OTF
(https://www.opentech.fund)

THE DECENTRALISED INFRASTRUCTURE OF ONLINE CENSORSHIP IN ASIA

Mon, 2023-05-08 15:56

The following blog post was written by ICFP fellow Gurshabad Grover as a summary of their work and research on online censorship in Asia.

Governments across the world engage in various forms of internet censorship – from internet shutdowns, geo-blocking of social media posts or accounts, and blocking of specific websites and apps. When it comes to the latter, information controls can be 'centralised' – best represented by the archetype of a "great firewall (https://www.opentech.fund/news/how-chinese-internet-users-are-climbing-a-bigger-badder-great-firewall-daily-dot/)" that is largely state-controlled and managed. On the other hand, many governments rely on private companies such as internet service providers (ISPs) and internet exchanges to implement censorship and surveillance orders.

In this blogpost, we discuss a spectrum of such 'decentralised (https://par.nsf.gov/servlets/purl/10142204)' information controls. We explore the legal background and technical architecture of information controls of three countries in Asia: India, Pakistan and Indonesia. The research includes first, an analysis of network measurements contributed by users, which helps us determine what websites are blocked, and what methods ISPs are using to block those websites. Second, we study the legal background and the powers of state authorities and the delegation of powers, if any, to private actors and other stakeholders. The analysis focuses on the network infrastructure, the state and private actors that control the infrastructure for censorship and surveillance, and the role of private players in exacerbating the adverse effects of censorship.

India

The Indian Government draws its powers of online censorship from the Information Technology (IT) Act, 2000. The Government sends orders to internet service providers (ISPs), which in turn are responsible for implementing the blocking of web endpoints. While most censorship is state-ordered, private actors (primarily ISPs in India's case) control the infrastructure for censorship and surveillance.

In India, this model has meant that ISPs are free to choose the technical methods of blocking. Our analysis (https://www.petsymposium.org/foci/2023/foci-2023-0006.pdf) of 9 million measurements contributed by 331 users from 25 states in India reveals that this implementation of censorship varies wildly across ISPs. The research revealed that different ISPs use different methods of blocking. This directly influences the right to freedom of expression in India, as the choice of technical methods dictates how easy or difficult circumventing such censorship is.

Most ISPs still use the method of monitoring and filtering of HTTP requests. The more sophisticated method of blocking based on the Server Name Indication (SNI) present in HTTPS connections is only used by 16 networks. Much of this style of blocking is conducted by two large pan-India ISPs – Bharti Airtel and Reliance Jio. SNI-based blocking is difficult to evade for lay people without the use of circumvention tools or VPNs. Additionally, we found that many ISPs in India are using methods that do not allow for the presentation of censorship notices, thus making it difficult for them to distinguish between network failures and censorship, and impeding legal challenges to state action.

ISPs in India also often end up blocking different websites – possibly due to expansive or incorrect interpretations of legal orders. For instance, we found that some ISPs were still blocking websites for longer durations than orders required them to, or were blocking websites that had been later ordered to be unblocked by the government. In this way, ISPs not only engage in blocking resources that should be legally accessible, but also violate net neutrality regulations.

Another important aspect of online censorship are the procedural rights enshrined in law. In India, the law empowers a committee of government employees to send orders to ISPs. The law allows the executive to engage in censorship unilaterally – without any immediate parliamentary or judicial oversight, and the mandated confidentiality of such orders enables an opaque regime of censorship (https://scroll.in/article/953146/how-india-is-using-its-information-technology-act-to-arbitrarily-take-down-online-content).

The only safeguard in the regulations is the requirement imposed on the government to contact affected content creators and website owners before any action is taken. However, our interviews (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4404965) with affected content creators and website owners – ranging from news publications to activists – empirically establish that the Government rarely implements this safeguard in practice. While many of the affected individuals and organisations we interviewed were well-known and their contact information easily available, most of them were not informed by the Government before or after their content was ordered to be blocked in India.

The courts have also rarely stepped in as a correcting force even though the law suffers from constitutional infirmities, with the judiciary having never overturned any online censorship enacted by the Government of India.

Amendments to the existing law or the introduction of new ones would ideally pave the way to remove the possibility of rights violations, but proposed legislation unfortunately retains the rights-infringing character of the present legal regime. For instance, in September 2022, the Department of Telecommunications released a draft Telecommunication Bill to replace colonial-era legislation that still regulates telecommunication in India. Amongst many other things, the new Bill will mandate a licensing regime (https://gurshabad.github.io/writing/Anunay_Kulshrestha-Gurshabad_Grover-Comments_Telecommunication_Bill_2022.pdf) for all online communication services, and sanction state surveillance without accountability (https://www.lawfareblog.com/indian-telecommunication-bill-engenders-security-and-privacy-risks).

Pakistan

The legal framework for online censorship in Pakistan is quite similar to India's current regime, in that a state authority – the Pakistan Telecommunications Authority (PTA) – is empowered to block resources for the public and direct ISPs in the jurisdiction to do so.

However, our comparative review (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4404965) of the legal framework and jurisprudence reveals more robust procedural safeguards for citizens and an involved judiciary. For instance, the Prevention of Electronic Crimes Act (PECA) explicitly allows content creators, website owners and any person aggrieved with censorship orders to file an appeal against the PTA.

Even though there is no ex-ante procedural safeguard in the law, the Islamabad High Court has admonished the PTA and directed it to offer a pre-decisional hearing to any citizen of Pakistan whose online content would be affected by censorship orders. Since the law grants unilateral power to the PTA and does not mandate judicial or parliamentary scrutiny of the censorship orders, the concerns of arbitrary censorship by the executive (https://bolobhi.org/wp-content/uploads/2020/07/Pakistan%E2%80%99s-Online-Censorship-Regime.pdf) remain despite these progressive judicial pronouncements.

Historically, the technical infrastructure of censorship in Pakistan was 'decentralised' as well, but is undergoing changes in recent years. While there is some diversity of market players, the PTA seems to be exploiting the fact that a significant portion of internet subscribers in Pakistan are served by entities controlled directly or indirectly by state enterprises (https://www.pta.gov.pk/assets/media/annual_report_2020_15012021.zip). Most lines of international connectivity (https://bolobhi.org/state-of-it-governance-in-pakistan-a-report-by-bolo-bhi/) are also under the direct control of state agencies.

This network topology means that the PTA is easily advancing on more centralised control over infrastructure. The PTA has acknowledged (https://www.codastory.com/authoritarian-tech/pakistan-web-monitoring-surveillance/) the successful implementation of the Web Monitoring System (https://www.pta.gov.pk/assets/media/tender_150218.pdf) (WMS), deployed at internet traffic exchanges and lines of international connectivity. The system is capable of monitoring and filtering internet traffic going upstream from most ISPs in Pakistan.

In 2022, it was also reported (https://www.dawn.com/news/1693213/pta-at-odds-with-isps-over-domain-policy) that the PTA wants all ISPs in the country to direct all DNS requests from internet users in the country to specified servers. However, this has not been implemented (https://tribune.com.pk/story/2362666/pta-dismisses-reports-of-implementing-centralised-dns-control) yet, possibly due to pushback from ISPs.

Thus, we see a concerted move towards centralised and mostly state-controlled infrastructure for online censorship in Pakistan.

Indonesia

Indonesia has also followed the decentralised model of information controls, with state authorities having the power to send legal orders to ISPs to block access to online resources. There are both private and public internet service providers (https://freedomhouse.org/country/indonesia/freedom-net/2021) in Indonesia, among which there is diverse interconnection and international connectivity (https://citizenlab.ca/2013/10/igf-2013-an-overview-of-indonesian-internet-infrastructure-and-governance/).

The Indonesian Government has issued technical guidance (https://www.lexology.com/library/detail.aspx?g=99fc618d-232e-4590-b4cd-e456496e5ce9) to ISPs in the form of regulations (https://www.lexology.com/library/detail.aspx?g=99fc618d-232e-4590-b4cd-e456496e5ce9). Indonesia is also different from India and Pakistan in the aspect that there is some transparency in what is blocked, with the TRUST+ Positif (https://trustpositif.kominfo.go.id/) list (which ISPs were mandated to follow as per regulations issued in 2014) being publicly available. This fact theoretically means greater coordination among ISPs, and one would not expect different websites to be blocked on different ISPs.

However, the 2014 regulations (later amended in 2020) did allow Indonesian ISPs to block websites on their own discretion, causing inconsistencies in what is blocked across ISPs (https://ooni.org/post/indonesia-internet-censorship/). This delegation of powers to ISPs means that they hold significant influence over what their customers are able to access and not. Popular services like Vimeo and Reddit have been found to be blocked only by a chunk of Indonesian ISPs, while they remain accessible to others.

There has historically not been any centralised infrastructure used by the Government for implementing information controls. This scenario may also be changing with some desire for centralised control. For instance, in 2022, a proposal (https://www.idnog.or.id/en/download.html?f=MjAyMjA3MjkwMjE1NDAucGRm&id=MTQ=) appeared in a Indonesia Network Operators' Group (IGNOG) and Indonesia Internet Service Provider Association (APJII) presentation to centralise DNS queries. In such a model, all DNS queries would be forwarded to the DNS servers in internet exchanges – that would ostensibly be directly overseen by state authorities or by the APJII. Our work did not present any evidence that this DNS forwarding has been implemented yet, but the internet censorship research community continues to document how the methods of blocking across ISPs are changing.

Conclusion

These case studies reveal that information controls in a single jurisdiction can exist at multiple levels – public and private ISPs, internet exchange points, lines of international connectivity or other network chokepoints controlled by the state. A comprehensive understanding of information controls in a country requires us to investigate – among its many aspects – the law and its technical implementation by state and private actors.

The case studies reveal in jurisdictions with decentralised controls, ISPs – by choosing opaque methods of blocking or by hiding the reasons of why a website is inaccessible – can exacerbate the effects of state-ordered censorship. Decentralised information controls may not always result in better outcomes for internet freedom in comparison to centralised information controls. As we see in Indonesia, ISPs may be given the discretion to block websites on their own, resulting in arbitrary blocking beyond what the government explicitly requires to be blocked. The findings and implications of the research across India, Pakistan and Indonesia are summarised in an essay I authored, which will appear later this year in a volume on the politics of Internet infrastructure by Meatspace Press.

Much of the technical evidence of online censorship is only possible because of network measurements, such as those collected and analysed by the Open Observatory of Network Interference (OONI). Our analysis of the network measurements (https://ooni.org/post/improving-data-quality-analysis-of-failed-measurements/) in OONI revealed that many instances of censorship from India, Pakistan and Indonesia were mis-classified as errors. We will continue to improve the quality of data to help researchers, journalists and civil society expose and fight against internet censorship.

The evidence of online censorship from countries decentralised information controls uncovers the critical role that private players such as ISPs play in how the rights to access information and freedom of expression are exercised online. We developed a questionnaire and assessment framework for ISPs (https://github.com/gurshabad/gurshabad.github.io/blob/master/writing/isp-assessment.md) that civil society organisations worldwide can use to push these private players to incorporate respect of human rights in their policies and processes. With the amount of leeway ISPs have in implementing state orders, they can also minimise the effects of state censorship by reading legal orders narrowly and/or by choosing technical methods that make censorship apparent to internet users.

At the same time, it is important to strengthen the security properties of network protocols, so that they are more resistant to censorship from governments and private actors. Our ongoing efforts include pushing for considerations for human rights when designing internet protocols (https://datatracker.ietf.org/doc/draft-irtf-hrpc-guidelines/),

Acknowledgements

The words ‘we’ and ‘our’ in this blogpost are used for readability, and because the work took the form of collaborations with many amazing researchers. The Open Tech Fund supported my contributions to these collaborations. I am grateful to Simone Basso and Divyank Katira for reviewing this blogpost. All opinions and mistakes in this blogpost remain mine.

I co-authored the paper on the technical implementation of online censorship (https://www.petsymposium.org/foci/2023/foci-2023-0006.pdf) in India with Divyank Katira, Kushagra Singh and Varun Bansal. The paper on due process rights in online censorship (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4404965) was co-authored with Divyansha Sehgal. Anunay Kulshrestha and I co-authored the analysis (https://www.lawfareblog.com/indian-telecommunication-bill-engenders-security-and-privacy-risks) of the draft Indian Telecommunication Bill (https://gurshabad.github.io/writing/Anunay_Kulshrestha-Gurshabad_Grover-Comments_Telecommunication_Bill_2022.pdf). The questionnaire and assessment framework for ISPs (https://github.com/gurshabad/gurshabad.github.io/blob/master/writing/isp-assessment.md) was developed in collaboration with Divyank Katira.

I am co-authoring Guidelines for Human Rights Protocol and Architecture Considerations (https://datatracker.ietf.org/doc/html/draft-irtf-hrpc-guidelines) with Niels ten Oever at the Human Rights Protocol Considerations research group in the Internet Research Task Force.

Lastly, I am very grateful to the staff and community of the organisation hosting my fellowship, the Open Observatory of Network Interference (http://ooni.org/) (OONI), and particularly to Simone Basso for his unwavering support and for co-investigating the data quality of OONI measurements (https://ooni.org/post/improving-data-quality-analysis-of-failed-measurements/) from India, Pakistan and Indonesia.