swami Ramdev* judgment, Google in this matter submitted that as per its geo-blocking mechanism, users will get directed to national versions of its search engine, depending on where they are accessing the Internet from, irrespective of which version of its website they actually access. For ex. an Internet user in France will get directed to Google's French service even if she manually enters google.co.in in the address bar of her browser. This nuanced understanding of geo-blocking wasn't undertaken by the Delhi High Court in *Swami Ramdev* (the court discussed the *Google v. CNIL* matter, but did not rely on the principles expounded therein), as one of the reasons for the court to grant a global injunction was that users could easily access global versions of social media platform subverting the geo-blocking exercise.

Just over a week after the CJEU delivered its judgment in *Google v. CNIL*, in another matter the court not just granted a global take down order, but also approved the selective monitoring of equivalent content, to ensure that the illegal content does not show up again on social media.

Specific monitoring and global take down
Eva Glawischnig-Piesczek v. Facebook (Austria, CJEU)

In a matter between an Austrian politician Ms. Eva Glawischnig-Piesczek and Facebook (*Eva Glawischnig-Piesczek v. Facebook Ireland Limited*[25]) the subject of contention was a Facebook post

23 Google v. CNIL C-507/17 CJEU (2019)
24 Id. at para. 59
25 Eva Glawischnig-Piesczek v. Facebook Ireland Limited C-18/18 CJEU (2019)

which showed a photo of Ms. Glawischnig-Piesczek along with a summary of an article which called her a "lousy traitor, corrupt oaf, and member of a fascist party." The politician asked Facebook to take down the post which it refused to act upon. Subsequently, Ms. Glawischnig-Piesczek got an order from a lower court in Austria which not only asked Facebook to remove the specific post, but ordered it to remove any 'equivalent content' from its platform. The matter eventually reached the Autrian Supreme Court which referred it to the CJEU for determination of certain key questions.

While interpreting the EU e-commerce directive ("the ECD"), the CJEU stated that it does not bar courts from issuing global take down orders within the framework of international law. The court also held that identification and removal of identical information, once found to be illegal by courts of Member States, cannot be termed as a general obligation to monitor (which was barred as per Article 15 of the ECD). On the question of take down of equivalent information, the court held that conducting specific monitoring of equivalent information wasn't outside the scope of law. Equivalent information was such content which was essentially the same but only diverged a little – to the extent that platforms were not obligated to conduct an independent assessment of the content while taking it down. The court reasoned that to provide an effective remedy, content which essentially conveyed the same matter, but with minor deviations would also be required to be taken down.

Eva Glawischnig has similar trappings of the Delhi High Court judgment in *Swami Ramdev*, but goes a step ahead by mandating the take down of identical and equivalent content. Unfortunately, the court does not assess the impact of its judgment on the freedom of speech on the Internet and how its order would contradict different standards of speech around the world. For ex. the speech held to be defamatory in this case would be perfectly legal in the US as per the first amendment right. As opposed to *CNIL*, the CJEU did not even consider how its order was proportionate and why geo-blocking would not be a sufficient remedy in this instance. By ordering for monitoring and taking down of identical and equivalent content from Facebook globally, the court has created risks of over-censorship and privacy. It is well known that filtering technology used by social media platforms is inefficient and regularly throws up false positives affecting free speech rights of Internet users.[26] The CJEU in *Eva Glawischnig* failed to take into account its own judgment in *CNIL* and also indirectly helped guide the Delhi High Court in *Swami Ramdev* in arriving at its global take down order (in *Swami Ramdev*, the Delhi High Court did not order for monitoring and removing of either identical or equivalent content, but relied on *Eva Glawischnig*).

Trade secrets and global de-listing
Google v. Equustek (Canadian Supreme Court)

Google Inc. v. Equustek Solutions Inc.[27] (Canada) is the first judgment from the highest court of any country imposing and affirming a global take town order[28] (the EU cases, though adjudicated upon by the CJEU, haven't been decided finally by the courts of their respective countries). Due to its finality, the case is one of the most important judgments on the subject of global take downs.

The dispute in *Equustek* arose between two private parties excluding Google. Two network infrastructure companies in Canada – Equustek and Datalink were manufacturing and selling competing products. Equustek accused Datalink of stealing its trade secrets to offer competing products, stating that though Datalink advertised the sale of Equustek's products, it actually sold its

26 The Future of Intermediary Liability in India (SFLC.in, 2020) – https://sflc.in/future-intermediary-liability-india.
27 Google Inc. v. Equustek Solutions Inc., [2017] 1 S.C.R. 824, 825 (Canada).
28 Speech Across Borders, Jennifer Daskal, Virginia Law Review Association (2019) – http://www.virginialawreview.org/sites/virginialawreview.org/files/Daskal_Book.pdf.

own products in disguise. When Equustek went to court, the court first ordered Datalink to return Equustek's source code, stop referring to Equustek on its own its website, and to direct customers to Equustek's website rather than selling them their own competing products. When Datalink did not comply with such an order, the court subsequently barred Datalink from selling its own products online. In response, Datalink exited Canada and continued to conduct its business from overseas.

Subsequently, Equustek sought the help of Google to de-list certain web pages run by Datalink from its search engine. Google did not de-list all web pages and applied such de-indexing only on its Canadian service – google.ca. All courts, including Canada's Supreme Court asked Google to suspend/ de-list the web pages from its global service and not just the Canadian service as that would be the only appropriate and effective remedy to Equustek.

The Canadian Supreme Court reasoned that as the Internet had no borders, the only effective remedy would be to ask Google to remove the web pages from where it operates i.e. globally. The court stated that it was not asking Google to conduct any monitoring and only de-list specific web pages which it regularly did for other subject matters such as child pornography, hate speech, and copyright matters. The illegal sale of goods could not be covered by free speech protection and there was no evidence that by taking down the links from its search engine Google would be violating the laws of another country, the court stated.

Aggrieved by the Canadian Supreme Court, Google approached the district court in California[29], which ruled in its favour giving an injunction for the Canadian judgment not be enforceable in the US. The California court stated that Google was protected by Section 230 of the Communications Decency Act ("CDA 230") in the US and that the Canadian judgment undermines the policy goals of CDA 230 and threatens free speech on the Internet. Subsequently, the trial court in Canada[30] refused to modify its judgment in reason with the California court, stating that Google did not establish how there was a conflict of law by de-indexing web links and it wasn't established that Google's first amendment rights were violated by doing such act. Another key argument which Google made was the improvement in its geo-blocking technology (as made before the CJEU in *CNIL*), stating that users could only access national versions of its search engine depending on their physical location and could not access foreign versions of its search engine by simply selecting a different region. This argument was rejected by the court too, as most of Datalink's sales originated outside of Canada.

Unlike disputes around defamation and harm to reputation, the *Equustek* judgment was a matter of trade secrets and illegal sale of goods. The court argued that for an effective remedy to Equustek, Google must de-list the relevant web links/ pages from its global service. Even if it's assumed that this was a reasonable requirement, this would just make Datalink's web pages inaccessible from Google's search engine. Patrons of their products could still access their websites by using the specific URLs or making use of other search engines like Bing or DuckDuckGo. Datalink could use social media channels such as those of Facebook or Twitter to promote its web pages and reach out to prospective customers. The Supreme Court of Canada failed to establish as to how de-listing the web pages from Google was a proportionate response, while all the other options would be available to Datalink's prospective customers to buy its products. By targeting once Internet platform and ordering it to remove links globally, the court has failed to understand the dynamic and multi-faceted nature of the Internet. It is true that Google's search dominates web searches on the Internet, but in protecting the commercial rights of a company, the court did not take into account the numerous other possibilities for Datalink to continue selling the illegal products.

29 Google LLC v. Equustek Solutions Inc. (2017), 5:17-cv-04207-EJD, Unites States District Court, Northern District of California, San Jose Division.

30 Equustek Solutions Inc. v. Jack, 2018 BCSC 610 (Supreme Court of British Columbia)

Banning of user accounts permanently
X v. Twitter (Australia, Supreme Court of New South Wales)

X v. Twitter Inc.[31] is one of the most far reaching global take down judgments internationally. In this case the Supreme Court of New South Wales (Australia) not just ordered for a global take down of the content in question, but upheld a mandate of proactive monitoring alongside permanent disablement of user accounts in addition to banning future attempts at user registration.

This case concerned the leakage of confidential financial information of an anonymous individual by an unidentified user on Twitter. Once the anonymous person – X alerted Twitter of leak of sensitive data and act of impersonation, Twitter removed the offending accounts of such users. But, subsequently, when more accounts propped up on Twitter sharing the content in question, Twitter failed to take the content/ accounts down citing its internal policies.

X took Twitter to court and demanded – the removal and prevention of publication of the content globally, removal of accounts which were disseminating the content, and preventing account holders from opening alternative accounts or posting further tweets irrespective of the content of such tweets. The Supreme Court of New South Wales ruled in favour of the plaintiff. It approved the global take down of content, concluded that proactive monitoring and take downs were possible to be acted upon by Twitter, and the court held it fair to keep users off Twitter once they had identified their credentials.

X v. Twitter does not only concern itself with global take downs, but forces Twitter to proactively monitor its platform for offending content and blocking accounts which are sharing the offending content. The most far reaching aspect of the case is prevention of identified account holders from opening alternative accounts and blocking them from tweeting irrespective of the content. This judgment has substantial implications for online free speech and privacy. Permanently blocking users from a social media platform is a disproportionate remedy and violates the fundamental rights of those users. There are questions about implementation of this order, as users who might be banned due to their identity, could easily fake their credentials, use alternate e-mail IDs to register with Twitter and create accounts.

Conclusion

On a close assessment of some of the key cases on global take down of content from around the world, one key observation is that, courts haven't demonstrated how in each instance, it was a proportionate remedy to grant a global blocking order on speech (the CJEU in *CNIL* emphasised on the importance of the proportionality principle and did take into account the varying standards of free speech law around the world). Not all cases relate to the same subject matter, questions of intellectual property might not fall squarely under free speech issues, but due to the precedential value of these judgments, a proper assessment of how orders would affect global free speech on the Internet would be essential to protect rights. If global take downs become the norm, then speech on the Internet will be regulated by the laws of countries with the most regressive approach to free expression. The *CNIL* judgment illustrates this argument well, *"60. Moreover, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality …"*[32]

31 X v. Twitter Inc. [2017] NSWSC 1300
32 Supra note 21

Similarly, another glaring gap in these matters is the lack of discussion on privacy implications of proactive monitoring on Internet platforms (where ordered), whether for identical/ equivalent content (CJEU in *Eva Glawischnig*) or content and user accounts (*X v. Twitter*). Proactive tools also run the risk of pre-censorship (censorship before publication) and over-censorship, which leads to a chilling effect on speech on the Internet. Monitoring tools are prone to errors, throwing up false-positives and run the risk of cutting out voices of marginalized and minority communities[33].

Methods adopted by Internet platforms as solutions to content take down challenges are often opaque and hence there's a distrust among courts while relying on them. In *Swami Ramdev*, the court commented that platforms hadn't technically explained what geo-blocking would entail, *"46. … Further, the Court had specifically directed the Defendants to throw some light on how geo blocking is done and to keep a technical person present in Court to seek clarification on geo blocking. None of the platforms have given a detailed explanation as to how geo-blocking is done."*[34] Even in *Equustek*, when Google tried to explain its geo-blocking technology to the Supreme Court of British Columbia[35], the court rejected its argument by stating that most of Datalink's sales originate from outside Canada anyway. Similarly, from an assessment of all these cases, it is unclear if courts understood the way data moves on the Internet and the complications thrown by technologies like VPN services and Tor. In *X v. Twitter*[36], the court asked Twitter to permanently ban certain users once they disclose their credentials, the technological feasibility of such a requirement was not taken into account by the court while arriving this reasoning. To safeguard Internet rights, it becomes imperative on technology and law experts and civil society organizations to assist courts in their understanding of unique challenges thrown by modern technology.

Global take downs, specially the ones asking for proactive monitoring, dilute safe-harbour protection afforded to Internet intermediaries. One of the key conditions under law for attaining safe-harbour protection, is the non-interference in the uploading of content by intermediary platforms (the law in India and EU also bars intermediaries from performing a constant monitoring function). By requiring platforms to monitor and take down, either identical or similar content, courts are diluting the safe-harbour protection which social media platforms enjoy on the Internet. The safe-harbour protection is an essential safeguard to ensure that Internet platforms remain the vibrant spaces they have come to be. If platforms are increasingly held liable for content flowing through their pipelines they will over-censor content to protect themselves from potential legal liability[37].

Another challenge with existing global take down orders is that they look at the Internet from the prism of social media platforms or/ and Google. It is true that large volumes of Internet traffic flows through the pipes of Facebook, Twitter, and Google, but content can exist on the Internet beyond the walls of these centralized platforms. Taking the example of the *Swami Ramdev* case, the defamatory videos which were the subject of the dispute in that matter, could be uploaded on other services such as – Vimeo or independent blogs/ websites maintained by individuals. Similarly, in *Eva Glawischnig*, though the court held that under EU law Facebook could be asked to remove content globally, the content in question could pop-up on other social media platforms like Twitter or Instagram. Global take downs acquire a new degree of menace due to the centralized systems of popular social media and web search channels.

33 Supra note 24
34 Supra note 5
35 Supra note 28
36 Supra note 29
37 See, SFLC.in's reports on the subject of Intermediary Liability – https://sflc.in/future-intermediary-liability-india, https://sflc.in/intermediary-liability-20-shifting-paradigm, and https://sflc.in/information-technology-intermediaries-guidelines-rules-2011-an-analysis-2

If Facebook, Twitter, or Google were not centralized services having absolute control on all versions and servers around the world, it would not be fruitful for courts to demand global take downs from these intermediary platforms. In *Swami Ramdev, Equustek, and X v. Twitter,* the court emphasised on the argument that platforms regularly took down speech from their global services in adherence to their internal policies, thus it would be possible for them to apply such take downs to the subject matter content as well. The Delhi High Court pointed to this in *Swami Ramdev, "94. … When disabling is done by the Platforms on their own, in terms of their policies, the same is global. So, there is no reason as to why court orders ought not to be global. …"*[38] Global take downs end up enhancing the power of centralized platforms by asking them to play an active role in what stays up/ gets removed from their services. Global take downs of the nature ordered on Facebook, Google, and Twitter would not be possible on a decentralized social media platform like Mastodon. Private determination of speech on large public forums affects free speech on the Internet and has been specially held to be non-permissible by the Indian Supreme Court in *Shreya Singhal*[39].

By far the biggest impediment posed by global take down orders is the precedential value and authority of these judgments, specially when delivered by the apex courts of these nations/ jurisdictions. (*Equustek* by the Supreme Court of Canada and *CNIL* and *Eva Glawischnig* by the CJEU, though the final judgments in the European matters has not been delivered by their national courts). Once, approved by higher judicial authorities, lower courts would not shy from issuing such orders. Since in some of these judgments the threat to online free speech and privacy was not comprehensively discussed and standards of proportionality were not established, it might open the flood gates for lower authorities to grant such global injunctions. It is essential that all stakeholders – civil society, academia, technology experts, legal professionals, come together in assisting courts when such matters are filed before them. The promise of the free and open Internet and the benefits of a boundary-less network will get severely diluted if global take down orders become the new standard.

38 Supra note 5
39 Supra note 2