<section-header>

Association for Progressive Communications (APC)



Special EDIFOR



Global Information Society Watch 2017 | Special edition Unshackling Expression: A study on laws criminalising expression online in Asia

Coordinating committee Gayatri Khandhadai (APC) Pavitra Ramanujam (APC) Geetha Hariharan

Project coordinator Gayatri Khandhadai (APC)

Edition coordinator Geetha Hariharan

Assistant editor, publication production Lori Nordstrom (APC)

Graphic design

Monocromo info@monocromo.com.uy Phone: +598 2400 1685

Cover illustration Ivana Kurniawati

Supported by the European Union under the Instrument for Democracy and Human Rights (EIDHR) and the Internet Policy Observatory (IPO)



Published by APC 2017

Printed in India

Creative Commons Attribution 4.0 International (CC BY 4.0) https://creativecommons.org/licenses/by/4.0/ Some rights reserved.

Global Information Society Watch 2017 | Special edition Unshackling Expression: A study on laws criminalising expression online in Asia

ISBN 978-92-95102-86-6 APC Serial Number: APC-201711-CIPP-R-EN-DIGITAL-276



Disclaimer: The views expressed in GISWatch are not necessarily the views of APC or of its members

Table of contents

About the report: Unshackling Expression

Freedom of expression and opinion, the foundation stone of every free and democratic society, faces new and exacerbated challenges in online spaces. Throughout Asia and the world, people have taken to social media and online platforms to express themselves in ways that were not possible through traditional offline mediums. In response to this, and to the reach of the internet, states have sought to regulate and control online speech and expression. Offline regulations, typically in penal legislation, are applied to online spaces, to bolster internet-specific legislation. Legitimate expression on the internet is increasingly being redefined as cybercrime.

The range of expression online currently being criminalised includes content related to religion, sexual expression, gender identity, political opinion, dissent and factual statements – which is often prosecuted as blasphemy, obscenity, sexual deviance, sedition and criminal defamation. States often rely on legal provisions relating to public order, national security, decency and religion-based exemptions to crack down on legitimate forms of expression and dissent. Non-state actors, some of whom benefit from the tacit support of the state, have attacked (and sometimes killed) individuals for expressing themselves online.

In this special edition of GISWatch, Unshackling Expression, APC brings together analysis on the criminalisation of online expression from six Asian states: Cambodia, India, Malaysia, Myanmar, Pakistan and Thailand. While the report mostly focuses on criminalisation, curbs placed on expression using laws, regulations and policies are also discussed in parts. These countries were chosen for closer study based on preliminary assessment. These six states have several socio-political characteristics that are similar and varied. They have largely similar legal systems, since India, Malaysia, Myanmar and Pakistan are former British colonies and follow the commonwealth system. These countries were also chosen keeping in mind sub-regional balance and to bring to the table a diverse experience with laws and violations. All these states, amongst many others, criminalise online expression for a variety of reasons, which they set out in their constitutions and legislations. In these country reports, the authors identify and analyse the reasons for which online expression is criminalised, from defamation to sedition, hate speech to blasphemy, national security to contempt of court.

This special edition is ordered as follows: the first section provides an overview of the methodology adapted for the purposes of the reports, which is followed by an identification of the international standards on online freedom of expression and the regional trends to be found across the six states that are part of the study. This is followed by the country reports, which expound on the state of online freedom of expression in their respective states. With this report, we hope to bring to light the problematic trends in online freedom of speech and expression in Asia.

The first chapter, on the methodology developed by SMEX, an NGO based in Lebanon, looks at the reasons why we studied laws and the process followed for analysing offline and online legislation. For the purposes of the report *Unshackling Expression*, the methodology developed by SMEX was modified, specifically looking at freedom of expression online. However, the methodology proposed by SMEX can be applied to study any aspects of digital rights.

The chapter on international standards takes a close look at existing international norms starting with the guarantees and limitations prescribed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights regarding freedom of expression and opinion. The extension of these guarantees to online spaces as affirmed by the Human Rights Committee, UN Special Rapporteurs and resolutions is captured, affirming that human rights offline apply online as well. The chapter on regional trends looks at the common trends in the countries studied, outlining key issues identified.

The following chapters on Cambodia, India, Malaysia, Myanmar, Pakistan and Thailand study the constitutional and legislative guarantees for freedom of expression domestically. They then look at the offline and specific online legislation and regulation, where applicable, used to criminalise and curb freedom of expression. Emblematic cases are also highlighted to shed light on how these provisions are used.

With this report, we hope to expand this research to other states in Asia and to make available a resource that civil society, internet policy experts and lawyers can use to understand the legal framework domestically and to reference other jurisdictions.

A methodology for mapping the emerging legal landscapes for human rights in the digitally networked sphere

By Jessica Dheere
SMEX
https://www.smex.org

The methodology used to conduct the research for Unshackling Expression is based on a methodology developed by SMEX. This chapter provides an overview of the methodology's development and use. For the purposes of our own research, the methodology, insofar as it related to the classification of laws into legal foundations, fundamental rights and freedoms, governance of online and networked spaces, sectoral laws and other laws, was especially helpful in defining the scope and limitations. In each country, these classifications were applied to understand the nature of laws affecting cyberspace, and more particularly, the laws criminalising online freedom of speech and expression. Thus, the entire concept of digital rights was not adapted for Unshackling Expression; we restricted our research to the right to freedom of opinion, speech and expression online, and more narrowly, to laws that criminalise this right. Towards this end, we adapted the le*qal classifications to identify the laws that affect* freedom of speech online by way of criminalising such expression.

There are, of course, many ways in which governments restrict digital rights, including the right to freedom of opinion, speech and expression. Laws are merely one tool. However, laws form the primary legitimising tool to restrict digital rights. As Article 19 of the International Covenant on Civil and Political Rights (ICCPR) makes clear, any restriction on the right to freedom of expression must be grounded in law, and this law must be both enacted and made available to the public. Laws that criminalise speech online form a sub-category of laws that restrict digital rights, and comprise the subject of this report, Unshackling Expression.

Introduction: Why we need a methodology to identify laws affecting human rights in the online sphere

Why study laws that restrict digital rights?

Around the world, civic space is shrinking.¹ This contraction is in large part the result of attempts by governments to assert their sovereignty and regulate the internet and other aspects of the digitally networked sphere through legal controls. In many cases these controls aim to deal with legitimate challenges, such as certifying e-transactions, the theft of personally identifiable information, and other forms of internet-enabled crime, but often they are drafted from an uninformed or myopic perspective of how law, and thus rights, translate to the digital realm. In other cases, these controls consist of outdated legislation, such as analogue-era press and publications laws, clumsily interpreted for the digital sphere. In most cases, because the development and application of law to the digital realm is frequently ad hoc, it can be difficult for online rights advocates to conceptualise these frameworks, identify their weaknesses, analyse emerging trends, qualify their impact and, most important, push for reform.

In 2013, as the optimism of the so-called Arab Spring began to wane, governments in the Middle East and North Africa (MENA) reacted to the uprisings and revolutions by cutting off NGO funding, upping surveillance, and detaining and arresting activists and journalists under false pretences – frequently under cover of vague statutes and arbitrarily applied law.

To gain a better understanding of this emerging minefield of red lines, SMEX launched two separate but concurrent inquiries into the emerging legal framework for online expression and press freedom. The first, a pilot research initiative conceived

Bustos, C. (2017, 17 April). The Shrinking of Civic Spaces: What is Happening and What Can We Do? *Dejusticia*. https:// www.dejusticia.org/en/the-shrinking-of-civic-spaces-what-ishappening-and-what-can-we-do

and executed with support from Hivos' now-defunct iGmena programme,² involved collecting legislation related to the digital sphere in six Arab countries (Egypt, Iraq, Jordan, Tunisia, Lebanon and Syria); the second, a report commissioned by the Doha Centre for Media Freedom, prompted a broad review of existing documentation of the legal and policy framework for online media in all 22 countries of the Arab League. The exchange between these two projects yielded the first iteration of both a methodology for collecting, categorising and analysing digital rights-related legislation, and a solid baseline of data on the emerging legal landscape for digital rights in the Arab region, which we now call the Arab Digital Rights Datasets (ADRD).

A public version of the ADRD³ has resided on the online data visualisation platform Silk⁴ since 2015.⁵ It contains 142 individual laws from 20 Arab states, organised by country and keywords, many of them accompanied by translations to English or French. It is the product of the work of more than a dozen contributors, including lawyers, journalists, activists and technologists from the countries in question, who through an inductive research process⁶ gathered laws that they considered to affect digital rights. These included laws that:

- Establish or limit freedom of expression, freedom to assemble, the right to privacy, the right to access information and press freedom.
- Criminalise acts of speech, including over electronic channels.
- Regulate the industries that operate electronic communications channels.
- Govern content production and sharing, such as copyright and intellectual property laws.
- Govern electronic commerce, such as etransaction and esignature laws.
- Empower state surveillance.
- Have been cited in digital rights-related cases.

Working with a clearly delineated methodology

By cataloguing national-level legislation affecting the online sphere, SMEX aimed to assist not only activists but also human rights lawyers, judges, law and policy makers, researchers and journalists to build credible, compelling narratives for the protection and promotion of human rights in the digitally networked sphere. In the information collected and the patterns it could help us identify, we saw numerous opportunities to advance a common understanding of emerging legal frameworks for the online realm. Free and open access to such data would help human rights lawyers locate relevant articles and guiding jurisprudence. Digital rights legal researchers or journalists could access essential texts or other data liberated from PDFs and available outside legal database paywalls. Advocates, faced with a deluge of assaults on digital rights, might discover trends or pressure points that would help them better allocate limited campaign resources. The data could also be used to brief public officials and representatives who are committed to rights but struggle to keep pace with technology's implications for the societies we live in.

Initially released in September 2015 at an Internet Policy Observatory research methods workshop in Istanbul, the datasets found an early following among researchers at civil society organisations that document and defend digital rights. In April 2016, the Electronic Frontier Foundation (EFF) released The Crime of Speech,⁷ a report by Wafa ben Hassine, who relied heavily on the dataset. Soon afterward, the Association for Progressive Communications (APC) published Digital rights advocacy in the Arab world and the Universal Periodic Review,⁸ also by Ben Hassine, and Digital safety in context: Perspectives on digital security training and human rights realities in the Arab world,⁹ by Reem al-Masri, both of which cited the dataset as a source. The ADRD was also presented as example of data journalism and research on the blog of the Research Center at the CUNY Graduate School of Journalism.¹⁰

² https://www.igmena.org

³ http://smex.silk.co

⁴ As of August 2016, the Silk platform has been deprecated, meaning that despite allowing new accounts to be created, no technical support or development resources are being provided to the platform.

⁵ The Silk platform is being taken offline on 15 December 2017. SMEX is currently working with the human rights information management NGO HURIDOCS (https://www.huridocs.org) to develop a new platform to host the data.

⁶ Inductive research is a bottom-up approach by which a researcher begins with observations to detect patterns that can form the basis for a hypothesis that can be tested and developed into theory. It contrasts with deductive research that aims to test a hypothesis to prove a theory.

⁷ Ben Hassine, W. (2016a). The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online. Electronic Frontier Foundation. https://www.eff.org/pages/crime-speechhow-arab-governments-use-law-silence-expression-online

⁸ Ben Hassine, W. (2016b). Digital rights advocacy in the Arab world and the Universal Periodic Review. Association for Progressive Communications. https://www.apc.org/en/pubs/ digital-rights-advocacy-arab-world-and-universal-p

⁹ Al-Masri, R. (2016). Digital safety in context: Perspectives on digital security training and human rights realities in the Arab world. Association for Progressive Communications. https://www. apc.org/en/pubs/digital-safety-context-perspectives-digital-securi

¹⁰ http://researchcenter.journalism.cuny.edu/tag/tool /

Being able to release this data on Silk in a publicly usable format established proof of concept for the datasets and their utility. Equally important, it helped SMEX secure funding to further refine the data collection methodology and expand the scope of its application from the Arab region to similar initiatives worldwide, as APC-IMPACT has done with its research on the criminalisation of online speech in six countries in South Asia and Southeast Asia. Furthermore, it helped lay the groundwork for the transformation of the methodology into a shared technical standard whose adoption would not only facilitate free and open access to digital rights law and case law in countries worldwide, but also enable the combination of legal source data with other datasets, comparative analysis between jurisdictions, and the charting of global trends in digital rights.

The SMEX methodology was adapted for use in this report, *Unshackling Expression*.

Grounded, global and adaptable

Between August 2016 and July 2017, SMEX, working with legal adviser Nani Jansen and technology adviser Seamus Tuohy and a cohort of legal researchers, designed, tested and transformed a methodology to map, organise and make available digital rights-related laws. The result is the third version of the ADRD,¹¹ which now includes more than 240 laws and, where possible, their translations; relevant articles of law; bills; and case law.

In this phase of the project, the aim was not only to expand the ADRD but also to build on earlier, crowdsourced phases of development to produce criteria and a process for collection of law and case law that were 1) rigorous enough to gain credibility among human rights researchers and legal professionals, and 2) flexible enough to be adapted by civil society actors around the world, and particularly in the global South, for multiple purposes across multiple channels.

To achieve this, SMEX mapped out a multi-step process that began with soliciting feedback from about a dozen current and potential users of the dataset to better understand their wants and needs. Then, we aimed to ground the methodology in current digital rights definitions and legal practice, reviewing influential literature and initiatives, including rights charters and analysis; UN resolutions and reports by special rapporteurs; and analogous law aggregation projects such as the Centre for Law and Democracy's Global RTI Rating¹² and Graham Greenleaf's Global Tables of Data Privacy Laws and Bills.¹³ Meanwhile, our discovery of the decades-old Free Access to Law Movement¹⁴ and the many online legal information institutes (LIIs) it has spurred around the world helped anchor our project to a broader context in which "ready access to law is a human right."¹⁵ Next, we triangulated several approaches to setting criteria for the inclusion of specific laws and related documents – this time including articles, bills and case law – in the dataset, as well as establishing a five-category framework that would help both expert and non-expert re-searchers locate them.

Once we had a strong rationale for the inclusion of legislation and/or case law in the dataset, we recruited and trained a team of a dozen legal researchers to identify relevant legislation from the 22 countries of the Arab League and code the results in a country-specific research workbook. This information will eventually be transformed into a web- and API-accessible database that anyone can access.

Below we explain how the underpinnings of the refined methodology evolved with each step. We also detail the implementation of the methodology, including logistical stumbling blocks that we hope other adopters will avoid, and note recommendations for improvement. Finally, we share our plans for further development and solicit feedback. The Resources section at the end of this chapter makes available the current methodology and research guidance.

Developing the methodology: Step by step

Step 1: Taking stock: Stakeholder interviews inform the methodology

In October 2016, we conducted more than a dozen interviews with users of the Silk-hosted dataset. Users came both from within the Arab region and beyond and included human rights lawyers, researchers at advocacy organisations, experts in business and human rights, technologists, journalists, as well as a policy director and legal counsel at a global social media platform. During these interviews, we asked stakeholders what they currently

¹² www.rti-rating.org

¹³ Greenleaf, G. (2015). Global Tables of Data Privacy Laws and Bills (4th edition, January 2015). https://ssrn.com/abstract=2603502

¹⁴ www.fatlm.org

¹⁵ Jamar, S. D. (2001). The Human Right of Access to Legal Information: Using Technology to Advance Transparency and the Rule of Law. *Global Jurist Topics*, 1(2), 1-14. https://ssrn.com/ abstract=1148802

¹¹ It is not yet public, pending expert review of the data.

used the dataset for and what more they would like to be able to do with it, such as which legal processes the dataset could support and whether there were other datasets that, if combined with the legislation data, would yield deeper insights. From these interviews, we develop a list of recommendations for improving the datasets that included:

- Establishing a working definition of digital rights as a foundational framework to develop criteria for which laws, cases and decisions are included.
- Including context on the legal landscape that encompasses the type of legal system, relevant portions of major pieces of legislation, specific case law, and relevant international legal instruments binding on the state.
- Including draft laws, because it is easier to challenge a bill than to reform legislation.
- Including specific provisions of laws, such as sections or articles governing digital rights.
- Including the most important of well-known court decisions to understand how the judiciary perceives the issues.
- Including corporate policies, terms of service, privacy policies, etc.
- Indicating the source of the law or translation, and whether it is official, as well as creating a source-ranking methodology for secondary sources (i.e., ranking of some reports would be higher than others) and categorising sources as either primary or secondary.
- Refining the categorisation of the laws and adding subcategories and tags to make data more granular and searchable and in line with existing taxonomies and schema.
- Noting discrepancies between international treaties and national constitutions and laws.
- Considering the addition of laws that impact association and assembly, social media companies and applications, such as VoIP restrictions or shutdown decrees.

Interviewees also shared ideas about specific functionalities for the dataset, as well as its design, maintenance and expansion. Even ethical considerations arose, as some warned that highlighting court cases without redacting names could potentially re-victimise people.

After consulting with the legal and technical advisers, it was clear that we would not be able to include all items on the wish list. We prioritised those elements that we considered essential to building a minimum viable data product, based in part on the frequency with which they were mentioned. These included being more explicit about how we define digital rights to limit the scope of the inquiry; sourcing the documents and translations so that their provenance and whether they were official or unofficial was easily verifiable; identifying relevant provisions within documents to help users pinpoint those articles that are most directly connected to digital rights; and including draft laws, where possible.

Step 2: Developing a working definition of "digital rights"

Creating a database of legislation related to digital rights is a simple notion in theory; in practice, it is quite something else. To quote privacy scholar Graham Greenleaf, who has catalogued the world's data privacy laws, "Before answering a simple question" – like, how many countries have data privacy laws? – "it is sometimes necessary to answer some more complex questions first."¹⁶

For the purposes of his research, Greenleaf needed to define "What is a country?", "What is a law?", "What scope must a law have?", "What data privacy principles must a law include?" and "How effective must a law be?" By considering and answering these questions, Greenleaf established "the minimum criteria that reasonable and impartial observers could agree constitute a 'data privacy law' or 'data protection law' when satisfied."¹⁷ Because the datasets intend to catalogue legislation affecting digital rights we also need to ask, What are digital rights? and, How will we identify and locate a law or other legal instrument that affects digital rights?

Defining "digital rights"

Perhaps surprisingly, there is no commonly accepted definition of digital rights. Nor is it clear when the term first emerged.¹⁸ The European Digital

17 Ibid.

¹⁶ Greenleaf, G. (2014). Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. *Journal of Law, Information & Science, Special Edition: Privacy in the Social Networking World,* 23(1). https://papers.ssrn.com/sol3/papers. cfm?abstract_id=2280877

¹⁸ We theorise that it could have emerged as a derivative or truncation of the phrase "digital rights management" or DRM, a process by which code embedded into multimedia files, like movies or songs, prevents users from sharing files. Searching the archive with the term "digital rights" brought up 98 pages of results from as early as 2003. Until the late 2000s, most of the results containing "digital rights" pertained to DRM, a key advocacy issue for the Electronic Frontier Foundation.

Rights initiative (EDRi), a Brussels-headquartered "association of civil and human rights organisations from across Europe,"¹⁹ was founded in 2002, perhaps reflecting one of the earliest uses of the term. People have, however, been drafting bills of internet rights since at least the mid-1990s,²⁰ and over the last decade a strong body of interdisciplinary literature has emerged that considers digital rights as an extension of human rights with specific characteristics and implications.²¹ The UN Human Rights Council, for instance, has affirmed multiple times:

[T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights.²²

Notwithstanding these efforts and milestones, digital rights has not yet emerged as a field of its own. Referring to the literature that does exist, internet scholars Rikke Jørgensen and Meryem Marzouki write:

The majority of these sources, however, are not anchored in a theoretical framework but present empirically grounded studies of 1) opportunities and threats to established human rights standards by use of communication technology, in particular the right to privacy and the right to freedom of expression, or 2) cases that focus on the use of technology for human rights and social change, or 3) standard-setting that seeks to establish norms for human rights protection in the online domain. At present there is a lack of scholarship connecting the human rights challenges raised by these numerous studies with their theoretical context.²³ In addition, most of the many organisations²⁴ that advocate and promote digital rights similarly reflect this practical grounding by referring to other established normative frameworks, such as civil liberties and human rights, and then situating them semantically "online" or "on the internet". Thus, the phrase "digital rights" does not yet refer to a specific set of rights or theory of rights. Rather, it is shorthand for a broad group of rights issues raised when interpreting human rights and civil liberties in digitally networked spaces.²⁵

Given, as Jørgensen and Marzouki note, that "the modalities of the online realm provide significant challenges to human rights protection, many of which remain largely unexplored" - such as the so-called right to be forgotten or the right to access the internet²⁶ – what exactly is a digital right is still left open to interpretation, posing potentially significant challenges, one of which for our purposes is whether the term can be used as the cornerstone of a rigorous and replicable research methodology. One outcome of this conceptual instability is a propensity of digital rights actors to "pick up" their "right of interest, with limited attention to the overall framework and the interdependence between the full architecture of rights."27 In short, the question that emerges for our methodology is, Which rights satisfy the definition of digital rights when looking at the legal framework and which do not?

¹⁹ https://edri.org/about

²⁰ Gill, L., Redeker, D., & Gasser, U. (2015). Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. Berkman Center Research Publication No. 2015-15. https:// ssrn.com/abstract=2687120

²¹ Jørgensen, R. F. (2016). Negotiating boundaries: How platforms shape human rights. ipp.oii.ox.ac.uk/sites/ipp/files/documents/ boundary%25200II.pdf

²² Human Rights Council. (2016). The promotion, protection and enjoyment of human rights on the Internet. A/HRC/RES/26/13. https://digitallibrary.un.org/record/845727/files/A_HRC_ RES_32_13-EN.pdf

²³ Jørgensen, R. F., & Marzouki, M. (2015). Reshaping the Human Rights Legacy in the Online Environment. L' Observateur des Nations Unies, 38, 17-33.

²⁴ For instance, on its home page, Access Now, an international non-profit advocacy organisation founded in 2009, says it "defends and extends the digital rights of users at risk around the world." Nowhere on the site, however, does it define digital rights. It is left to visitors to interpret what digital rights are via the programme areas it covers: business and human rights, digital security, freedom of expression, net discrimination, and privacy. The San Francisco-based Electronic Frontier Foundation (EFF), founded in 1990, regularly uses the term "digital rights" in advocacy and press communications. Its mission, however, is phrased as "defending civil liberties in the digital world," including user privacy, free expression, and innovation. The organisation also maintains a web page called "Themes in Digital Rights", but does not define digital rights, except as through the themes listed, which include NSA spying, fair use, transparency, freedom of speech, drones, and blogger's rights, among others. Other digital rights advocacy organisations similarly skirt defining the term, except through their work. EDRi, for example, defends "rights and freedoms in the digital environment," in programme areas such as privacy, copyright, self-regulation, freedom of expression, security and surveillance. The objective of the Chile-based Derechos Digitales, whose name means "digital rights" in Spanish, is "the development, defence and promotion of human rights in the digital environment," encompassing free expression, privacy and personal data, and the rights of authors and access to knowledge. Digital Rights Ireland, meanwhile, "is dedicated to defending Civil, Human and Legal rights in a digital age." It currently campaigns on the issues of privacy and data retention, web blocking and filtering, and copyright reform.

²⁵ Here, we adopt sociologist Zeynep Tufecki's definition of "networked" from the preface to her 2017 book Twitter and Teargas: The Power and Fragility of Networked Protest, as "the reconfiguration of publics and movements through assimilation of digital technologies into their fabric."

²⁶ Jørgensen, R. F., & Marzouki, M. (2015). Op. cit.

²⁷ Ibid.

In the absence of an agreed-upon definition of digital rights, we had two choices: 1) to find another term to describe the scope of the datasets we wanted to build or 2) to propose a working definition of digital rights that met our primary goal of being able to set clear criteria for the inclusion of legal instruments in our database. In the first case, we considered other terms, such as "internet rights",28 which had been used early on by organisations like APC, or "internet freedom", a phrase that originated with the administration of former US Secretary of State Hillary Clinton. "Internet freedom",²⁹ we decided, was too closely tied to US government policy. Meanwhile, because it describes a configuration of technology. "internet" itself also seemed unnecessarily restrictive, or at least more restrictive than a broader term such as "digital", which could more easily encompass emerging technologies and locations other than the internet (such as data storage, biometrics and drones). We were also aware of other initiatives, like the Africa ICT Policy Database,³⁰ which aimed to collect all laws affecting information and communications technologies (ICTs). But for our purposes of identifying laws that had a direct impact, positive or negative, on human rights in digitally networked spaces, broadening the scope to include all laws that impact ICTs was deemed too broad.

Without a satisfactory alternative and given the already prevalent use of "digital rights" in the mission statements and names of so many of our peer organisations around the world, including in translation, we opted to propose a working definition based on existing literature and usage. We began by reviewing many of the key charters of digital rights and in a stroke of luck (searching the open Social Science Research Network) discovered that a 2015 article titled "Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights", by Lex Gill, Dennis Redeker and Urs Grasser, had already done much of our work for us.

Developing a working definition of "digital rights"

"Towards Digital Constitutionalism?" reviews 30 charters of internet or digital rights cumulatively endorsed by hundreds of groups from multiple sectors. The earliest charter is dated 1999; the most recent is from 2015. They include laws (adopted and proposed), official positions, and advocacy statements. From these charters, the authors extracted 42 aspects of digital rights in seven categories: basic or fundamental rights and freedoms, general limits on state power, internet governance and civic participation, privacy rights and surveillance, access and education, openness and stability of networks, and economic rights and responsibilities.

The authors observed that the charters all depend on the language of the Universal Declaration of Human Rights and to varying extents that of the ICCPR and the International Covenants on Economic, Social and Cultural Rights (ICESCR). The charters also all exhibit a "constitutional character", speak to a political community, aspire toward formal recognition and legitimacy within that community, and share a degree of comprehensiveness.³¹

Meanwhile, the bills are far from universal. They differ in their content and focus, their prioritisation of rights, the stakeholders involved and political communities targeted, contexts of reference, and drafting and review methods. Despite their common spirit, their diversity presents a challenge when trying to 1) decide what is a digital right, and 2) assess whether that right has been encoded in law, further underscoring the observation that there is no universal understanding or agreement on which rights constitute digital rights or how they are interconnected.

For example, advocates within the digital rights sector disagree on whether there is a right to access the internet or a right to be able to delist oneself from search results and be "forgotten". Both these "rights" appear in the list. The charters also acknowledge that other rights – workers' rights, children's rights, sexual rights – are significantly affected by digital technologies and in digital spaces. UNESCO considers the right to cultural diversity in education a kind of digital right in its book on internet governance, but does not mention the rights to association and assembly, as APC does in its conception of digital rights.³²

Meanwhile, internet rights are being defined as they are viewed through the lenses of rights and legal frameworks at the international, regional and national/local levels – both in legally binding treaties and legislation and in case law – as well as through the policies and practices of private-sector corporations, adding further complexity to understanding what is a digital rights law or a law that

²⁸ Released in November 2006, the Association for Progressive Communications' Internet Rights Charter was one of the earlier charters of digital rights. https://www.apc.org/en/pubs/ about-apc/apc-internet-rights-charter

²⁹ See, for example: https://www.state.gov/j/drl/internetfreedom/ index.htm

³⁰ www.ictpolicy.org

³¹ Gill, L., Redeker, D., & Gasser, U. (2015). Op. cit.

^{32 &}quot;Internet rights are human rights" multimedia toolkit, Association for Progressive Communications. www.itrainonline.org/ itrainonline/mmtk/irhr.shtml#Intro

implicates digital rights, especially when interpreting those rights in local jurisdictions. In addition, the ad hoc nature of establishing and interpreting digital rights through the law also means that our understanding of legal frameworks for digital rights at any level is far from comprehensive.

With all this in mind, we drafted a working definition of digital rights that attempts to capture their interdisciplinary, multidimensional, evolving nature. We wanted to highlight that these rights cannot be traced to a single authority or source, but rather are a product of distributed work, like the charters themselves. Further, we wanted to recognise that the spaces in which digital rights exist. like human rights, are unbounded. Thus, we adopted the phrase "digitally networked" to encompass not just the browsable internet but other digital networks. This is becoming even more important with the growing recognition that even people who are not connected online are increasingly affected by what happens in the digital sphere.33 Finally, we wanted to acknowledge that rights can be situated not just in content and interaction but also in other protocols, such as algorithms, on these networks or at their nodes, which come in the form of objects (devices) and in the form of expressions of our identities, whether individuals or groups, hidden, imagined, or in plain sight. Below is the definition we drafted. As a cornerstone of the refined methodology, it was meant to establish a reference point by which one can judge whether a law affects digital rights. It is a work in progress.

Working definition: "Digital rights" describe human rights - established by the Universal Declaration of Human Rights, UN resolutions, international conventions, regional charters, domestic law, and human rights case law - as they are invoked in digitally networked spaces. Those spaces may be physically constructed, as in the creation of infrastructure, protocols and devices. Or they may be virtually constructed, as in the creation of online identities and communities and other forms of expression, as well as the agency exercised over that expression, for example, management of personally identifiable data, pseudonymity, anonymity and encryption. Such spaces include but are not necessarily limited to the internet and mobile networks and related devices and practices.

33 Tufecki writes "digitally networked movements' or 'networked movements,' does not mean 'online-only' or even 'online-primarily.' Rather, it's a recognition that the whole public sphere, as well as the whole way movements operate, has been reconfigured by digital technologies, and that this reconfiguration holds true whether one is analyzing an online, offline, or combined instantiation of the public sphere or social movement action." Our working definition of digital rights served as a touchstone as we developed the rest of the methodology. In particular, it helped us devise a strategy for locating relevant legislation and then categorising that law.

Step 3: Establishing criteria and a research path to identify relevant legislation

Just as digital technologies have been integrated into every aspect of life, we can expect them to appear in multiple and increasingly diverse areas of law, from constitutions that make internet access a right, to health care laws that aim to protect patients' data privacy, to anti-terrorism laws that restrict speech glorifying violent extremism on online platforms. Radar Legislativo,³⁴ a legal data initiative from Brazil that tracks draft laws, recently counted 303 bills that affect the internet under review by that country's National Congress.³⁵ So even with the working definition in hand, we still needed to set criteria to help researchers narrow the field of inquiry and also give them a reasonable degree of certainty that the laws they found were in fact the laws they were looking for. To do this, we employed two complementary strategies: first, we looked at how Greenleaf identified data privacy laws, and second, we tried to locate the most likely areas in a legal framework where a researcher would find laws related to digital rights.

In Greenleaf's model, a researcher could identify a data privacy law in one of three complementary ways. First, they could look for laws that address data privacy principles, as defined by a "strong consensus' that has emerged as to what are a set of twelve 'fair information principles'."36 Even a law with provisions that address only some of the principles could qualify the law as a data privacy law. To apply this to the problem of identifying a digital rights law would mean identifying the kinds of laws that routinely affect digital rights, or that are designed explicitly to establish norms for digitally networked spaces. While we know of no "strong consensus" about what laws might comprise a list of digital rights-related laws, we can deduce from the laws we and others have collected that it would likely include data privacy laws, right to information laws, etransactions laws, anti-cybercrime laws, and broad internet laws like Brazil's Marco Civil da Internet (Civil Rights Framework for the Internet).³⁷

³⁴ https://www.radarlegislativo.org

³⁵ Conversation with Kimberly Anastácio, Coding Rights, 18 October 2017.

³⁶ Greenleaf, G. (2014). Op. cit.

³⁷ www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180

Conversely, a researcher might define a law as affecting digital rights even if its scope was not limited to the internet and digitally networked spaces. For instance, an intellectual property law may deal with works produced in both analogue and digital media, but its sections or provisions dealing specifically with the internet or digitisation would qualify it as a law affecting digital rights. With that in mind, we could use Gill et al.'s 42 rights³⁸ as a kind of checklist when analysing laws of any kind for their effects on digital rights.

Finally, because law is constituted not just by static text but by interpretation, Greenleaf emphasises the importance of international law and soft law. In the case of data privacy laws, he specifically refers to the OECD Privacy Guidelines of 1981 and the Council of Europe Data Protection Convention 108 of 1981. From this approach, we can assess whether a law affects digital rights, or a specific digital right, based on the growing body of analysis of digital rights within international covenants and related human rights frameworks, such as the ICCPR and ICESCR, special rapporteur reports, and their derivatives, including the digital rights charters, data privacy and access to information frameworks mentioned above, as well as other frameworks such as the UN Guiding Principles on Business and Human Rights, etc. We would add to that interpretation of law by courts and tribunals in case law and other types of precedent that would afford insight not only into how laws were being applied but also into how laws with no overt relationship to digitally networked spaces might be adapted or abused.

We believed this triangulated approach would help researchers recognise a digital rights law when they saw it. Still, we knew that researchers could not and would not read every law on the books to decide whether or not they affected digital rights. With this in mind, we aimed to ease the search further by offering several entry points for their inquiries. Working from types of law developed for the existing laws in the dataset and category structures devised by Gill et al.³⁹ and ARTICLE 19,⁴⁰ we developed five categories⁴¹ into which we believed the majority of laws would fall: 1) legal foundations, 2) fundamental rights and freedoms, 3) governance of online and networked spaces, 4) sectoral laws, and 5) other laws.

In the *legal foundations* category, we intended to collect laws that (1) form part of the foundation of the legal system and address universal rights, responsibilities, due process or, following Gill et al., other "general limits on state power,"⁴² and (2) contain provisions that refer or apply to how an individual can exercise their rights and freedoms in digitally networked spaces. Examples of laws that would fit in this category include constitutions, basic laws, penal codes and codes of procedure.

We described laws pertaining to *fundamental rights and freedoms* as those laws and regulations that (1) establish norms for, enable or restrict the exercise of fundamental rights and freedoms – including the right to freedom of expression, privacy, freedom of religion and freedom of association – and (2) contain provisions that refer or apply to how an individual can exercise these rights and freedoms in digitally networked spaces. Examples are press laws or laws protecting or limiting the right to privacy, freedom of expression or to access information.

The drive to establish new norms in the digitally networked sphere and to mitigate the negative potential of digital technologies – realised as computer fraud and identity theft, the circulation of child pornography, online harassment, so-called "revenge porn" and doxxing, for instance – has been the genesis of many newer laws and regulations explicitly for *governing online, networked spaces*, a category developed to collect laws such as data privacy and protection laws, anti-cybercrime laws, and net neutrality regulations. Here, we might also find laws or judicial decisions that acknowledge the new so-called right to be forgotten, a concept that did not exist before the internet.

Digital technologies have had a pervasive effect on some industries and sectors, and the laws and regulations in these sectors are sometimes some of the first that deal with the new modalities of the online realm directly and in depth. To acknowledge this, we created a category for *sectoral laws*. Specifically, we sought laws and regulations that (1) update or establish norms that implicate digital rights in a specific sector, such as banking or health care, or for a specific group of people, such as government employees, and (2) contain provisions that

³⁸ Gill, L., Redeker, D., & Gasser, U. (2015). Op. cit.

³⁹ Gill, Redeker and Gasser organised the 42 rights extracted from the 30 charters into seven categories: Basic or Fundamental Rights and Freedoms, General Limits on State Power, Internet Governance and Civic Participation, Privacy Rights and Surveillance, Access and Education, Openness and Stability of Networks, and Economic Rights and Responsibilities.

⁴⁰ ARTICLE 19 used six categories of inquiry when analysing how the laws in the Internet Legislation Atlas (affected digital rights in seven Middle Eastern countries: constitutional protection, regulation of online content, regulation of media workers, regulation of internet intermediaries, surveillance and data protection, and access to the internet and net neutrality. See: https://internetlegislationatlas.org/#/about/ executive-summary#breakdown

⁴¹ ADRD Research Guidance Document (see the Appendix to this chapter).

⁴² Gill, L., Redeker, D., & Gasser, U. (2015). Op. cit.

refer or apply to how an individual can exercise their rights and freedoms in digitally networked spaces. Examples here are laws on electronic patient files, consumer protection, or issues such as privacy in the workplace.

Finally, in some countries, laws having no specific language on digital rights had been used to repress free expression. For example, in Tunisia, drug laws have been used to prosecute alleged speech crimes.⁴³ Around the world, anti-terror laws are regularly being used against journalists.⁴⁴ In the US, a law meant to curtail copyright infringement was ultimately rejected for its potential to chill speech.⁴⁵ And in Vietnam, tax laws are regularly used to prosecute bloggers.⁴⁶ To acknowledge this phenomenon, we created a category of *other laws* to capture the counterintuitive and sometimes systematic use of laws not in the first four categories. Identification of these laws often depends on monitoring and analysis of case law.

Because legal systems are always changing, being amended, reinterpreted, appealed, the triangulation process and the five-category structure did not always support clear-cut decisions. The research process surfaced differing opinions about which laws qualified as affecting digital rights, where to categorise a law, or whether one law could fit into two categories. For example, some researchers elected not to include press and publications laws if they did not expressly mention electronic media. Others saw the potential for these laws to be used to restrict digital spaces, so they listed them. Then, there were divergent approaches to categorisation: does a press and publications law belong in the fundamental rights and freedoms category or is it a sectoral law?

While perfect precision is not possible, the aim was to help researchers blaze a path through complex and evolving legal systems by offering several entry points where one might find digital rights-relevant law. Grounding the research and review process in a consistent approach would yield more or less comparable results that could be further refined during peer and expert reviews. The next challenge was to transform these underpinnings - the working definition of digital rights, the triangulated criteria for identifying relevant laws, and the five-category structure – into a usable, adaptable research methodology and to launch the research process.

Step 4: Concretising and implementing the methodology

We had three main goals when developing the research methodology and guidance. First, we wanted it to be simple and accessible enough that any researcher – even ones without legal research experience – could use it. Second, we wanted it to be flexible enough that it could be adapted by other initiatives around the world doing similar types of work. Third, we wanted to be able to share this methodology and a collection of user scenarios for using the data with a technologist to develop a machine-readable data model that would undergird future applications that make use of the data.

The implementation phase by and large demonstrated that the methodology successfully met our goals of being rigorous enough to gain credibility among users seeking verified legal information yet flexible enough to be adapted to different jurisdictions and legal themes. There were challenges, however, and for future applications, we have identified opportunities for further refinement in each section below.

Creating data collection tools and guidance

For data collection, we created a multi-tab workbook in Google spreadsheets and individual folders for each country on Google Drive. We then produced two research guidance documents: ADRD Research Guidance and ADRD File Management and File-Naming Formats. Both these documents are included in the Resources section.

The data collection workbooks functioned as an index for three key types of information: original laws, case law and draft law. Researchers were asked to name the laws in the original language and to upload the document to a corresponding Google Drive folder – using the prescribed file-naming convention - and indicate the link to the law in that folder. For each type of information, we also asked for relevant translations. For laws and bills, we asked researchers to identify the key provisions that affect digital rights. For case law, we asked for a summary of the impact of the decision on digital rights. In addition to this key data, we also gathered metadata such as dates, keywords and sources. The workbooks also included a cover sheet with links to the research guidance, a tab where researchers

⁴³ Ben Hassine, W. (2016a). Op. cit.

⁴⁴ Ginsberg, J. (2017, 26 October). Targeting journalists in the name of national security. *Index on Censorship*. www.indexoncensorship. org/2017/10/targeting-journalists-name-national-security

⁴⁵ SOPA/PIPA: Internet Blacklist Legislation, Electronic Frontier Foundation. https://www.eff.org/issues/ coica-internet-censorship-and-copyright-bill

⁴⁶ Jansen, N. (2013, 9 July). Advocates Keep Spotlight on Le Quoc Quan. Global Voices. https://advox.globalvoices.org/2013/07/10/ advocates-keep-spotlight-on-le-quoc-quan

could note laws currently in the dataset that should be removed, a sheet asking researchers to note their general sources of information, and a locked data validation tab. The workbooks summarised relevant research guidance at the top of each column.

The country folders contained five subfolders and two spreadsheet documents. Two folders corresponded to the laws and draft laws, each of which had subfolders for each category of law. A third folder was for case law, a fourth for translations, and the fifth was for secondary sources. One spreadsheet listed the laws currently in the ADRD dataset and the second was the new data collection workbook.

For further refinement: While Google Drive and Docs satisfied our needs for an easily accessible and configurable tool - especially for being able to share documents among several users and track comments between them - there was at least one researcher who had trouble negotiating the folder structure and creating links to shared files. In addition, we used available data verification features to populate dropdown menus from one spreadsheet to another. This worked seamlessly when connecting original laws to their translations, for example, but not as well when connecting articles of law to primary or secondary legislation. For example, on the key provisions worksheet, researchers were asked to enter relevant articles. These entries populated a dropdown menu in the case law spreadsheet. But when a researcher wanted to indicate which article was relevant to the case law, they would sometimes see two articles with the same number but from different laws and not know which to choose, potentially leading to documentation errors. In future iterations of the workbook, we will explore tools that would make it more difficult for researchers to make these and other kinds of coding errors. Finally, organisations that prefer not to use Google products for security reasons may also want to adapt the workbook to other tools.

Recruiting and orienting researchers

Earlier data collection was conducted by volunteers and journalists, but not legal experts. Because the refined methodology relied much more on an understanding of law and legal systems, we prioritised working with lawyers preferably with expertise in the countries they were researching, or at least in the region. We launched a 10-day call for legal researchers⁴⁷ and although our timeline was short we received 16 applications, among them researchers who had worked on the previous versions. Twelve candidates were contracted to do one round of research and one round of peer review. Some candidates took on more than one country. Researchers came from Egypt, Jordan, Lebanon, Morocco, Oman, Palestine, Sudan, Syria, Tunisia and Yemen, as well as the US and France.

Researchers were asked to attend one of two one-hour virtual orientation sessions48 held by SMEX and led by legal adviser Jansen. Before the orientation session, researchers were able to review the data collection workbook and the research guidance and make suggestions for refinements. The sessions began with an overview of the scope of work and then relied on researchers to ask guestions to clarify any unclear guidance. They also noted specificities within national legal systems that would pose challenges to capturing data in the format we had provided. For example, it was noted that in some jurisdictions, amendments are issued separately from the laws to which they apply, rather than integrated into a reissued law. This, plus questions about whether regulations should also be included, resulted in adding a column that gualified laws as either primary or secondary. Researchers raised concerns about different definitions of case law, which was clarified as referring to "judicial decisions and other jurisprudence that constitutes an authoritative interpretation of the law."49 Also with regard to case law, some researchers relayed that in their jurisdictions the names of the parties are not used to name the cases. To create unique case names, researchers were asked to assign unofficial names to the cases. These notes and others were captured in an addendum to the research guidance document (available in the Resources section at the end of this article) called ADRD Workbook Updates Doc.50

After the sessions, a Google Group mailing list was set up where researchers could ask questions during the data collection process and further refine the research guidance as needed.⁵¹ More active researchers posed sporadic queries to the mailing list, but many remained quiet, making it necessary to follow up on an individual basis, which was burdensome given that one person was managing 12 researchers and 22 workbooks.

⁴⁸ Budget constraints prevented us from being able to host an inperson training workshop.

⁴⁹ https://docs.google.com/document/d/11NAys-JDDiU4Ht4VLyV4H PH3dzVqBxKwrsvUYTIoLQE/edit

⁵⁰ Ibid.

⁵¹ ADRD Summary Report, August 2017, submitted by Nani Jansen.

For further refinement: In retrospect, the short time frame for recruiting and training researchers led to some inconsistencies in the research results. In particular, the legal adviser's review revealed that not all researchers demonstrated the same understanding of the level of detail being requested, which has led SMEX to conduct additional rounds of review. In future, we recommend that, when resources are available, in-person trainings on the research methodology and workbook should be organised and attendance should be a condition of payment. A longer, multi-round recruitment process, with some kind of assessment to measure the researcher's capacity and eve for detail, would also be useful and help expedite data review and verification.

Data collection and review: Findings and challenges

After five months' preparation, data collection began in early March 2017. Researchers were given one month to complete the original research process and one month to complete their peer review, which involved checking the folder and workbook of a second country.

Three researchers dropped out before the research was complete for health and family reasons. Meanwhile, one researcher revealed late in the process that they did not read Arabic. Also, because some researchers were behind schedule, the peer review process was also delayed. Ultimately, the first round of original research and peer review concluded in June 2017.

In July 2017, SMEX and the legal adviser conducted an overall review of all the workbooks. In all, the law catalogues grew from 142 in the first dataset to around 240, the vast majority of them with official or unofficial translations. Dozens of key provisions were identified. Several draft laws were noted, and case law, a completely new type of information in this version of the ADRD, was identified in six countries.⁵² Following a final review by SMEX and in-country experts, the expanded datasets will be made public.

For further refinement: As mentioned above, SMEX has added two more rounds of review to ensure that the data we have is as accurate and upto-date as possible. Unfortunately, this has delayed making the data available, which could also compromise its accuracy, if too much time passes. To avoid such delays in the future, we recommend that research supervisors implement a phased approach with interim milestones. For example, data could be collected, reviewed and verified for one worksheet at a time and combined with periodic group calls to raise and resolve concerns or challenges encountered. This would not only help ensure that researchers develop a shared understanding of the nuances of the research process but will also yield better results that can be publicised more quickly.

Finally, while we included draft laws and provisions and case law in the current workbook in response to stakeholder requests for this data, we are delaying their integration into the public dataset pending more detailed research and review. Gathering data about case law posed several problems with regard to not only locating and sourcing decisions but also in developing a consistent approach to explaining how cases interpret the relevant laws, which is essential to being able to publish authoritatively on their impact. In subsequent phases of the project, we will explore addressing such challenges by integrating into the methodology existing approaches to analysing case law, such as that of Columbia University's Global Free Expression Case Database.53

The future roadmap

Perhaps unlike other research methodologies, the one for the Arab Digital Rights Datasets was also designed to be expressed as a data model, or a conceptual framework to organise and standardise the data collected. Rendering the methodology as a data model makes it much easier to share, extend, combine and repurpose information, especially by machines. In parallel with the data collection and review process, we worked with technologist Seamus Tuohy to create the data model for the ADRD and a related API, or application programming interface. An API is a piece of code that sits between a database and a graphic user interface (GUI) that calls information from the database according to what a user needs.

This data model and API will be used to build a database of the Arab laws collected and make the data both human and machine-readable. But it is our hope that these technical interpretations of the methodology will also afford other organisations conducting similar research the opportunity to make their data more available and accessible too. To this end, SMEX is now forming a working group to explore the potential for this data model to become a global standard for aggregating, organising

⁵² Case law was identified in only six countries: Egypt, Jordan, Kuwait, Lebanon, Morocco and Mauritania.

⁵³ https://globalfreedomofexpression.columbia.edu/cases

and analysing the evolution of digital rights law and to encourage other researcher-technologist teams to develop new applications that draw on this data and/or combine it with other datasets. Other challenges we will turn our attention to as the project develops include devising strategies for keeping the information up-to-date across many countries, as well as for tracking draft laws and new cases. If you would like to be a part of this group, we encourage you to let us know at adrd@smex.org.

Resources for implementing the methodology

ADRD Research Guidance

https://docs.google.com/document/d/1vxKMC-GIXcQoFPqubRyJS9Io8Jq9hBboEE5a7IcvoxCs/ edit# ADRD Workbook Updates Doc

https://docs.google.com/document/d/11NAys-JD-DiU4Ht4VLyV4HPH3dzVqBxKwrsvUYTIoLQE/ edit

ADRD File Management & File-Naming Formats https://docs.google.com/document/d/17ALaTotCXy-8evSWscoKcF5VFmVdUM-xP_MWAPUH37M/ edit

ADRD Sample Data Collection Workbook: Egypt https://docs.google.com/a/smex.org/ spreadsheets/d/1rQoRdXDBqLWgyCgWEmOUzAkdClLt7U2YRTHFSh1JbFo/ edit?usp=sharing

Data Model and API To access the current versions of the data model or API, please email jessica@smex.org.

Understanding international standards for online freedom of expression

Geetha Hariharan

In this report, Unshackling Expression, APC and its partner organisations study the state of freedom of expression on the internet in six Asian countries: Cambodia, India, Malaysia, Myanmar, Pakistan and Thailand. While the national reports provide an indepth study of the state of freedom of expression online in the six countries, a study of internet rights in Asia is incomplete without a preliminary study of the international standards for freedom of expression. International standards form the yardstick, the baseline, for national standards on freedom of expression – and are the standards to which national laws must adhere. The six countries that form part of this study also have protections for freedom of expression in their constitutions, and most of these states are parties to international human rights treaties, imbuing them with an obligation to protect and respect international standards for the protection of human rights.

Unshackling Expression is a study of the criminalisation of and curbs placed on freedom of expression using laws and policies at the domestic level. A harsh measure, criminalisation affects the freedom of expression of people both directly and indirectly. Directly, it forms a clear, physical restraint on speakers who make their views known online. Indirectly, it causes a chilling effect on citizens, often resulting in self-censorship, leading to a less diverse and more conformative cyberspace. Further, restrictions on freedom of opinion and expression adversely affect the right to "to seek, receive and impart information and ideas of all kinds." In a 2011 report to the UN Human Rights Council, former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, states:

[L]egitimate online expression is being criminalized in contravention of States' international human rights obligations, whether it is through the application of existing criminal laws to online expression, or through the creation of new laws specifically designed to criminalize expression on the internet. Such laws are often justified on the basis of protecting an individual's reputation, national security or countering terrorism, but in practice are used to censor content that the Government and other powerful entities do not like or agree with.¹

Freedom of expression is particularly crucial when it comes to the internet. Offline, one may have multiple ways of expressing oneself, but online, publication and participation are the first acts. All exercise of freedom of expression online begins with the act of publication – whether it be a publication of views through writing, posts, comments, messages or tweets, or through the use of visual, video or audio content. As such, any restriction on online content becomes a harsh restraint on freedom of expression, and none more so than the criminalisation of content or other forms of expression. Not only this, but in Asia in particular, there are several trends that are problematic to the free use of the internet.

In this chapter, we consider the international standards that define freedom of expression, and in particular, freedom of expression online, and also take a look at the regional standards established by the Association of Southeast Asian Nations (ASEAN).

International standards on freedom of speech and expression online

The history of the right of freedom of speech and expression precedes the internet. It finds its beginnings in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). As a binding treaty, the IC-CPR has more value in international law. The UDHR and ICCPR guarantee certain inalienable rights to

¹ La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/17/27. https://www.un.org/ga/ search/view_doc.asp?symbol=A/HRC/17/27

human beings. Recognising the inherent dignity of all beings, the ICCPR and UDHR guarantee, *inter alia*, the right to freedom of expression,² the right to privacy,³ the right against advocacy of national, religious or racial hatred (it has been understood as the right against "hate speech")⁴ and the right to freedom of religion.⁵ Moreover, the ICCPR prohibits discrimination on grounds of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.⁶ These rights, among all the others guaranteed under the ICCPR, are available to all human beings, regardless of their countries of origin and residence.

The right to freedom of opinion and expression is a crucial right in the ICCPR. It is the "foundation stone of every free and democratic society."⁷ Without freedom of expression, the full development of the individual is impossible. Moreover, the "marketplace of ideas" aids the pursuit of truth. Without freedom of expression, the autonomy of an individual may be considered curtailed and restrained.

The importance of the right led the Human Rights Committee to hold that a general reservation to paragraph 2 of Article 19 of the ICCPR was unacceptable.⁸ Article 19 of the ICCPR as well as the UDHR guarantees the right to hold opinions without interference and guarantees everyone the right to freedom of expression and the right to receive and impart information, regardless of frontiers. Any limitations placed on this right must meet the standards required and justified by provisions in

- 3 Article 17, ICCPR: (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks.
- 4 Article 20, ICCPR: (2) Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.
- 5 Article 18, ICCPR: (1) Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching; (2) No one shall be subject to coercion which would impair his freedom to have or to adopt a religion or belief of his choice...
- 6 Article 26, ICCPR.
- 7 Human Rights Committee. (2011). General comment No. 34, Article 19: Freedoms of opinion and expression. CCPR/C/GC/34. www2. ohchr.org/english/bodies/hrc/docs/gc34.pdf

Article 19(3) of the ICCPR. Article 19 of the ICCPR reads:

(1) Everyone shall have the right to hold opinions without interference;

(2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice...

As the text of the right makes clear, the right to freedom of opinion, speech and expression is available regardless of borders or frontiers. More importantly, it is available *through any media* of one's choice. It is this terminology that is crucial when considering freedom of speech online.

In addition to the international treaties, several regional charters also guarantee the right to freedom of opinion and expression. In Asia, it is the ASEAN Charter⁹ and the ASEAN Human Rights Declaration¹⁰ that enshrine this right. Vowing to respect and protect "human rights and fundamental freedoms," the ASEAN Charter incorporates as one of its principles the "respect for fundamental freedoms, the promotion and protection of human rights, and the promotion of social justice." Article 14 of the Charter states that "ASEAN shall establish an ASEAN human rights body" in accordance with the purposes and principles of the ASEAN Charter.

Taking off from this, the ASEAN Intergovernmental Commission on Human Rights was established in 2009, and the ASEAN Human Rights Declaration was unanimously adopted in November 2012. Under Article 23 of the ASEAN Human Rights Declaration:

Every person has the right to freedom of opinion and expression, including freedom to hold opinions without interference and to seek, receive and impart information, whether orally, in writing or through any other medium of that person's choice.

In its General comment No. 34, the Human Rights Committee confirmed the applicability of Article 19 online, equally as it applies offline.¹¹ The General Comment contains the authoritative interpretation of Article 19, including the scope and extent of the right.

² Article 19, ICCPR: (1) Everyone shall have the right to hold opinions without interference; (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice...

^{8 &}quot;[A] general reservation to the rights set out in paragraph 2 would be incompatible with the object and purpose of the Covenant." Ibid., at para. 6.

⁹ www.hrlibrary.umn.edu/research/Philippines/ASEAN%20Charter. pdf

¹⁰ www.mfa.go.th/asean/contents/files/ other-20121217-165728-100439.pdf

^{11 &}quot;They include all forms of audio-visual as well as electronic and internet-based modes of expression." Human Rights Committee. (2011). Op cit., at para. 12.

The Human Rights Committee holds that there shall be no exceptions to the right to hold opinions, whether they are of a "political, scientific, historic, moral or religious nature."¹² In particular, the Committee makes clear that it is unacceptable to criminalise the holding of an opinion:

The harassment, intimidation or stigmatization of a person, including arrest, detention, trial or imprisonment for reasons of the opinions they may hold, constitutes a violation of article 19, paragraph 1.¹³

As we shall see in the following national reports, the Asian states that form part of this study stand in potential violation of this understanding of Article 19, paragraphs 1 and 2. Moreover, the right to freedom of expression encompasses a wide variety of activities, including offensive speech (not falling within the ambit of Article 20, ICCPR),¹⁴ and applies to "all forms of audio-visual as well as electronic and internet-based modes of expression."¹⁵

In addition to Article 19. Article 20 of the ICCPR also impacts speech. Article 20 prohibits any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. Speech that falls within the ambit of Article 20 (as hate speech) cannot merely be offensive, but must have an intent to cause harm, and be likely to cause harm. That is, for speech to fall within the definition of hate speech, it must have the quality of inciting imminent violence.¹⁶ It cannot merely be a statement, but rather a call to violence on any of the above grounds, in order to gualify as hate speech. While restrictions are permissible on the above given grounds, they must also be necessary and proportionate to the aim sought to be achieved, and imposed by law.

Where the internet is concerned, the abovementioned report of former Special Rapporteur Frank La Rue gathers importance. La Rue highlights the "unique and transformative nature of the Internet not only to enable individuals to exercise their right to freedom of opinion and expression, but also a range of other human rights."¹⁷ The internet enables individuals not merely to be passive

12 Human Rights Committee. (2011). Op. cit., at para. 9.

13 Ibid.

14 Human Rights Committee. (2000, 18 October). Communication No. 736/97, Ross v. Canada.

15 Human Rights Committee. (2011). Op. cit., at para. 12.

16 Khandhadai, G. (2016). Desecrating Expression: An Account of Freedom of Expression and Religion in Asia. Bytes for All, Pakistan and FORUM-ASIA. https://www.forum-asia.org/uploads/ wp/2016/12/Final_FOER_Report.pdf

17 La Rue, F. (2011). Op. cit.

receivers of information, but to be active publishers of knowledge and information, for the internet, as an interactive medium, enables individuals to take active part in the creation and dissemination of information.

Moreover, the Human Rights Council has affirmed that offline human rights must be equally protected and guaranteed online. In its 20th session (29 June 2012), the Human Rights Council adopted a resolution which unanimously declared:

[T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.¹⁸ (Emphasis supplied.)

However, it is important to remember that the right to freedom of speech and expression is not absolute. The ICCPR states that the right may be curtailed, if necessary and if provided by law, for the following reasons:

For respect of the rights or reputations of others;

For the protection of national security or of public order (*ordre public*), or of public health or morals.¹⁹

The ASEAN Human Rights Declaration goes one step further. Its clause on restrictions, Article 8, states:

The human rights and fundamental freedoms of every person shall be exercised with due regard to the human rights and fundamental freedoms of others. The exercise of human rights and fundamental freedoms shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition for the human rights and fundamental freedoms of others, and to meet the just requirements of national security, public order, public health, public safety, public morality, as well as the general welfare of the peoples in a democratic society.

As the text makes clear, the ASEAN Human Rights Declaration expands the scope of justifications on the basis of which the right to freedom of opinion and expression may be restricted. In addition to the justifications provided in the ICCPR, the ASEAN

¹⁸ Human Rights Council. (2012). The promotion, protection and enjoyment of human rights on the Internet. A/HRC/20/L.13. https://daccess-ods.un.org/TMP/3578843.1763649.html

¹⁹ Article 19(3), ICCPR.

Human Rights Declaration also adds public safety and the vague and open-ended "general welfare of peoples in a democratic society" as legitimate aims for the restriction of freedom of speech.

While restrictions are indeed permissible, they must meet tests of permissibility: they must be outlined by law, necessary and proportionate to protect a legitimate aim. These are the conditions laid down in the UDHR and the ICCPR. The test of legality requires that the restriction set by any government on the right to freedom of expression be expressly laid out in a law. This legislation, order or bylaw must be publicly available and understandable by the public, and no restriction is valid unless it has the backing of the law.²⁰ The law must be both *accessible* and *foreseeable*.²¹

Not only must the restriction be based in law, it must also be *legitimate*. The test of legitimacy requires that the restriction on freedom of expression be based on one of the justifications laid out in Article 19(3).²² What are these justifications? Article 19(3) states that "protection of national security or of public order (*ordre public*), or of public health or morals" and "respect of the rights or reputations of others" constitute legitimate reasons for the restriction of freedom of expression. Any restriction - and indeed, criminalisation – of expression that does not fall in with these justifications is liable to be contested as falling foul of Article 19, ICCPR.

Finally, the test of necessity and proportionality requires that the restriction be based on a "pressing social need" which makes the restriction "necessary in a democratic society."²³ It must be placed so as to fulfil the aims set forth in Article 19, paragraph 3, ICCPR. Of course, the state has a margin of appreciation in testing the necessity of the restriction, but the margin is narrow where freedom of expression is considered.²⁴ In determining pressing social need, the test of pluralism, broadmindedness and tolerance is to be applied,²⁵ which accommodates divergent views and opinions.

Not only this, but the restriction placed by the state on freedom of expression must be *proportional* – i.e., the *least onerous* restriction must be applied to *appropriately meet* the need.²⁶ A broad restriction is unacceptable, and the restriction must be narrowly tailored. For instance, the incidence of internet shutdowns across the world, where access to the internet is completely cut off in response to any situation (primarily, states use the excuse of security) is *disproportional* to the aims of the restriction,²⁷ and so would be contested under Article 19, paragraph 3.

²⁰ *Hinczewski* v. *Poland*, No. 34907/05, § 34, ECHR 2010 (ECHR).

²¹ Keun-Tae Kim v. Republic of Korea, Communication no. 574/1994 CCPR/C/64/D/574/1994 (4 January 1999) (HRC); Sunday Times v. United Kingdom (no. 2), Judgment of 26 November 1991, no. 13166/87, Series A no. 216 (ECHR); Article 19 v. Eritrea, (2007) AHRLR 73 (ACHPR 2007).

²² Vladimir Petrovich Laptsevich v. Belarus, Communication no. 780/1997, § 8.5, UN Doc. CCPR/C/68/D/780/1997 (2000) (HRC); Vladimir Velichkin v. Belarus, Communication no. 1022/2001, § 7.3, UN Doc. CCPR/C/85/D/1022/2001 (2005) (HRC).

²³ Jacobs, F. C., & White, R. C. A. (1996). The European Convention on Human Rights. Oxford: Clarendon Press; Handyside v. United Kingdom, Judgment of 7 December 1976, Series A no. 24 (ECHR); Vogt v. Germany (no. 1), Judgment of 26 September 1995, Series A no. 323 (ECHR); Proposed Amendments to the Naturalization Provisions of the Constitution of Costa Rica, Advisory Opinion OC-4/84, (1984) (Inter-Am. Ct.); Prince v. South Africa, 2004 AHRLR 105 (ACHPR 2004).

²⁴ Lehideux & Isorni v. France, no. 22662/94, ECHR 1998-VII (ECHR); Schwabe v. Austria, Judgment of 28 August 1992, Series A no. 242-B (ECHR).

²⁵ Handyside v. United Kingdom, Judgment of 7 December 1976, Series A no. 24 (ECHR); Sunday Times v. United Kingdom (no. 1), Judgment of 26 April 1979, Series A no. 30 (ECHR); Dudgeon v. United Kingdom Judgment of 23 September 1981, Series A no. 45 (ECHR).

²⁶ The Queen v. Minister of Agriculture, Fisheries and Food and Secretary of Health, ex parte Fedesa and others, [1990] ECR I-4023 (ECJ); Klass v. Germany, Judgment of 6 September 1978, Series A no. 28 (ECHR); Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism, §§ 33-5, 54, Advisory Opinion 5/85 (1985) (Inter-Am. Ct.); Nebraska Press Association v. Stuart; Reno v. ACLU 521 U.S. 844 (1997) (US Sup. Ct.); Human Rights Committee. (2011). Op. cit., at para. 34: "[...] must be the least intrusive instrument amongst those which might achieve their protective function."

²⁷ Kaye, D. (2017). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/35/22. https://undocs.org/A/HRC/35/22.

Regional trends in criminalisation of expression online: An overview

Geetha Hariharan

Some speech is criminal, says the law. *Unshackling Expression* is about this speech, which, legitimately or otherwise, is criminalised in the six states across Asia that are addressed in this report. It studies the criminalisation, and more broadly, some of the restrictions that are placed on the right to freedom of opinion and expression on the internet in Cambodia, India, Malaysia, Myanmar, Pakistan and Thailand. These states were chosen as representative of South and Southeast Asia, and therefore show us a representative picture of the state of freedom of expression on the internet in the region.

The constitutions of these six states guarantee the right to freedom of opinion and expression to their citizens. In none of these states is this right absolute, and the states lay down justifications for the curtailment of the right in their constitutions or other legal documents. Some of the prominent justifications that states provide are national security, friendly relations between states, sedition, defamation, hate speech, blasphemy, public order, obscenity, pornography and related expressions, and gender and sexual expression, among others. These justifications, applied variously in the six states, have a direct and detrimental impact on the right to freedom of opinion and expression, including political expression.

While each of these states is unique in the restrictions it places on online freedom of expression, and the manner in which it applies them, certain common threads run across the region. This chapter studies the commonalities and differences among these states in their criminalisation and restriction of freedom of expression. The first part provides an overview of the six states that are part of *Unshackling Expression*. The second part of this chapter considers commonalities, pointing to trends that run across the six states. Finally, it enumerates some of the divergent trends that distinguish the six states from each other.

Introduction to the six states

This section introduces each of the six states that are part of *Unshackling Expression*, with a focus on the laws affecting online freedom of expression.

Cambodia

The Cambodian constitution guarantees the right to freedom of speech and expression in Article 41, which states: "Khmer citizens shall have freedom to express their ideas." Not only this, but the constitution protects a series of connected rights, such as the rights to political participation and privacy. International human rights law is directly applicable in Cambodia, by way of Article 31 of the constitution.

Cambodia has a growing number of internet users. As of November 2016, its internet penetration stood at 46.4% of the population. The internet has revolutionised news and information consumption in Cambodia. Prior to the advent of the internet, Cambodian media were all state-run or state-affiliated, directly or indirectly, and therefore, all news and information was mediated by the state. However, with the internet, this trend has changed, with individuals and alternative media being able to play a more active, independent role in news and content creation and consumption.

But the state continues to expand its role as gatekeeper, by placing strict and increasing controls on the internet. For instance, while there exist several laws, such as the constitution, the Law on the Press, the Law on Education, etc., which guarantee the right to freedom of opinion and expression to citizens, the government has simultaneously placed strong restrictions through other means. Informal orders of the government and orders from the telecom regulator are used to curb expression online. Offline laws are used to target online speech as well. Political opposition is strongly discouraged through the use of criminalisation. Not only are there laws that target associations and NGOs, political parties and electoral speech, but a cybercrime bill has been proposed which also enables the government to dissolve legal entities (including civil society organisations) on the

grounds that individuals associated with those entities have been accused of cybercrimes. Cambodia primarily uses the justifications of state security, morality and political neutrality, among others, in order to criminalise speech.

India

India's constitution guarantees the right to freedom of expression to all its citizens.¹ Legitimising reasonable restrictions, the constitution provides "interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence" as justifications.² While the constitution makes no reference to the internet or communications, the right has been held as applicable to online speech.³

India has a long history of criminalising speech. The colonially drafted Indian Penal Code criminalises various kinds of expression, and includes offences relating to obscenity, hurting religious sentiments and uttering words to hurt religious feelings (broadly understood as hate speech), defamation and sedition, among others. While the Penal Code also makes no reference to the internet, its sections have been applied to online speech as well. From arrests of WhatsApp group administrators and Facebook users to charges of sedition and defamation, online speech is widely criminalised in India, as the India country report notes.

In addition to the Indian Penal Code, the Information Technology Act, 2000 (as amended in 2008) (IT Act) also includes provisions criminalising online speech. The IT Act targets cyberspace specifically, and includes provisions against obscenity, violation of privacy, etc. Prior to 2015, the IT Act also contained a provision criminalising the sending of messages that are "offensive" or are known to be false but are sent to cause "annoyance, inconvenience, danger, obstruction, insult, injury [...],"⁴ but it was struck down as unconstitutional.⁵

Malaysia

Malaysia has a long history of suppressing freedom of opinion and expression. Article 10 of the Malaysian constitution guarantees to citizens the right to freedom of speech and expression,⁶ with the exceptions being "the interest of the security of the Federation or any part thereof, friendly relations with other countries, public order or morality and restrictions designed to protect the privileges of Parliament or of any Legislative Assembly or to provide against contempt of court, defamation, or incitement to any offence."⁷ In addition to this, Article 149(1) of Malaysia's constitution states that if the country passes a law fearing organised violence or any action disturbing public order, such a law is valid notwithstanding its divergence from Article 10.

Despite the guarantee of freedom of expression, Malaysia criminalises a wide variety of expression, including online speech and expression. The Sedition Act, 1948, for instance, renders certain kinds of speech criminal and seditious, and may result in imprisonment of the speaker. Moreover, the Security Offences (Special Measures) Act, 2012 (SOSMA) criminalises the committing of (and attempt of) activity "detrimental to parliamentary democracy," and the publication and possession of publications detrimental to parliamentary democracy. The procedural sections of the law stipulate that a law enforcement officer can detain an individual for 24 hours under suspicion of offences, and for a further 28 days for the purposes of investigation.

Particularly when it comes to internet speech, Malaysia utilises the provisions of the Communications and Multimedia Act, 1998 (CMA). The CMA has a broad range. For instance, Section 233 criminalises "any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person."⁸ The Malaysia report notes that in the year 2016 alone, over 180 instances of "social media abuse" have been recorded under Section 233.

Myanmar

Myanmar's constitutional history is long and chequered. Its 2008 constitution, in Article 354, guarantees to citizens the right to "express and publish freely their convictions and opinions."⁹

¹ Constitution of India, 1950. Article 19(1). http://lawmin.nic.in/ olwing/coi/coi-english/coi-indexenglish.htm

² Constitution of India, 1950. Article 19(2). http://lawmin.nic.in/ olwing/coi/coi-english/coi-indexenglish.htm

³ Shreya Singhal v. Union of India. AIR 2015 SC 1524.

⁴ Information Technology Act, 2000. Section 66A. http://meity.gov. in/content/information-technology-act-2000

⁵ Shreya Singhal v. Union of India. AIR 2015 SC 1524.

⁶ Federal Constitution of Malaysia. Article 10(1)(a). www.agc.gov.my/ agcportal/uploads/files/Publications/FC/Federal%20Consti%20 (B1%20text).pdf

⁷ Federal Constitution of Malaysia. Article 10(2)(a). www.agc. gov.my/agcportal/uploads/files/Publications/FC/Federal%20 Consti%20(Bl%20text).pdf

⁸ Communications and Multimedia Act, 1998. Section 233. www.unodc.org/res/cld/document/mys/communications_ and_multimedia_act_html/Malaysia_Communications_and_ Multimedia_Act_1998.pdf

⁹ Constitution of the Republic of the Union of Myanmar, 2008. Article 354. http://www.burmalibrary.org/docs5/Myanmar_Constitution-2008-en.pdf

Despite the guarantee of this right, the government reserves the right to restrict freedom of expression on grounds of "Union security, prevalence of law and order, community peace and tranquility or public order and morality."¹⁰ These restrictions (including the creation of criminal offences) have been exercised through the use of laws, such as the Myanmar Penal Code, the Computer Science Development Law, Electronic Transactions Law, Telecommunications Law, etc.

The Myanmar Penal Code, like that of India, is a colonial legislation. Enacted in 1860, it includes offences relating to obscenity, outraging religious feelings, and defamation, among others. While the Penal Code makes no mention of the internet, there is nothing to suggest that the Penal Code cannot be used to target online speech. However, it is the Electronic Transactions Law and the Telecommunications Law that have been most commonly used against online speech in Myanmar. Section 66(d) of the Telecommunications Law criminalises "lelxtorting, coercing, restraining wrongfully, defaming, disturbing, causing undue influence or threatening to any person by using any Telecommunications Network."¹¹ The Electronic Transactions Law, for its part, criminalises any act that is "detrimental to the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture," for which the punishment is a jail term of five to seven years.12 Myanmar does, in fact, utilise these provisions to criminalise online speech; as the Myanmar report notes, there have been over 73 cases in the span of one year alone.

Pakistan

In Pakistan, the distrust of electronic media and the internet is glaringly obvious. As the Pakistan report shows, the state authorities have made it clear that social media has a detrimental influence on the cultural and religious values of the country, and that they intend to crack down on such influences. Towards this end, Pakistan employs a structured network of laws to criminalise and, more broadly, restrict freedom of speech and expression.

Pakistan guarantees freedom of speech and expression through Article 19 of its constitution.¹³ The

article also lays down the grounds on which the right can be restricted: "the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, [commission of] or incitement to an offence." As the Pakistan report notes, these justifications have been enabled through laws in the country.

The Pakistan Penal Code is one such law, which criminalises speech and expression, among other offences. Blasphemy is a major provision by way of which speech, including and particularly online speech, is criminalised in Pakistan. As the Pakistan report notes, there is a "well-developed body of case law focused on the online space" relating to blasphemy. On the ground of blasphemy, YouTube has been banned, bloggers have disappeared, and vigilante murders have occurred. The Prevention of Electronic Crimes Act, 2016, is another legislation that is used to criminalise online expression in Pakistan. Several sections, detailing offences and in some cases, heavier penalties than for offline offences, address online speech and expression. These provisions include hate speech, blasphemy, defamation, etc. In addition to blasphemy, national security, contempt of court and sedition, among others, have been frequently used in Pakistan against online speech. A crucial divergence in Pakistan is the mob justice that is meted out against "offensive" religious speech, though we see similarities to this in India as well.

Thailand

Thailand's constitution of 2017 guarantees the right to freedom of opinion and expression under Section 34. Section 34 reads: "A person shall enjoy the liberty to express opinions, make speeches, write, print, publicise and express by other means," and expressly protects academic freedom. However, the right is not absolute, and may be curtailed on grounds of "maintaining the security of the State, protecting the rights or liberties of other persons, maintaining public order or good morals, or protecting the health of the people."¹⁴

Following the military coup of 22 May 2014, Thailand has been ruled by the National Council for Peace and Order (NCPO). The NCPO controls expression in Thailand through a series of laws, including the Penal Code and the Head of NCPO Announcements. Lèse majesté is a crucial wing of the NCPO's control

¹⁰ Ibid.

¹¹ Telecommunications Law. Section 66(d). www.burmalibrary.org/ docs23/2013-10-08-Telecommunications_Law-en.pdf.

¹² The Electronic Transactions Law. Section 33(a). www.burmalibrary. org/docs15/2004-SPDC_Law2004-05-Electronic_Transactions_ Law-en.pdf

¹³ Constitution of the Islamic Republic of Pakistan. Article 19. https:// pakistanconstitutionlaw.com/article-19-freedom-of-speech-etc

^{14.} Constitution of the Kingdom of Thailand. Section 34. www.constitutionnet.org/sites/default/files/2017-05/ CONSTITUTION%2BOF%2BTHE%2BKINGDOM%2BO F%2BTHAILAND%2B%28B.E.%2B2560%2B%282017%29%29.pdf

over online expression in Thailand.¹⁵ Even peaceful or humorous expression of opinion concerning the royalty is charged with lèse majesté, under Section 112 of the Penal Code. As the Thailand report notes, over a three-year period, over 90 people have been arrested on grounds of lèse majesté.

In addition to lèse majesté, Thailand uses Section 116 of the Thai Penal Code to criminalise seditious express. Section 116 criminalises acts or expressions that seek to use force or violence to "bring about a change in the Laws of the Country or the Government," or to raise unrest and disaffection among people to cause disturbance.¹⁶ Sedition charges have been filed against multiple people even without the presence of force or violence. While both these sections of the Thai Penal Code make no mention of the internet, they have been used to punish online expression. The Computer Crimes Act, 2007 specifically targets online activities. The Thai control over the internet and online activities is strong, and the many arrests and convictions stand witness to this.

Following this introduction of the six states, the next section considers the common trends among the states where the criminalisation of online freedom of opinion and expression is concerned.

Common trends among states in Unshackling Expression

Among the six states that are part of *Unshackling Expression*, there are some commonalities. All these states either have laws that target cyberspace specifically (along with legal provisions that affect online speech), or they are moving towards such a law. All of these states also utilise offline laws to criminalise and punish online speech. Most of them also utilise multiple legal provisions to target and criminalise a single instance of online speech. They also prescribe harsher punishments for online "offences" than for offline speech.

Towards cyber-specific laws

It is a trend that can be seen across Asia that states are adopting laws that target cyberspace specifically. These laws not only describe the way in which the internet and electronic transactions are to be conducted, but they also create online offences and prescribe punishments. Many of these offences target online freedom of opinion and expression, and are relevant to our discussion.

15 Thai Penal Code. Section 112. https://www.thailandlawonline.com/ laws-in-thailand/thailand-criminal-law-text-translation#chapter-2

16 Thai Penal Code. Section 116. https://www.thailandlawonline.com/ laws-in-thailand/thailand-criminal-law-text-translation#chapter-2

Cambodia, for instance, has a cybercrime bill which has not yet been signed into law. Malware attacks in Cambodia have lent a sense of urgency to the need for a cybercrime law, with the private sector in the country pushing for the same.¹⁷ While the law has not yet been passed, several provisions of the bill have proved troubling for freedom of opinion and expression. For instance, as noted in the Cambodia report, the first draft of the law contained an article that outlawed content that could be "deemed damaging to the moral and cultural values of the society," including "manipulation, defamation, and slanders." In addition to the cybercrime bill, the Law on Telecommunications governs online and networked spaces in Cambodia. The law, while outlawing any use of telecommunications networks which may result in "national insecurity", also prescribes heavier penalties for Criminal Code offences.

India has had a cyber legislation since the year 2000. The Information Technology Act, 2000 (as amended in 2008) (IT Act) specifically targets cyberspace. In addition to setting up a Computer Emergency Response Team, a Cyber Appellate Tribunal, a National Critical Infrastructure Protection Authority, etc., and setting out encryption standards, digital and electronic signatures, etc., the IT Act also sets out a series of offences and prescribes punishments. Several of these sections affect online speech, including provisions on the violation of privacy, pornographic material (characterised as obscenity), etc.

In Malaysia, the Communications and Multimedia Act, 1998 (CMA) targets the internet. As the Malaysia report shows, the CMA sets out offences that affect online speech – the most notable being Section 233. Section 233 criminalises any online expression that is "obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person."

The Telecommunications Law and Electronic Transactions Law affect the internet in Myanmar. Article 66(d) of the Telecommunications Law, and Articles 33 and 34 of the Electronic Transactions Law, directly impact online speech.

In Pakistan, the Prevention of Electronic Crimes Act, 2016 (PECA) targets online speech. Section 34 of the PECA grants the Pakistan Telecommunication Authority the power to block or remove "unlawful online content", while several other provisions in Chapter II of the law outline offences and punishments. Hate speech, the glorification of an offence, false information that harms the privacy or reputation of an individual, etc. are all criminalised.

¹⁷ Vannak, C. (2017, 3 July). Cybercrime law on the way. *Khmer Times*. www.khmertimeskh.com/news/39866/cybercrime-law-on-the-way

The Computer Crimes Act, 2007 (CCA) is the law targeting the online space in Thailand. The Thailand report notes that, along with the Penal Code, the CCA is used to suppress and criminalise online expression. Section 14, which involves forged or false computer data, has been most used to criminalise online speech, including in cases involving defamation.

Offline laws used to criminalise online speech

Across Asia, states use offline laws to target and criminalise online speech and expression. The Penal Codes are most commonly used towards this end. The Indian Penal Code, the Malaysian Penal Code, the Myanmar Penal Code and the Pakistan Penal Code, remnants of the colonial era, are similar in content and structure. They codify offences against the state (for instance, sedition), hate speech (outraging religious feelings or blasphemy in Pakistan), obscenity and defamation. These are applied online as and when considered convenient, and individuals are arrested on the grounds of the above offences. While some states, such as Myanmar, have provisions against defamation codified in an internet-specific law,18 the offline laws are also used to target online speech in most states.

Section 305 of the Cambodian Criminal Code targets defamation both offline and online, while also criminalising incitement to commit a crime (Article 495) and incitement to commit discrimination (Article 496). In Cambodia, it is not only the right to freedom of speech that suffers at the hands of these provisions, but also the right to political participation. In India, Section 124A of the Indian Penal Code (IPC), the provision for sedition, is utilised to target online speech as well, as is Section 500, IPC, the provision on defamation. Sections 153A and 295A, IPC, the provisions concerning promoting enmity between groups on grounds of religion, etc., and outraging religious feelings, are also used against online speech and expression.

Malaysia routinely uses provisions of the Sedition Act, 1948, and Sections 499 and 500 of the Malaysian Penal Code, in conjunction with Section 233 of the Communications and Multimedia Act, to criminalise online expression. Malaysia also applies Section 298 ("Uttering words, etc., with deliberate intent to wound the religious feelings of any person") of the Malaysian Penal Code to online speech. The same is true for Myanmar, where Section 295A (outraging religious feelings) is applied both offline and online, as is Section 124A (sedition). In addition to Section 10A of the Prevention of Electronic Crimes Act, 2016 (hate speech), Pakistan also applies the blasphemy provisions in the Penal Code to online speech and expression. Similarly, Thailand applies Penal Code Sections 112 (lèse majesté) and 116 (an offence against internal security) to both offline and online speech.

Multiple legal provisions to target a single "offence"

Case studies show that all the six states utilise multiple legal provisions to charge a single instance of online speech. In India, for example, Section 295A of the IPC (which criminalises acts or expression that outrages religious feelings) is often clubbed with Section 153A, IPC (promoting enmity between groups on grounds of religion, etc.), and when Section 66A of the IT Act was on the books, it was clubbed with that provision as well. In Malaysia, in instances involving sedition, the Malaysia report notes that individuals are often simultaneously booked under the Sedition Act, 1948 as well as the Communications and Multimedia Act, 1998.

In Myanmar, Section 34(d) of the Electronic Transactions Law ("creating, modifying or altering of information or distributing of information [...] to be detrimental to the interest of or to lower the dignity of any organization or any person") is clubbed with Section 66(d) of the Telecommunications Law ("Extorting, coercing, restraining wrongfully, defaming," etc., using a telecommunications network), as well as Section 500 of the Myanmar Penal Code (defamation). In Pakistan as well, charges under the PECA are often clubbed with charges under the Pakistan Penal Code. In Thailand, while the Computer Crimes Act, 2007 makes no direct reference to defamation, the Thailand report notes that defamation under the Thai Penal Code has often been clubbed with Section 14(1) of the CCA.

The effect of this clubbing is two-fold. *First*, an individual may be found guilty on one count, while acquitted on another. So this raises the chances of the individual's conviction for an instance of speech and expression. *Second*, as the case studies from Thailand make clear, the clubbing of provisions also means that a higher punishment, combined on the basis of multiple charges, may be ordered on the individual.

Harsher punishments for online offences

The states that form part of this study have been found to grant harsher punishments for online offences than for their offline counterparts in some cases. Table 1 gives a bird's eye view of some offences in which the online penalties are higher.

¹⁸ Telecommunications Law. Article 66(d).

TABLE 1. PENALTIES FOR OFFLINE AND ONLINE OFFENCES					
Country	Offline legal provision	Offline penalty	Online legal provision	Online penalty	
India	Section 292, Indian Penal Code: Sale, etc. of obscene books	On first conviction with imprisonment of either description for a term which may extend to <i>two years</i> , and with fine which may extend to <i>two thousand rupees</i> , and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to <i>five thousand</i> <i>rupees</i> .	Section 67, Information Technology Act, 2000: Punishment for publishing or transmitting obscene material in electronic form	On first conviction with imprisonment of either description for a term which may extend to <i>three years</i> , and with fine which may extend to <i>five lakh* rupees</i> , and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to <i>ten lakh</i> <i>rupees</i> .	
Myanmar	Section 500, Myanmar Penal Code: Defamation	Simple imprisonment for a term which may extend to <i>two years</i> , or with fine, or with both	Section 66(d), Telecommunications Law: Whoever commits any of the following acts shall, on conviction, be liable to imprisonment for a term not exceeding three years or to a fine or to both. (d) Extorting, coercing, restraining wrongfully, defaming, disturbing, causing undue influence or threatening to any person by using any Telecommunications Network.	Imprisonment for a term not exceeding <i>three years</i> or to a fine or to both	
Pakistan	Section 298, Pakistan Penal Code: Uttering words, etc., with deliberate intent to wound religious feelings Section 298A, Pakistan	Imprisonment of either description for a term which may extend to <i>one year</i> or with fine, or with both. Imprisonment of either description for a term which	Section 10A, Prevention of Electronic Crimes Act, 2016: Hate speech Section 10A, Prevention of	Imprisonment of either description for a term which may extend to <i>seven years</i> or with fine, or with both. Imprisonment of either	
	Penal Code: Use of derogatory remarks, etc., in respect of holy personages	may extend to <i>three years</i> , or with fine, or with both.	Electronic Crimes Act, 2016: Hate speech	description for a term which may extend to <i>seven years</i> or with fine, or with both.	
Thailand	Section 305, Thai Penal Code: Defamation	Imprisonment not exceeding one year or fined not exceeding twenty thousand Baht, or both.	Section 14(1), Computer Crimes Act, 2007: Whoever commits the following acts shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or both: (1) input into a computer system wholly or partially fake or false computer data that is likely to cause damage to another person or the public	Imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both	

Divergences among the six states

As we saw in the previous section, there exist several common trends among the six states across Asia. However, there are several divergent trends among the six states as well. First, each state uses a unique combination of legal provisions to target online speech; that is, each state has a certain set of provisions that it uses most commonly to criminalise online speech, but these provisions differ across the states. Second, the definitions of different provisions, while similar, differ across the states; the example of defamation will be used to show such differences. Third, the punishments given to offences differ across the states; the example of hate speech and blasphemy, as well as defamation, will be used to illustrate this.

Unique combinations of legal provisions

While similar provisions exist across the countries, each state is unique in its choice of go-to provisions to target online speech. No two states use the exact same provisions to commonly and widely target online speech. While they have in common the provisions themselves, in practice, they each have different go-to legal provisions to best control online expression in each of their territories.

Prior to 2015, India made extensive use of Section 66A, Information Technology Act, 2000 (as amended in 2008).¹⁹ Section 66A criminalised the sending of "offensive messages" through the internet, and stated that the sending of false messages that cause "annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will" would be penalised with a jail term extending to three years and with a fine. However, Section 66A was struck down by the Supreme Court of India as unconstitutional, as it violated unreasonably the freedom of expression of citizens.²⁰ Following this, there has been an increase in the use of Section 295A, Indian Penal Code (the hate speech provision).²¹ One of the most notable cases of the use of this provision involved the arrests of Shaheen Dada, who posted a Facebook post critical of a state bandh or shutdown (it was instituted due to the death of a prominent politician), and Renu

Srinivasan, who liked the said post. In addition to these provisions, India also liberally uses other provisions to target online speech, such as defamation and provisions from both the Indian Penal Code and the IT Act. India is, in that sense, an outlier.

Cambodia is also an outlier. While Cambodia has multiple provisions criminalising speech, the country utilises them to exemplify the consequences of breaking the law. For instance, in the case concerning the assassination of Kem Ley, several individuals were arrested on charges of defamation under the Cambodian Criminal Code for insinuating government ties to the assassination, as will be seen in the Cambodia report. Similarly, Articles 495 and 496 of the Cambodian Criminal Code (incitement to commit a crime and incitement to commit discrimination) have often been used to criminalise Facebook comments.

Malaysia focuses on the use of Section 233 of the Communications and Multimedia Act, 1998, to criminalise online speech. As the Malaysia report notes, over 180 cases have been registered in 2016 alone, and "[o]ffences that have surfaced under this law include lèse majesté, alleged fake news, satire, graphics that are perceived as insulting the prime minister, and a wide variety of other 'affronts'."

In Myanmar, the largest number of cases have been reported under Section 66(d) of the Telecommunications Law. Section 66(d) criminalises the "[e]xtorting, coercing, restraining wrongfully, defaming, disturbing, causing undue influence or threatening to any person by using any Telecommunications Network," with a jail term of two years, or with a fine, or with both. As the Myanmar report notes, over 90 cases have been registered under Section 66(d) alone, concerning online speech.

Pakistan, on the other hand, relies on its blasphemy laws to target online speech and expression. It has acted in a variety of ways, from criminalising blasphemous speech with imprisonment for life, to blocking content considered to be blasphemous under the Prevention of Electronic Crimes Act, 2016.²² For instance, as the Pakistan report notes, a death sentence was once awarded to a man who sent a poem considered blasphemous over WhatsApp.

In Thailand, lèse majesté is the provision of choice when targeting online speech. The provision, Section 112 of the Thai Penal Code, criminalises anyone who "defames, insults, or threatens the King, the Queen, the Heir-apparent, or the Regent," with a punishment of three to 15 years of imprisonment. Most cases in recent years concerned posts and messages on Facebook.

¹⁹ Information Technology Act, 2000. Section 66A. http://meity.gov. in/content/information-technology-act-2000.

²⁰ Shreya Singhal v. Union of India, AIR 2015 SC 1524

²¹ Indian Penal Code, 1860. Section 295A: "Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs.- Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of [citizens of India], [by words, either spoken or written, or by signs or by visible representations or otherwise], insults or attempts to insult the religiour or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to [three years], or with fine, or with both." www.lawmin.nic.in/ld/P-ACT/1860/186045.pdf

²² Prevention of Electronic Crimes Act, 2016. Section 34. http://www. na.gov.pk/uploads/documents/1470910659_707.pdf

TABLE 2. DEF	INITIONS OF DEFAMATION IN THE SIX STATES		
Country	Definition		
Cambodia	Article 305, Cambodian Criminal Code: Any allegation or charge made in bad faith which tends to injure the honour or reputation of a person or an institution.		
India	 Section 499, Indian Penal Code: Defamation Whoever, by words either spoken or intended to be read, or by signs or by visible representations makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person. Explanation 1 It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives. Explanation 2 It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such. Explanation 3 An imputation in the form of an alternative or expressed ironically, may amount to defamation. Explanation 4 No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsom state, or in a state generally considered as disgraceful. 		
Malaysia	 Section 499, Malaysia Penal Code: Whoever, by words either spoken or intended to be read or by signs, or by visible representations, makes or publishes any imputation concerning any person, intending to harm, or knowing or having reason to believe that such imputation will harm the reputation and shall also be liable to fine of such person, is said, except in the cases hereinafter excepted, to defame that person. Explanation 1 – It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives. Explanation 2 – It may amount to defamation to make an imputation concerning a company, or an association or collection of persons as such. Explanation 3 – An imputation in the form of an alternative, or expressed ironically, may amount to defamation. Explanation 4 – No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful. 		
Myanmar	 Article 499, Myanmar Penal Code: Defamation Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person. Explanation 1 It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives. Explanation 2 It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such. Explanation 3 An imputation in the form of an alternative or expressed ironically, may amount to defamation. Explanation 4 No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful. 		

TABLE 2. DEF	INITIONS OF DEFAMATION IN THE SIX STATES
Country	Definition
Pakistan	 Section 499, Pakistan Penal Code: Whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person. Explanation 1 It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives. Explanation 2 It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such. Explanation 3 An imputation in the form of an alternative or expressed ironically, may amount to defamation. Explanation 4 No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful.
	 (1) Any wrongful act or publication or circulation of a false statement or representation made orally or in written or visual form which injures the reputation of a person, tends to lower him in the estimation of others or tends to reduce him to ridicule, unjust criticism, dislike, contempt or hatred shall be actionable as defamation. (2) Defamation is of two forms, namely:- (i) Slander; and (ii) Libel. (3) Any false oral statement or representation that amounts to defamation shall be actionable as slander. (4) Any false written, documentary or visual statement or representation made either by ordinary form or expression or by electronic or other modern means of devices that amounts to defamation shall be actionable as slander.
Thailand	 Section 326, Thai Penal Code: Whoever, imputes anything to the other person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to be hated or scorned, is said to commit defamation, and shall be punished with imprisonment not exceeding one year or fined not exceeding twenty thousand Baht, or both. Section 329, Thai Penal Code: Whoever, in good faith, expresses any opinion or statement: By way of self justification or defense, or for the protection of a legitimate interest; In the status of being an official in the exercise of his functions; By way of fair comment on any person or thing subjected to public criticism; or By way of fair report of the open proceeding of any Court or meeting, shall not be guilty of defamation.

Definitions of offences differ across states

While the six states share commonalities in their criminalisation of speech and expression, the way in which the offences are understood in these states differs. For instance, the ways in which defamation is understood in the six states is illustrated in Table 2.

At a glance, it is clear that the definitions of defamation in India, Malaysia, Myanmar and Pakistan are the same. Their common colonial past throws light on this. In these countries, defamation is defined on the basis of four factors: (1) there must be a publication or speech of an imputation; (2) there must be intent, knowledge or reason to believe that such imputation will harm the reputation of the subject of the imputation; (3) the imputation must lower "the moral or intellectual character of that person"; and (4) such a lowering of character must occur in the estimation of others. It should be noted that there is no requirement of bad faith in making the imputation. There are also general defences, of truth, opinion in good faith under certain circumstances, or the public good.

However, the definitions of defamation in Cambodia and Thailand are markedly different. In

TABLE 3. PEI	TABLE 3. PENALTIES FOR HATE SPEECH AND BLASPHEMY				
Country	Offline penalties	Online penalties			
Cambodia	Article 516, Criminal Code: Insult of Buddhist monks, nuns and laymen: Imprisonment from one day to six days and a fine from one thousand to one hundred thousand Riels.	No online counterpart.			
India	Section 295A, Indian Penal Code: Imprisonment of three years, or with fine, or with both. Section 298, Indian Penal Code: Imprisonment of one year, or with fine, or with both.	No online counterpart. Offline law used to charge online offences.			
Malaysia	Section 298, Malaysia Penal Code: Imprisonment of one year, or with fine, or with both. Section 298A, Malaysia Penal Code: Imprisonment for a term of not less than two years and not more than five years.	No online counterpart. Offline law used to charge online offences.			
Myanmar	Section 295A, Myanmar Penal Code: Imprisonment of either description for a term which may extend to two years, or with fine, or with both. Section 298, Myanmar Penal Code: Imprisonment of either description for a term which may be extend to one year, or with fine, or with both.	No online counterpart.			
Pakistan	Section 295A, Pakistan Penal Code: Imprisonment of 10 years, or with fine, or with both. Section 295C, Pakistan Penal Code: Death, or imprisonment for life, and with fine. Section 298, Pakistan Penal Code: Imprisonment of either description for a term which may extend to one year, or with fine, or with both. Section 298A, Pakistan Penal Code: Imprisonment of three years, or with fine, or with both.	Section 10A, Prevention of Electronic Crimes Act, 2016: Imprisonment for a term which may extend to seven years, or with fine, or with both.			
Thailand	landArticle 44, Sangha Act 1962: Fine of not more than five thousand Baht or an imprisonment of not more than one year or both. Section 206, Criminal Code: Imprisoned as from two years to seven years or fined as from two thousand Baht to fourteen thousand Baht, or both. Section 207, Criminal Code: Imprisonment not exceeding one year or fined not exceeding two thousand Baht, or both.No online counterpart.				

Cambodia, the requirements are far less: (1) there must be an allegation or charge, (2) the allegation or charge must be made in bad faith, and (3) the allegation or charge must tend to injure the honour or reputation of the natural or juristic person. There are no exceptions as to truth, holding an opinion, or public good. In Thailand, (1) there must be an imputation made to a subject, (2) the imputation must be made before a third party, and (3) the imputation must be likely to damage the reputation of the subject of the imputation. Thailand is different from Cambodia in that there is no need for bad faith in making the imputation, and moreover, Thailand also creates the exception of good faith imputations to the crime of defamation.

Punishments for offences differ across states

While the six states share similar laws and provisions, they differ, if but slightly, in the way they punish these offences. For instance, in the case of hate speech, each state offers different punishments (imprisonment as well as fine). As can be expected, Pakistan offers the greatest punishment, from 10 years to life imprisonment. Cambodia offers the least punishment, with imprisonment of only days, but with a large fine. In the case of defamation, however, while Cambodia prescribes a maximum of ten million Riels as punishment, in Thailand, an individual may be imprisoned for five years. The penalties for these offences in the six states are compared in Tables 3 and 4.

Country	Offline penalties	Online penalties
Cambodia	Article 305, Cambodian Criminal Code: Defamation shall be punishable by a fine from one hundred thousand to ten million Riels if it is committed by any of the following means: (1) any words whatsoever uttered in a public place or in a public meeting; (2) written documents or pictures of any type released or displayed to the public; (3) any audio-visual communication intended for the public.Same as for offline offence	
India	Section 500, Indian Penal Code: Simple imprisonment for a term which may extend to two years, or with fine, or with both.	Same as for offline offence.
Malaysia	Section 500, Malaysian Penal Code: Imprisonment for a term which may extend to <i>two years</i> or with fine or with both.	Section 233, Communications and Multimedia Act, 1998: Shall be liable to a fine not exceeding <i>fifty</i> <i>thousand ringgit</i> or to imprisonment for a term not exceeding <i>one year</i> or to both and shall also be liable to a further fine of one thousand ringgit for every day during which the offence is continued after conviction.
Myanmar	Section 500, Myanmar Penal Code: Simple imprisonment for a term which may extend to <i>two years</i> , or with fine, or with both.	Section 66(d), Telecommunications Law: Imprisonment for a term not exceeding <i>three years</i> or to a fine or to both
Pakistan	Section 500, Pakistan Penal Code: Imprisonment for a term which may extend to <i>two years</i> , or with fine, or with both.	Section 18, Prevention of Electronic Crimes Act, 2016: Imprisonment for a term which may extend to <i>three years</i> or with fine which may extend to <i>one million rupees</i> or with both.
Thailand	Article 326, Thai Penal Code: Imprisonment not exceeding <i>one year</i> or fined not exceeding <i>twenty thousand Baht</i> , or both.	Section 14(1), Computer-related Crimes Act, 2007: Imprisonment for not more than <i>five years</i> or a fine of not more than <i>one hundred thousand baht</i> or both.

intimidates or harms the reputation or privacy of a natural person [...]." www.na.gov.pk/uploads/documents/1470910659_707.pdf

Conclusion

As APC's joint written statement to the Human Rights Council at its 35th session²³ notes, states in Asia are moving towards repressive regimes where online freedoms are concerned. Although freedom of expression is guaranteed in the constitutions of Asian states, including the six that are part of this report, states liberally use legal justifications to curtail and also to criminalise online speech. Some states, such as Cambodia, also use informal means to repress freedoms, and create high-profile cases to serve as deterrents against political expression and opposition. Not only political expression, but artistic expression also suffers in the first instance. In states like India, laws on obscenity affect educational and artistic expression in practice. Although the law may say otherwise, the very fact of arrest and charging for the offence itself constitutes harassment and punishment. Furthermore, expressions of wit and humour that touch upon religion are affected in states like Pakistan and Malaysia, where laws on blasphemy and outraging religious feelings severely restrict the scope of expression. The following reports show the state of online freedom of expression in their respective countries.

²³ Association for Progressive Communications. (2017). Joint written statement submitted by Association for Progressive Communications (APC), non-governmental organizations in general consultative status. https://www.apc.org/sites/default/ files/2570_A_HRC_35_NGO_Sub_En.pdf

Mapping the criminalisation of online expression: Cambodia

Anonymous

Introduction

The internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies.

Frank La Rue, former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, May 2011.¹

The number of internet users in the Kingdom of Cambodia is growing exponentially. Reports from the Ministry of Posts and Telecommunications (MPTC) show that internet subscriptions have increased from only 43,417 in 2008 to 6,984,709 in June 2016. In November 2016, internet penetration stood at 46.4% with 7.25 million subscribers.² The internet has now surpassed all other forms of media as a source of news in Cambodia.

The internet is changing the information landscape by creating an alternative to the classical model of state and state affiliate-run news outlets. In 2015, Cambodia's Media Ownership Monitor found that the majority of traditional media (TV stations, radio stations and newspapers) were affiliated with the ruling Cambodian People's Party (CPP). It reported that of the 27 Cambodian media owners, 11 were on the government payroll, advisors to the government, or affiliated to a political

1 La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/17/27. daccess-ods.un.org/ access.nsf/Get?Open&DS=A/HRC/17/27&Lang=E party.³ Even among news outlets without any overt link to the ruling CPP, self-censorship is rife, with many news outlets reluctant to publish information that may be overly critical of the government. While small numbers of independent radio stations and English-language newspapers were generally tolerated since the end of the Cambodian civil war in 1991, an unprecedented August 2017 crackdown against independent media led to the silencing of most independent traditional media in Cambodia, with 32 broadcasts reportedly shuttered.⁴ The crackdown also extended to the shutdown of the *Cambodia Daily* newspaper, a publication renowned internationally for its critical investigative reporting.⁵

Due to the dominance of the Royal Government of Cambodia (RGC) in the traditional media, the Cambodian people have increasingly turned to the internet and social media (in particular Facebook) to gather and exchange information and opinions. In February 2017, Noun Vansuy of the Cambodian Center for Independent Media stated, "If people are able to use social media properly, they are unknowingly contributing to promote access to information and freedom of expression."⁶

The rise of the internet in Cambodia has also provided an unprecedented space for open political discussion and criticism of the RGC. Online expression has become a popular means of social advocacy, especially among activists and human rights defenders. During the 2013 National Assembly election, social media was used by the recently

² Khothara, H. (2016). Workshop on Economic Aspects of Spectrum Management. Ministry of Post and Telecommunications of Cambodia (MPTC), Tehran, Iran, 21-23 November. www.itu.int/en/ ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/ Nov-SM-Economics/Presentations/Day%202%20-%20 Session%204%20(Cambodia).pdf

³ mom-kh.com/en/pages/affiliations

⁴ LICADHO. (2017, 9 September). Restricting Critical Voices on Cambodian Airwaves. *LICADHO*. www.licadho-cambodia.org/ articles/20170909/148/index.html

⁵ The Cambodia Daily. (2017, 4 September). Cambodia Daily Announces Immediate Closure Amid Threats. The Cambodia Daily. www.cambodiadaily.com/topstory/cambodia-daily-announcesimmediate-closure-amid-threats-134283

⁶ Cambodian Center for Independent Media. (2017, 24 February). Smartphone and Internet: Weapon of Choice for Young Citizen Journaliss. CCIM. www.ccimcambodia.org/what-we-do/citizenjournalism/155-smartphone-and-internet-weapon-of-choice-foryoung-citizen-journalists

merged opposition Cambodia National Rescue Party (CNRP) as a tool to challenge the CPP-dominated media and to promote the party's platform in that election. This led to a historic result for the opposition CNRP, which came within a few seats of winning an unprecedented majority. Online networking also facilitated unprecedented anti-government protests following the election, as the opposition alleged electoral fraud. These protests merged with enormous garment worker demonstrations. This resulted in some of the biggest anti-government protests Cambodia has ever seen, which were organised and popularised primarily online. The year-long protests – based on accusations of electoral fraud, which allegedly denied the CNRP an outright victory - were violently suppressed in January 2014, resulting in numerous deaths and one enforced disappearance after security forces opened fire on demonstrators and passers-by.7

Since then, there has been a string of arrests, charges and convictions resulting from critical posts written on Facebook. For instance, political activists and ordinary people have been convicted for incitement, defamation and similar speech-related criminal offences. It is in this deteriorating climate for freedom of expression that Kem Ley, a much-loved political commentator known for his criticism of the ruling CPP, was murdered in July 2016. Observers have pointed to a potential political motivation for the assassination, while local and international organisations have slammed the ineffective investigation into the alleged perpetrators.8 Several individuals who have dared to publicly link the assassination to the ruling party through Facebook posts have been prosecuted for defamation and related offences.

The criminalisation of individuals who speak out on social media is likely to increase as the legal framework tightens around the freedom of expression and the 2018 election draws closer. The space for freedom of expression was already not up to international standards, but recent legislative developments such as the Law on Telecommunications adopted in 2015 have acted to further restrict this space. The situation is likely to deteriorate even further if the draft Cybercrime Law currently under consideration is passed. These legislative developments have been accompanied by an increase in the numbers of arbitrary judicial actions taken against individuals for expressing themselves online. Moreover, with a pivotal national election coming in July 2018, the RGC is multiplying its attempts to extend control over individuals with respect to the exercise of their freedom of expression online. At the beginning of August 2017, the National Police announced they were monitoring Facebook to detect and prevent "rebel movements" of "the enemy".⁹ Under such surveillance, it is easily conceivable that people feel ever less comfortable freely expressing themselves online, leading to self-censorship out of fear of the government's reprisals.¹⁰

Methodology

Cambodian laws, policies, reports and other official documents were the primary data sources for this report. Expert analysis of the content of these documents, through a desk review process, was used to assess the degree to which legal guarantees are in place to ensure the freedom of expression online. The documents were primarily located from Cambodia's Royal Gazette – a weekly government-issued publication, which is supposed to contain all new primary and secondary laws.

An initial review of the Constitution of the Kingdom of Cambodia (the Constitution), Criminal Code, Civil Code, Code of Criminal Procedure and Code of Civil Procedure was added to by consulting Cambodian legal experts regarding the identification of other legislation which impacts upon freedom of expression online. Finally, case studies were selected by drawing upon an existing database of relevant case law, which is maintained by a Cambodian human rights organisation.

Lay of the legal land

Legal foundations and fundamental laws and freedoms

Domestic law

Constitution of Cambodia

The Constitution explicitly protects the right to freedom of expression and related rights. However, it should be noted that these protections fail to meet international standards because they

⁷ Freedom House. (2014). Freedom on the Net 2014. https:// freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_ compressedv2_0.pdf

⁸ Human Rights Watch and others. (2017, 7 July). Joint Letter on Investigation Into Killing of Kem Ley: Request for Cambodian Government to Create a Commission of Inquiry. Human Rights Watch. https://www.hrw.org/news/2017/07/07/ joint-letter-investigation-killing-kem-ley

⁹ Handley, E. (2017, 1 August). Government's 'chilling effect' on free speech. The Phnom Penh Post. www.phnompenhpost.com/ national/governments-chilling-effect-free-speech

¹⁰ Vida, T. (2015, 8 September). Monitoring the Internet. The Phnom Penh Post. www.phnompenhpost.com/national/ monitoring-Internet

explicitly extend only to "Khmer citizens" rather than all individuals subject to the jurisdiction of Cambodian law. For example, Article 41 states that "Khmer citizens shall have freedom of expression of their ideas."¹¹

Article 80 guarantees the right to freedom of expression of members of the National Assembly. It states: "No assembly member shall be prosecuted, detained or arrested because of opinions expressed during the exercise of his (her) duty."

The Constitution also safeguards freedom of expression by guaranteeing closely related rights. Article 35 promotes an environment in which citizens are empowered to exercise their right to freedom of expression and involve themselves in public affairs. It states: "Khmer citizens of either sex shall have the right to participate actively in the political, economic, social and cultural life of the nation. All requests from citizens shall be thoroughly considered and resolved by institutions of the state."

Article 39 ensures the right to denounce public officials for a breach of the law committed during the course of their duties. It states: "Khmer citizens have the right to denounce, make complaints, or claim for compensation for damages caused by any breach of the law by institutions of the states, social organizations or by members of such organizations."

Article 40 of the Cambodian Constitution confers upon citizens the "right to privacy of residence, and to the secrecy of correspondence by mail, telegram, fax, telex and telephone." As the Constitution was drafted at the beginning of the 1990s, no reference to the internet or ICT was included.¹²

Law on the Press (Press Law)

At first glance, the Press Law seems to take a relatively liberal and protective approach to freedom of expression.

Article 1 provides: "This law determines the regime of the press and assures freedom of the press and freedom of publication in conformity with article 31 and 41 of the Constitution of the Kingdom of Cambodia."¹³ Article 3 provides for the right to freedom from pre-publication censorship: "To maintain the independence of the press, pre-publication censorship shall be prohibited."

According to Article 4, "[t]he publication of official information such as statements, meetings, meeting minutes or reports, etc. may not be penalized if such publication is fully true or an accurate summary of the truth."

Finally, in its Article 20, the Press Law provides that no person shall face criminal liability for the expression of opinion: "Any act committed by an employer, editor or author of a text which violates the criminal law shall be punished according to the criminal law. No person shall be arrested or subject to criminal charges as the result of the expression of opinions."

Nevertheless, the Press Law also contains broad restrictions and obligations intended to regulate or to control the press. Freedom of expression may be endangered. See the section on sectoral laws for more detail.

Law on the Election of Members of the National Assembly (LEMNA)

The importance of human rights in the context of elections is recognised by the LEMNA. Article 73 provides: "During the electioral campaign period and on polling day all political parties and candidates, members and supporters of political parties [...] shall respect the principles of human rights and democracy enshrined in the Constitution of the Kingdom of Cambodia."¹⁴

The LEMNA also contains numerous restrictions on freedom of expression that appear to be applicable to online expression. See the section on sectoral laws for further details.

Law on Education (Education Law)

Article 18 of the Education Law stipulates that "[h]igher education shall teach learners to have complete personality and characteristic and promote the scientific, technical, cultural and social researches in order to achieve capacity, knowledge, skill, morality, inventive and creative ideas and enterprise spirit to the development of the country."¹⁵ These goals will be difficult to reach if freedom of expression is not ensured.

¹¹ Constitution of the Kingdom of Cambodia (1993). English translation referenced from: sithi.org/admin/upload/ law/2008_02_19_Constitution(EN)_including%20Amendment%20 (1).pdf

¹² CCHR. (2016). Digital Wrongs? An Overview of the Situation of Digital Rights in Cambodia. cchrcambodia.org/admin/media/ analysis/analysis/english/2016_03_03_CCHR_Briefing_Note_ Digital_Wrongs_ENG.pdf

¹³ Law on the Press (1995). English translation referenced from: sithi. org/admin/upload/law/Law%200n%20the%20Press%20(1995). ENG.pdf

¹⁴ Law on the Election of Members of the National Assembly (1997). English translation referenced from: sithi.org/admin/upload/law/ Law%200n%20the%20Election%200f%20the%20Members%20 of%20the%20National%20Assembly%20(1997)%20with%20 first,%20second%20and%20third%20a.pdf

¹⁵ Law on Education (2007). English translation referenced from: www.moeys.gov.kh/images/moeys/laws-and-regulations/48/ EducationLaw-EN.pdf

In that respect, Article 35 affords students the right to "free expression of their academic views" and the right to "freedom of study."¹⁶

See the section on sectoral laws for an analysis of the restrictions on freedom of expression contained in the Education Law.

International human rights law enshrined in domestic law

Article 31 of the Constitution enshrines international human rights law into Cambodian domestic law. It states: "The Kingdom of Cambodia recognises and respects human rights as stipulated in the United Nations Charter, the Universal Declaration of Human rights and the covenants and conventions related to human rights, women's rights and children's rights."

The direct applicability of international human rights law was confirmed by a 10 July 2007 decision by the Constitutional Council of Cambodia – the body tasked with constitutional interpretation.¹⁷ The decision states that no law should be applied by the courts in such a way that violates the Constitution or the human rights treaties to which Cambodia is a party.

As a consequence, individuals subject to the jurisdiction of Cambodian law – and not only "Khmer citizens" as outlined elsewhere in the Constitution – can, in theory, invoke international standards for the protection of their right to freedom of expression. It should be further noted that Cambodia has a high rate of ratification of international human rights treaties, having ratified eight of the nine core treaties¹⁸ (with the exception being the Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families).

Freedom of expression

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and Article 19 of the Universal Declaration of Human Rights (UDHR) guarantee the right to freedom of expression. Article 19 of the ICCPR specifies that freedom of expression "shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

Both the UDHR and the ICCPR were drafted with the foresight to include and accommodate technological developments through which individuals are able to exercise their right to freedom of expression, owing to the explicit inclusion of a provision that states that everyone has the right to express him or herself through any media. The treaty body responsible for interpreting the ICCPR - the United Nations Human Rights Committee - has advised that modes of expression do include all forms of electronic and internet-based methods of communication.¹⁹ meaning that international human rights law – and by extension, Cambodian law – is equally applicable to new and developing communication technologies, such as the internet and social media networks.20

This was confirmed on 5 July 2012 by the United Nations Human Rights Council (UNHRC) in a resolution – the first of its kind – to protect human rights online.²¹ The resolution states that "the same rights that people have offline must also be protected online." The resolution also acknowledges that "the internet can be an important tool for development and for exercising human rights."

Right to privacy

The right to privacy is enshrined in Article 12 of the UDHR, and Article 17 of the ICCPR. The latter states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Traditionally, the reference to "correspondence" in the UDHR and the ICCPR was interpreted to mean written communication; however, as stated above, this term now applies to all forms of communication, including via the internet.

In 2013, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, stated that there were interrelations between the rights to privacy and the right to freedom of opinion and

¹⁶ CCHR. (2012). Fundamental Freedoms Series: Freedom of Expression and Academic Freedom. cchrcambodia.org/admin/ media/factsheet/factsheet/english/2012_03_16_CCHR_ Fundamental_Freedoms_Series_Fact_Sheet_Freedom_of_ Expression_and_Academic_Freedom_March%202012_(ENG).pdf

¹⁷ Constitutional Court of Cambodia. (2017, 10 July). Decision No. 092/003/2007.

¹⁸ www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments. aspx

¹⁹ UN Human Rights Committee. (2011, 12 September). General Comment 34: Freedoms of Opinion and Expression, CCPR/C/GC/34 (GC 34) [12]. www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

²⁰ CCHR. (2016). Op. cit.

²¹ UN Human Rights Council. (2012, 29 June). The promotion, protection and enjoyment of human rights on the Internet, Resolution 20/8, A/HRC/RES/20/8. documents-dds-ny. un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325. pdf?OpenElement

expression.²² He noted that "[u]ndue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas," and therefore have a chilling effect on freedom of expression.

Regional law

In November 2012, the 10 member states of the Association of Southeast Asian Nations (ASEAN) – including Cambodia – adopted the ASEAN Human Rights Declaration (AHRD).

The AHRD affords every person the "right to freedom of opinion and expression" under Article 23, including the right to "hold opinions without interference [...] in writing or through any other medium."²³

The AHRD contains a general limitation clause in Article 8 of its opening principles, whose ultimate effect is to undermine its acknowledgement of the non-derogable or absolute nature of several human rights under customary law and the ICCPR. It holds that limitations on the exercise of fundamental freedoms can be subject to a wide range of limiting factors, including "the just requirements of national security, public order, public health, public safety, public morality, as well as the general welfare of the peoples in a democratic society." This is problematic as its wide scope and potential field of application fail to recognise that some human rights can never, under any circumstances, be restricted by the state. Conversely, derogations from civil and political rights protected by the ICCPR may only be made in strict accordance with the ICCPR itself, and some rights are specifically non-derogable.²⁴ In this context, the AHRD is inconsistent with Cambodia's international obligations, and in fact, undermines them.25

Governance of online and networked spaces

The Law on Telecommunications governs online and networked spaces in Cambodia. It is the only Cambodian law that specifically addresses online activity. Indeed, the law defines telecommunications as "the science and technology in sending and receiving the signals, data, sound, pictures or types

22 La Rue, F. (2013, 17 April). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40. www.ohchr.org/Documents/HRBodies/ HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

24 ICPPR, Article 4(2). No derogation is permitted from Articles 6, 7, 8(1)(2), 11, 15, 16 and 18.

25 CCHR (2016). Op. cit.

of other information by using the energy in the form of electro-magnetic, electricity, radio, light, or other forms."²⁶

Even though it is not enacted yet, it is also important to consider the draft Cybercrime Law, which would also regulate online content.

Law on Telecommunications

The 2015 Law on Telecommunications contains multiple restrictions on the right to freedom of expression, which are not in line with Cambodia's international and constitutional human rights obligations. The law poses a threat to private, confidential communications as well as online public expression and increases the control of the MPTC over the telecommunications sector. Several of the new criminal offences introduced by the Law on Telecommunications can lead to imprisonment and significant fines, and are disproportionate and overly broad.

Some of the most serious threats posed by the law can be summarised under the following themes: surveillance powers, criminalisation of expression and restriction of rights, and excessive state control.²⁷

Surveillance powers

The Law on Telecommunications gives the government the power to secretly monitor the telecommunications of any individual in Cambodia with a near-complete absence of checks and balances, and no requirement for judicial oversight.

Article 6 states: "All telecommunications operators and persons involved with the telecommunications sector shall provide to the Ministry of Posts and Telecommunications the telecommunications, information and communication technology service data." Under this provision, telecommunications operators appear to be required to pass over data on their service users, without any recourse to judicial or other independent oversight. The meaning of "service data" is undefined in the law and as such could be interpreted to include all user communication records, browsing history and other confidential information. This appears to be in violation of Article 40 of the Constitution, which ensures the right to confidentiality.

Furthermore, Article 97 criminalises eavesdropping by private individuals, with sanctions of

²³ www.asean.org/storage/images/ASEAN_RTK_2014/6_AHRD_ Booklet.pdf

²⁶ Law on Telecommunications (2015), Annex: Glossary for using this law. English translation referenced from: sithi.org/admin/upload/ law/20150127_TelecommunicaitonDraftLaw_En%20edited-2.pdf

²⁷ LICADHO. (2016). Cambodia's Law on Telecommunications: A Legal Analysis. www.licadho-cambodia.org/reports/ files/214LICADHOTelecomsLawLegalAnalysis_March2016ENG.pdf

imprisonment from one month to one year and a fine from 100,000 riels (USD 24) to two million riels (USD 480), but permits secret surveillance with approval of a "legitimate authority". Arguably, this provision allows the monitoring of individuals' phone calls, emails, texts and social media activity and other online correspondence without their knowledge.²⁸ Moreover, "legitimate authority" is an undefined term, which may simply refer to administrative or internal authorisation, rather than the independent judicial oversight necessary to protect individual rights. In effect, this provision appears to give carte blanche surveillance powers to the Cambodian government.

Criminalisation of expression and restriction of rights

The law also introduces new criminal offences with heavy sanctions for telecommunications activity. These provisions could not only be used to criminalise freedom of expression online, but may also be further abused to "spy on high profile individuals and selectively interpret the content of their communications as criminal activity."²⁹

Article 80 creates a broad criminal offence that imposes high sentences. It states: "Establishment, installation, or modification of telecommunication infrastructure and network or establishment, installation and utilization of equipment in telecommunication sector, if these acts lead to national insecurity, shall be sentenced in prison from 7 (seven) years to 15 (fifteen) years." Furthermore, Article 81 states that violation of Article 80 can lead to fines from 140 million riels (USD 33,600) to 300 million riels (USD 72,000). No telecommunication activity (the term is undefined) appears to be excluded: any form of expression, public or private, and conducted by any electronic means of communication could be criminalised if it is deemed to create "national insecurity". Such a vaguely drafted provision, which potentially includes a wide range of legitimate expression within its scope, cannot be considered proportionate, narrowly defined, transparent or easy to understand. While such broad criminalisation of expression affects all individuals and groups in Cambodia, it is of particular concern to associations who may in their work be critical of the government and could easily be subject to targeting by authorities choosing to construe their internal or external communications as contributing to "national insecurity".

Similarly to Article 80, Article 66 includes a general prohibition on telecommunications activity stating that the "establishment, installation, utilization, and modification of telecommunication infrastructure... which may affect public order and lead to national insecurity are prohibited." Again, there is no requirement of actual harm, but rather activity that "may" affect public order or national security. Therefore, an activity that causes no harmful or palpable consequences may be criminalised.

Articles 93-95 are offences new to the Law on Telecommunications but replicate existing Criminal Code provisions on expression, whilst imposing higher penalties. Article 93, which prohibits "threats", carries sanctions from one month to three years imprisonment and fines from 100,000 riels (USD 24) to six million riels (USD 1,440). Equally, Articles 94 and 95 further criminalise threats and impose heavy sanctions. This is problematic not least because there is a risk of conflict between these provisions and those in the Criminal Code.

Article 65(b) preserves the "[r]ights to privacy, security and safety of using the telecommunications service." However, this protection is nullified by the exception clause authorising the government to disregard it should it be "[o]therwise determined by other specific laws." Unfortunately, in claiming to protect the right to privacy, as enshrined in the Constitution, the provision includes an exception clause, which renders it unconstitutional and a violation of the right to privacy.

Excessive state control

Article 7 provides that "[i]n the event of a force majeure, MPTC [...] may order relevant telecommunications operators to take necessary measures," which could likely encompass internet shutdowns. Troublingly, there is no definition of what constitutes a "force majeure"; however, this provision could be used to inhibit internet usage, including forms of messenger and means of social mobilisation.30 Further competencies are afforded to the MPTC under Article 24, which states: "Telecommunications infrastructures and networks and supporting telecommunication infrastructures shall fall under the competence of MPTC." Under these provisions, the government appears to be granted control of the entire telecommunications industry including activity and infrastructure. This is particularly threatening to organisations and individuals who are critical of the government and whose work may be affected by the prospect of surveillance.

²⁸ Ibid. 29 Ibid.

Cybercrime Law

First draft

In May 2012, the RGC announced its intention to adopt Cambodia's first ever Cybercrime Law in order to regulate online content and to prevent the "ill-willed" from "spreading false information."³¹

A first draft was leaked in April 2014, but the RGC refused to publicly release an official version. This first draft contained several provisions which would have unduly restricted freedom of expression online.

One of the most controversial provisions was Article 28 of the law. This article severely limited the content of online activity and websites. It sought to prohibit content deemed to "generate insecurity, instability and political incohesiveness," as per Article 28(3), or "deemed damaging to the moral and cultural values of the society," including "manipulation, defamation, and slanders", under Article 28(5) (c). Article 28(4) prohibited content "undermining the integrity of any governmental agencies." These broad terms could have led to abuses that clearly would have fallen afoul of Cambodia's international human rights obligations.³²

Violations of these prohibitions would have been sanctioned by imprisonment from one to three years and heavy fines ranging from two million riels (USD 480) up to six million riels (USD 1,440).

Furthermore, Article 6 of the first draft law would have established a 14-person body called the National Anti-Cybercrime Committee, composed of high-ranking members of the government, which would have had control over the implementation of the law.³³

Second draft

In response to the outrage expressed over the first draft, a second draft was leaked to certain non-governmental organisations (NGOs) from the Ministry of Interior in September and October 2015.

Although the second draft removed some of the most troubling provisions contained in the first draft – such as Articles 28 and 6 – it nonetheless contains new provisions which also threaten freedom of expression online. Article 27 allows for the dissolution of legal entities – including NGOS – on the basis of the cybercrimes of individuals affiliated with the organisations.³⁴

Additionally, the draft confers overly broad and intrusive powers upon police and investigators to search and seize the property of those suspected of cybercrimes, with a complete lack of judicial oversight and procedural safeguards, threatening the right to privacy and the right to freedom of expression.

The individual crimes enumerated in the draft are very broadly defined, and would give significant scope to the RGC to implement the law abusively against its perceived opponents, in violation of national and international human rights guarantees. For example, Article 13(1) criminalises obtaining data that "are considered to be confidential and which are specifically protected against unauthorized access." There is no intent element; a person may be imprisoned for receiving an email containing such data, even if that email was sent by mistake or the receiver did not know that they did not have permission to view it.

Sectoral laws

In Cambodia, many sectoral laws impose administrative penalties that can be used to stifle freedom of expression. Often, opposition political parties, NGOs and civil society organisations (CSOs) which are critical of the government are targeted in this manner.

None of the sectoral laws outlined below explicitly refer to online activities. Nevertheless, case studies suggest their uniform applicability to the online world. See the section below on curtailment of freedom of expression for more detail.

Law on Associations and Non-Governmental Organizations (LANGO)

The LANGO curtails freedom of expression through a number of vague provisions.

Article 24 states that "[d]omestic non-governmental organizations, foreign non-governmental organizations, or foreign associations shall maintain their neutrality towards political parties in the Kingdom of Cambodia."³⁵ This vague provision leaves space for serious violations of freedom of expression and abuses by authorities in order to silence dissent and criticism. There are a number of legitimate civil society activities which could potentially fall under the scope of this vague provision.

³¹ Di Certo, B., & Yuthana, K. (2012, 24 May). The 'ill-willed' spark cyber law: officials. *The Phnom Penh Post*. www.phnompenhpost. com/national/'ill-willed'-spark-cyber-law-officials

³² CCHR. (2016). Op. cit.

³³ Wilwohl, J., & Reaksmey, H. (2014, 10 April). Cybercrime Law May Silence Critics, NGOS Say. The Cambodia Daily. www.cambodiadaily.com/archives/ cybercrime-law-may-silence-critics-ngos-say-56288

³⁴ CCHR. (2016). Op. cit.

³⁵ LANGO (2015). English translation referenced from: sithi.org/ admin/upload/law/Unofficial-Translation-LANGO.pdf

CASE STUDY: CAMBODIA'S POLITICAL PRISONERS

In May 2016, Justice Ministry officials warned human rights group LICADHO that its new webpage documenting Cambodia's "political prisoners" could be in contravention of the LANGO, arguing that the page could violate Article 24 of the law, which requires political neutrality. Justice Ministry spokesman Kim Santepheap said the following in a Facebook post: "Licadho is walking away from its professionalism and its statute." He added: "I want to inform public opinion that Cambodia does not have political prisoners at all. In all prisons and correctional centers throughout Cambodia, there are only inmates jailed over criminal offenses."³⁶

Article 30 (1) governs the consequences of non-compliance with Article 24. It states that any domestic organisation which does not comply with Article 24 will first be issued a warning, then have their activities suspended for 90 days, and if there is continued non-compliance, the Ministry of Interior shall remove it from the register.

The LANGO also prohibits both domestic associations and NGOs, under Article 30(3), and foreign associations and NGOs, under Article 35, from conducting activities that adversely affect "security, stability and public order" or that "harm security, stability, and public order, or endanger the national security, national unity, culture, good traditions and customs of Cambodian national society." The broad wording of these provisions could easily encompass legitimate expression made by associations and NGOs, for example, commenting on political events or criticising government action. This is particularly concerning for CSOs working in the field of human rights and the rule of law.37 "National unity" and "good traditions and customs of Cambodian national society", being undefined in the law, are particularly open to subjective and discriminatory interpretation to serve political ends.

CASE STUDY: THE "SITUATION ROOM"

A loose and ad hoc coalition of NGOs known as the "Situation Room", which was formed to monitor the 2017 Commune Council elections, was threatened with legal action under the LANGO. On 4 July 2017, the Interior Ministry issued a letter to the Situation Room ordering it to cease its activities in alleged violation of the neutrality requirement of the LANGO.³⁸

Article 30 (3) provides for sanctions in case of breaches of Article 35, entailing a penalty of deregistration for domestic associations and NGOs. Article 35 entails a penalty of termination of the memorandum of understanding for foreign associations and NGOs. Deregistration is the ultimate form of limitation of expression for associations, because, according to Articles 9 and 12 of the LANGO, all NGO activities are prohibited unless the NGO is registered.

Law on the Election of Members of the National Assembly (LEMNA)

The LEMNA contains numerous restrictions on freedom of expression linked to electoral campaigns, which could be applied to online activities.

Article 71 restricts political parties and candidates or supporters from making verbal remarks or written statements that are "immoral" or that "insult" candidates, their supporters or any person. This provision is vague and could therefore lead to abuses. Simply disagreeing with a political party could be characterised as "insult".³⁹

Article 72 states that electoral campaigns can only occur during a 21-day period and must stop 24 hours before the polling day. There is no reason given in the law for this restriction of freedom of expression, and campaign activities outside the sanctioned period could be subject to punishment.

Political neutrality of NGOs is also enforced in the LEMNA. Articles 84 and 137 rule that organisations, both local and international, as well as all foreigners, must be "neutral and impartial" in the elections. Furthermore, Article 84 lists a number of direct or indirect activities that are prohibited

³⁶ Narim, K., & Wright, G. (2016, 20 May). Rights Group Warned Over 'Political Prisoners' Page. The Cambodia Daily. www.cambodiadaily.com/archives/ rights-group-warned-over-political-prisoners-page-112823

³⁷ As noted by then Special Rapporteur on the Situation of Human Rights in Cambodia, Surya Subedi, following a visit to Cambodia in 2014, in relation to the (then draft) LANGO and draft Cybercrimes Law, "Any laws regulating freedom of expression online and the formation and operations of associations and NGOs are necessarily a direct concern for civil society." Subedi, S. (2014, 24 June). Press Statement. cambodia.ohchr.org/sites/default/files/ pressstatementsource/SR_statement24062014_Eng.pdf

³⁸ Sokhean, B., & Paviour, B. (2017, 5 July). Interior Ministry Issues Stop-Order to Situation Room NGOs. The Cambodia Daily. www.cambodiadaily.com/news/ interior-ministry-issues-stop-order-to-situation-room-ngos-132133

³⁹ European Union Follow-up Mission to Cambodia. (2015). *Final Report*. eeas.europa.eu/sites/eeas/files/efm_cambodia_2015_ final_report_publ.pdf

for local and international organisations, including "releasing a statement or doing any activities with the aim of supporting or showing bias towards or against a political party or candidate." There is no similar provision for government employees. Therefore, any activity could be seen as a violation of the law even if it is not intended to support a party. For instance, Article 84 of the LEMNA could be interpreted by the authorities to mean that monitoring groups commenting on elections violate the requirements of impartiality and neutrality.

Article 85 prohibits foreigners from "carrying out direct or indirect activities in the election campaign to support or oppose a political party." This restricts the activities that foreigners can be involved with around the election period and restricts their freedom of expression regarding political parties or candidates. Once again, the vagueness of this provision could lead to abuses. Terms like "indirect" or "foreigners" are indeed not defined.

Articles 140 to 161 state the penalties for the various violations of the LEMNA. A violation of Article 84 leads to the removal of the responsible person from the voter lists for five years (Article 147). A violation of Article 85 leads to the deportation of the foreigner who expressed his/her opinion (Article 149). Article 152 outlines high penalties (five million to 10 million riels – USD 1,200 to USD 2,400) for "any person who [...] publicly insults a political party or a candidate running in the election." This is another example of how the law may be abused to sanction legitimate criticism of a party, policy or candidate.

Law on Political Parties (LPP)

The LPP contains multiple undue restrictions on freedom of expression, many of which appear to apply in the online sphere.

Article 6 of the LPP prohibits political parties from "caus[ing] secession that leads to the destruction of national unity and territorial integrity", "subvert[ing] the liberal multiparty democracy and the constitutional monarchy", "affect[ing] the security of the state", "recruit[ing] armed forces" and "incitement that would lead to national disintegration."⁴⁰ Terms such as "subversion", "incitement", "destruction", "integrity" and "disintegration" are undefined. They are vague, unquantifiable and subjective and therefore leave the provisions open to arbitrary interpretation. In March and July 2017, the National Assembly passed two separate amendments to the LPP. Both these amendments received widespread criticism from human rights organisations due to their severe and unjustifiable restrictions on freedom of expression and other fundamental freedoms. Many of the amended provisions apply to the online space, as they regulate the types of images and symbols which can be used by political parties, and they further invoke severe sanctions – including suspension and dissolution – for political parties that communicate with any individual who has committed any misdemeanour or felony at any point in their lives.

The first amendments to Article 6 of the LPP state that political parties should not:

(6) Use [...] voices, messages, images, written documents or activities of a person convicted of felony or misdemeanor for political gains/interests of its party.

(7) Openly or tacitly agree or conspire with a person convicted of felony or misdemeanor to carry out any activities for political gains/interests of its party.

(8) Support or develop any plans or conspire with any individuals who carry out activities aiming at opposing the interest of the Kingdom of Cambodia.

These amendments drastically expand the scope of Article 6 and further burden the right to freedom of expression. The provisions are excessively broad and unpredictable. They exacerbate the ambiguous nature of Article 6. For example, Article 6(7), by prohibiting the "tacit" agreement of a political party with the supportive statement of any convicted person, could entail the dissolution of a political party unless it dissociates itself from every convicted person who expresses support for the party online, every time such support is expressed. This would likely be practically impossible to enforce; and in fact, many observers have commented that the two amendments were introduced purely to target former opposition leader Sam Rainsy.

The amended LPP also introduced new articles, including Articles 11 and 45. Article 11 (3) states that "[t]he symbol/logo of a political party should not be copied or taken from a national symbol or picture representing a religion, Angkor Wat temple or pictures of sculptures of all Khmer Kings or the picture of a physical person." The prohibition on the use of "the picture of a physical person" constitutes an excessive and unjustifiable restriction on freedom of expression. Banning all images of all individuals from political

⁴⁰ CCHR. (2017). Legal analysis of the July 2017 proposed amendment to the LPP. cchrcambodia.org/admin/media/analysis/analysis/ english/2017-07-19-CSO-ssubmit-Legal-Analysis-of-Proposed-Amendment-to-LPP-to-CC_ENG.pdf

party symbols does not serve any legitimate aim, such as public health or national security, as outlined in Article 19 (3) of the ICCPR. As such, this provision constitutes an impermissible restriction on freedom of expression.

CASE STUDY: SAM RAINSY

In February 2017, the opposition leader, Sam Rainsy, resigned as president of the CNRP in the face of threats by Prime Minister Hun Sen to pass an earlier amendment to Article 6 of the LPP. This amendment barred convicts from political leadership and dissolved parties led by individuals convicted of crimes by Cambodia's courts.⁴¹ Sam Rainsy was sentenced numerous times since he left Cambodia in November 2015. He had to resign to avoid the possible dissolution of the CNRP, just months ahead of the Commune Council elections.

Trade Union Law (TUL)

The TUL severely restricts the freedom of expression of workers and trade unions by limiting the scope of their legitimate activities. It is likely that these provisions apply to online speech, though there have not yet been any relevant cases to verify this.

Article 65(f) provides that it is unlawful for a union "to agitate for purely political purposes or for their personal ambitions or committing acts of violence at the workplace and other places."42 Unions have long been legitimate centres of political activity; indeed their key objectives of protecting and promoting the rights of workers will inevitably entail engagement with political issues, institutions and processes. Similarly, regardless of the moral or social merits of "personal ambitions", it cannot seriously be argued that they should render a union's activities unlawful. The subjective and broad nature of these terms also means that they could easily be abused by authorities to characterise a union leader's social media commentary as unlawful.43 Further, Article 71 considers as "interference,

41 Naren, K. (2017, 11 February). Sam Rainsy Resigns as Opposition Party President. *The Cambodia Daily*. www.cambodiadaily.com/ morenews/sam-rainsy-resigns-opposition-party-president-124975 incitement or interruptions" acts by which minority unions demand to express their views.⁴⁴

Anti-Corruption Law

The Anti-Corruption Law contains numerous provisions which restrict the right to freedom of expression.

The law not only fails to provide a legal framework for the physical and legal protection of individuals who blow the whistle on corrupt practices; in fact, Article 41 creates a criminal offence if "defamation or disinformation complaints [...] lead to useless inquiry."45 Such an offence is subject to serious penalties: imprisonment from one to six months and a fine from one million riels (USD 240) to 10 million riels (USD 2,400). "Useless inquiry" is not defined in the law, and there is no requirement of intention in relation to a false complaint. It is therefore unclear whether an incorrect complaint, rather than a deliberately false one, constitutes an offence under the law. These provisions, and the lack of certainty as to how they will be interpreted, are likely to instil fear in people, and therefore act as deterrents to those who might come forward with information about corruption.46

The Anti-Corruption Law also gives significant and unchecked surveillance powers to the Anti-Corruption Unit (ACU). According to Article 27 of the law, the ACU is authorised to "monitor, oversee, eavesdrop, record sound and take photos, and engage in phone tapping" where there is a "clear hint of corruption." It is also authorised to "check documents and documents stored in the electronic system." This means that the subjective interpretation of a "hint" of corruption could open an individual's private communications to scrutiny and monitoring.

Law on the Press (Press Law)

The Press Law contains many vague provisions which restrict the right to freedom of expression, not only of journalists, but also of newspaper

⁴² Trade Union Law (2016). English translation referenced from: sithi. org/admin/upload/law/trade_union_law_eng.pdf

⁴³ CCHR. (2016). Trade Union Law 2016 (the "TUL"). cchrcambodia. org/admin/media/factsheet/factsheet/english/2016_08_24_ cchr_fs_lcs_trade_union_law_ENG.pdf

⁴⁴ For more detailed analysis of this and other provisions of the TUL, see: Office of the United Nations High Commissioner for Human Rights in Cambodia. (2016). *A Human Rights Analysis of the Draft Law on Trade Unions*. cambodia.ohchr.org/~cambodiaohchr/sites/ default/files/FINAL%20OHCHR%20Analysis%200n%20Trade%20 Union%20Law-%20En%20%20FOR%20NA%20SUBMISSION.pdf and International Center for Not-for-Profit Law. (2015). *Analysis of Draft Trade Union Law*. www.icnl.org/programs/asia/ICNL%20 Legal%20Analysis_TradeUnionLaw.pdf

⁴⁵ Anti-Corruption Law (2010). English translation referenced from: sithi.org/admin/upload/law/National%20Assembly_Feb%20 24,2010_Draft%20Law%200n%20Anti-Corrution%20in%20Eng.pdf

⁴⁶ CCHR. (2011). Law on Anti-Corruption. cchrcambodia.org/ admin/media/factsheet/factsheet/english/CCHR%20Fact%20 Sheet%20-%20Law%20Review%20Series%20-%20The%20Anti-Corruption%20Law%202010%20(ENG).pdf

owners, editors and publishers working within the media.

For instance, while Article 20 claims to guarantee freedom of expression, no indication or guidance is given as to what would constitute the expression of a protected opinion as opposed to an act of defamation or libel, which means that the effectiveness and reliability of this carve out is unfortunately compromised due to the loose drafting of the provision.⁴⁷

Moreover, the Press Law imposes content restrictions in relation to anything which "may affect the public order by inciting directly one or more persons to commit violence" (Article 11) or which "may cause harm to the national security and political stability" (Article 12) or which affects "the good custom of society" (Article 14). The Press Law also constrains criticism of public officials and institutions by providing that "[t]he press shall not publish or reproduce false information which humiliates or contempts national institutions" (Article 13).⁴⁸

These terms remain undefined and therefore undermine the scope of Article 1, which, as stated earlier, takes a protective approach. They are potentially problematic because they involve high financial sanctions and, in the case of Article 12, the possibility for the Ministries of Information and Interior to suspend publications for up to 30 days, without any recourse to appeal.⁴⁹

Law on Education (Education Law)

Article 34 of the Education Law states: "Educational institutions and establishments shall respect the principles of neutrality. Political activities and/or propaganda for any political party in educational establishments and institutions shall be completely banned." It is unclear whether this provision applies to online activity, although it can be assumed that it does, based on the general trend of laws in Cambodia restricting expression being applied online despite lacking any overt mention of online activity.

This provision, by preventing political groups from organising events or conducting activities in educational contexts, and preventing the formation of political groups in educational institutions and establishments, constitutes a severe restriction on freedom of expression. Vague terms like "neutrality" and "propaganda" can be used to target activities by groups not aligned with or deemed not supportive of the ruling party. It is worth highlighting that, in practice, Article 34 does not apply equally to all political parties.

Article 52 outlines high penalties for violations of Article 34. The fine is normally between one million riels (USD 240) and five million riels (USD 1,200); it will be doubled in the case of a repeat violation. Article 52 also outlines larger and more punitive sanctions for legal entities: the fine will be between 10 and 20 million riels (USD 2,400 and USD 4,800); this amount will be doubled in the case of a repeat violation. For educational institutions, nevertheless, a recidivous violation will lead to the suspension or the permanent revocation of the educational licence of the establishment.

In addition, the "Instruction on preventing political activities or political propaganda at public and private academic institutions" (also known as the Education Circular) – a form of secondary law which outlines in greater detail the scope of the Education Law – provides that the fines established in the Education Law⁵⁰ for violation of Article 34 apply to academic staff, in addition to educational institutions, as already provided for in the law, adding a further restriction on individual freedom of expression.

Article 42 deals with advertising or propagandising educational information. It gives significant powers to the Ministry of Education, Youth and Sport (MoEYS), which is in charge of authorising such information. Article 53 outlines severe penalties for violations of Article 42. The fine is normally between two million riels (USD 480) and 10 million riels (USD 2,400); it will be doubled in the case of a repeat violation and may lead to the suspension or the cancellation of the educational licences of educational institutions or establishments.

Education Circular

On 11 August 2015, the MoEYS published an Education Circular which goes beyond the text of the Education Law to impose additional restrictions on the freedoms of expression and association in an educational context. It appears to directly contradict the rights guarantees contained in Articles 35 and 37 by imposing a sweeping ban on freedom

⁴⁷ CCHR. (2012). An overview of Cambodian laws relating to freedom of expression and a summary of recent case examples to show how laws are used and abused to stifle dissent. cchrcambodia.org/ admin/media/analysis/analysis/english/2012_10_30_CCHR%20 Briefing%20Note%20_%20Cambodian%20laws%20relating%20 to%20freedom%200f%20expression%20and%20recent%20 case%20examples%20-%20ENG.pdf

⁴⁸ Sopheap, C. (2015, 19 February). Cambodia: a long way towards freedom of expression. WACC. www.waccglobal.org/articles/ cambodia-a-long-way-towards-freedom-of-expression

⁴⁹ CCHR. (2011). The Law on the Press 1995 ("the Press Law"). cchrcambodia.org/admin/media/factsheet/factsheet/english/ CCHR Fact Sheet Law Review Series - Press Law (ENG).pdf

⁵⁰ Law on Education (2007). English translation referenced from: www.moeys.gov.kh/images/moeys/laws-and-regulations/48/ EducationLaw-EN.pdf

of association in the context of educational institutions and establishments.

Article 1 of the Education Circular states: "Associations, NGOs or any agencies are not allowed to conduct any activities at the educational institutions without the permission from the Ministry of Education, Youth and Sport." Therefore, the Education Circular provides a greater restriction upon the right to freedoms of expression and association than contained within the Education Law. Whereas the Education Law allowed for associations and NGOs to conduct "neutral" activities at educational institutions, there is now a blanket ban on all activities carried out by any NGO, association or agency unless permission has been granted by the MoEYS.

Any restriction on the freedoms of expression and association must be prescribed by law, necessary and proportionate. The Education Circular effectively imposes a complete restriction on freedom of association in educational institutions, subject to permission from the MoEYS. The Circular is vaguely drafted and restricts a wide range of persons and activities. Thus, in addition to limiting CSOs that wish to conduct activities in educational institutions, it will also apply more broadly; for example, to students wishing to form associations or societies.

Circulars are lower down in the hierarchy of Cambodia's legal framework. They are ministerial implementing measures, and thus are designed to organise the implementation of other legislation, rather than to create new law. As a restriction on a constitutionally protected fundamental freedom, and given that the Circular appears to be inconsistent with the Education Law itself, it is unclear whether the measures provided for in the Education Circular are valid in the domestic legal order, adding a further lack of clarity to the legal framework governing freedom of expression and freedom of association.

Law on the Denial of Crimes Committed During Democratic Kampuchea (Denial Law)

The Denial Law states that anyone who refuses to recognise, denies, opposes the existence of or promotes the crimes committed during the Khmer Rouge era could face up to two years imprisonment and up to four million riels (USD 1,000) in fines.⁵¹ It is likely that this law also applies to the online space, though there are no cases to confirm this assumption. The Denial Law is contrary to provisions protecting freedom of expression under both domestic and international law. Education, debate, discussion and research into the Khmer Rouge era are essential in helping the country to move on and to prevent similar events from reoccurring. A law aiming at restricting opinions and debate about the crimes perpetrated by the Khmer Rouge could potentially stifle such invaluable discussion. Furthermore, the Denial Law could be used for political purposes to control the historical narrative surrounding the Khmer Rouge – which is particularly problematic given that many figures in the current Cambodian government were themselves Khmer Rouge commanders and officials.⁵²

Law on Access to Information

The right to information is crucial for the protection of other human rights like the freedom of expression. As stated by the UN General Assembly during its first session in 1946, "freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated."⁵³

The Draft Law on Access to Information contains important restrictions on the right to information.

According to Article 20 of the Draft Law, any information that would (1) damage Cambodia's national security and public order, (2) affect international relations, (3) threaten the economy or finances, or (4) affect case files or confidentialities of the court, could be withheld from the public. Public institutions may also deny providing information to the public if the disclosure of such information would (5) violate the personal privacy of individuals, (6) endanger law enforcement agencies and their missions, or (7) be harmful to legal documents and other prohibitive provisions on confidential information.

The Draft Law gives examples of which types of information would be considered confidential. It mentions civil servants' cases, health-related cases and case files of private rights litigation. This list is not limited and could therefore be interpreted broadly. These provisions are vague and could be misused to prevent the disclosure of a wide range of information.⁵⁴

⁵¹ Freeman, J. (2014, 6 June). KR denial law sees no cases in 1st year. *The Phnom Penh Post.* www.phnompenhpost.com/national/ kr-denial-law-sees-no-cases-1st-year

⁵² CCHR. (2013). CCHR expresses grave concern relating to the potential impact of a Khmer Rouge crimes denial law on Freedom of Expression in Cambodia. cchrcambodia.org/media/files/ press_release/391_200cpcecrtpkrcdle_en.pdf

⁵³ UN General Assembly. (1946, 14 December). Calling of an International Conference on Freedom of Information. A/RES/59. www.refworld.org/docid/3boof0975f.html

⁵⁴ Turton, S. (2015, 10 June). Officials' affairs may be secret under law. *The Phnom Penh Post.* www.phnompenhpost.com/national/ officials-affairs-may-be-secret-under-law

Curtailment of freedom of expression

Criminal Code

The Criminal Code is increasingly used to curb freedom of expression, and provides for heavy and disproportionate punishments for violators. While there is no mention of online speech in the Criminal Code, case studies show that provisions used to limit freedom of expression are applicable in the online world. These provisions can be classified in various categories, outlined below.

Defamation and related offences

Provisions on defamation are often invoked to target opposition figures or those critical of the government. In March 2017, the ASEAN Parliamentarians for Human Rights (APHR) warned that "criminal trials over cases of alleged defamation have become prevalent and normalized."⁵⁵

Article 305 outlines the definition of public defamation: "Any allegation or charge made in bad faith which tends to injure the honour or reputation of a person or an institution."⁵⁶ This article provides for infringements on freedom of expression by not requiring an actual harm to an individual's honour or reputation but by stating that a charge only needs to tend to harm reputation and honour.⁵⁷ Moreover, the commission of the offence merely requires that the defamation be made by means of "any words whatsoever uttered in a public place or in a public meeting." This implies that individuals may be prosecuted for private conversations.

Defamation is punished by a fine of 100,000 to 10 million riels (USD 24 to USD 2,400). Many Cambodians would not be able to pay a heavy fine, which would lead to their imprisonment for 10 days to two years (Article 525 of the Cambodian Code of Criminal Procedure).

The blanket criminalisation of all forms of defamation is not consistent with international human rights standards and best practices, and, in particular, the existence of such a broadly drafted criminal offence must be considered to be disproportionate. While defamation laws can be a permissible restriction on freedom of expression to protect the reputation of others, the UN Human Rights Committee has made clear that such laws must not in practice stifle freedom of expression, that they should include defences such as truth and public interest in the subject of criticism, and that application of the criminal law should only be permitted in the most serious cases.58 In its General Comment No. 34 (2011) on Article 19 of the ICCPR (Freedoms of opinion and expression), the Human Rights Committee further called on ICCPR states parties to "consider the decriminalization of defamation" and noted that "the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty."59 It is worth mentioning that on 21 April 2006, the RGC removed the custodial sentence of eight days to one year for defamation under Article 63 of the 1992 Criminal Law, commonly known as the UNTAC Law.60

CASE STUDY 1: SAM RAINSY

On 28 July 2016, the Cambodian opposition leader Sam Rainsy was convicted of defamation against National Assembly President Heng Samrin and ordered to pay USD 37,500 in compensation. Mr. Rainsy had posted on Facebook a video clip of a speech by former King Norodom Sihanouk in the early 1980s. Under the video clip, you could read: "We remember that the regime born on 7 January 1979 used their tribunal to sentence our late King Norodom Sihanouk to death by accusing him of being a traitor."⁶¹ On 27 December 2016, Rainsy was convicted of forgery and incitement in relation to this case and was sentenced to five years in prison.⁶²

⁵⁵ ASEAN Parliamentarians for Human Rights (APHR). (2017). Death Knell for Democracy. aseanmp.org/wp-content/uploads/2017/03/ APHR_Cambodia-MPs-Report_Mar-2017.pdf

⁵⁶ Criminal Code (2009). English translation referenced from: sithi. org/admin/upload/law/Criminal_Code_Book_with_cover_ Jan_2014.pdf

⁵⁷ CCHR. (2014). The criminalization of defamation and freedom of expression in Cambodia. cchrcambodia.org/admin/media/ analysis/analysis/english/2014_05_27_CCHR_Briefing_Note_ Defamation_in_Cambodia_(ENG).pdf

⁵⁸ UN Human Rights Committee. (2011, 12 September). Op. cit.

⁵⁹ The UN Human Rights Council's recommendation in the Report of the Working Group on Cambodia's second Universal Periodic Review (A/HRC/26/16, 27 March 2014) that Cambodia "Repeal or amend relevant articles of the Penal Code, such as those regarding defamation or the discrediting of judicial decisions, which would bring Cambodia's domestic legislation into line with its international human rights obligations on freedom of expression" was noted, but not accepted, by the Cambodian government. See "Views on conclusions and/or recommendations, voluntary commitments and replies presented by the State under review", A/HRC/26/16/Add.1. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session26/ Documents/A.HRC.26.16.Add.1_AV.doc

⁶⁰ Asian Human Rights Commission. (2006, 24 April). CAMBODIA: New law removes custodial sentence for defamation but restricts freedom of expression. www.humanrights.asia/news/ahrc-news/ AS-078-2006

⁶¹ Khmer Times. (2016, 28 July). Rainsy Fined For Defamation Khmer Times. www.khmertimeskh.com/news/27778/ rainsy-fined-for-defamation

⁶² Sovuthy, K. (2016, 28 December). Jail Time Piles Up for Sam Rainsy. *The Cambodia Daily*. www.cambodiadaily.com/news/ jail-time-piles-sam-rainsy-122536

On 8 November 2016, Rainsy was found guilty of defamation after posting on Facebook that Prime Minister Hun Sen's Facebook likes were bought from "click farms" in India and the Philippines.⁶³

CASE STUDY 2: KEM LEY

Political commentator and activist Kem Ley was assassinated on 10 July 2016 at a petrol station in Phnom Penh. Since then, several people have been charged and convicted for accusing the Cambodian government of being responsible for his death. In November 2016, opposition Senator Thak Lany was convicted of defamation and incitement *in absentia* and sentenced to 18 months in prison for alleging that Prime Minister Hun Sen was behind the assassination of Kem Ley. The offending remarks were made in a video – later uploaded to Facebook – of a speech to party supporters in Ratanakkiri province.⁶⁴

In February 2017, political commentator Kim Sok was arrested under charges of defamation and incitement after having made comments in an interview with Radio Free Asia, in which he accused the government of being involved in the death of Kem Ley.⁶⁵

In March 2017, Sam Rainsy was found guilty of defamation and incitement for stating in a Facebook post that the death of Kem Ley was "state-backed terrorism."⁶⁶ He was given a 20-month sentence and a fine of 10 million riels (USD 2,400). The Appeal Court upheld the sentence on 11 August 2017.⁶⁷

Defamation is accompanied by a plethora of other offences in the Criminal Code, which severely limit the right to freedom of expression, and almost

- 64 Sarom, K. (2017, 11 August). Court hears Thak Lany appeal defamation conviction. *The Phnom Penh Post.* www.phnompenhpost.com/national/ court-hears-thak-lany-appeal-defamation-conviction
- 65 Odom, S. (2017, 17 February). Commentator Kim Sok Jailed Over Defamation, Incitement Charges. *The Cambodia Daily*. www.cambodiadaily.com/news/commentator-kim-sok-jaileddefamation-incitement-charges-125375
- 66 Chheng, N. (2017, 30 March). Sam Rainsy handed jail time in defamation case against PM. *The Phnom Penh Post.* www.phnompenhpost.com/national/ sam-rainsy-handed-jail-time-defamation-case-against-pm
- 67 Odom, S. (2017, 11 August). Appeal Court Upholds 20-Month Sentence for Sam Rainsy. *The Cambodia Daily*. www.cambodiadaily.com/news/ appeal-court-upholds-20-month-sentence-sam-rainsy-133552

completely undermine the government's removal of the custodial sentencing for defamation. In practice, defamation is often coupled with complementary charges, which do carry custodial sentences.

Article 307 (Public Insult) makes it a crime subject to the same penalties as the offence of defamation to use any "[o]utrageous expression, term of contempt or any invective that does not involve any imputation of fact." Like under Article 305, the commission of the offence requires that the insult be made by means of "any words whatsoever uttered in a public place or in a public meeting." This implies that individuals may be prosecuted for private conversations.

Article 502 (Insult of a Public Official) criminalises individuals whose words, gestures, written documents, pictures or objects are held to undermine the dignity of a public official or "holder of public elected office", while Article 523 criminalises any criticism of court decisions which is said to be aimed at "disturbing public order" or "endangering an institution" of Cambodia.⁶⁸ Violators of Article 502 are subject to punishments of one to six days imprisonment and a fine from 1,000 riels (USD 0.2) to 100,000 riels (USD 24). Violators of Article 523 are subject to punishment of one to six months imprisonment and a fine from 100,000 riels (USD 24) to one million riels (USD 240).

Article 311 penalises "malicious denunciation", which is defined as:

The act of denouncing a fact that is known to be incorrect and it is so knowingly to result in criminal or disciplinary sanctions constitutes a slanderous denunciation, when it is addressed to: (1) a competent authorities, such as a judge, a judicial police officer, or an employer; (2) or a person with power to refer the matter to the competent authorities.

This provision limits freedom of expression by discouraging whistleblowers and those who may be critical of government or judicial actions, such as human rights defenders. The punishment for this offence includes imprisonment of between one month and one year and a fine of between 100,000 riels (USD 24) to two million riels (USD 480).

Article 42 of the Criminal Code is also noteworthy. It indicates that where expressly provided by law and/or statutory instruments, legal entities may be held criminally liable for offences committed on their behalf by

⁶³ Titthara, M. (2016, 9 November). Rainsy Convicted of Defamation. Khmer Times. www.khmertimeskh.com/news/31841/ rainsy-convicted-of-defamation

⁶⁸ CCHR. (2012). An overview of Cambodian laws relating to freedom of expression and a summary of recent case examples to show how laws are used and abused to stifle dissent. cchrcambodia.org/ admin/media/analysis/analysis/english/2012_10_30_CCHR%20 Briefing%20Note%20_%20Cambodian%20laws%20relating%20 to%20freedom%200f%20expression%20and%20recent%20 case%20examples%20-%20ENG.pdf

their organs or representatives. The criminal responsibility of the legal entity does not exclude the criminal responsibility of natural persons for the same acts. This provision is particularly relevant to advocacy NGOs, newspapers and political parties, as individuals accused of an offence can also be held liable, regardless of any charges brought against the legal entity itself.⁶⁹

Incitement to commit felonies or discrimination

Article 495 (Incitement to Commit a Crime) and Article 496 (Incitement to Commit Discrimination), which do not on their face require a crime to actually take place as a result of the incitement in question, constitute unjustified restrictions of freedom of expression. Courts in Cambodia have the tendency to misuse incitement provisions to restrict certain legitimate advocacy activities.⁷⁰

CASE STUDY 1: KONG RAYA

On 15 March 2016, university student Kong Raya was charged with incitement based on a post on his personal Facebook account, which called for a "color revolution in order to change the cheap regime running Cambodian society."⁷¹ He was released on 23 February 2017 after serving an 18-month sentence.

CASE STUDY 2: SENATOR HONG SOK HOUR

On 7 November 2016, after 450 days of pre-trial detention, Senator Hong Sok Hour was convicted of forgery and incitement and sentenced to seven years imprisonment for displaying an allegedly fake border treaty between Cambodia and Vietnam in a video clip posted on the Facebook page of CNRP president Sam Rainsy.⁷² Sam Rainsy, as well as two CNRP staffers who worked on his Facebook page, were convicted of being accomplices the following month.⁷³

- 71 Sony, O., & O'Connel, T. (2016, 16 March). Student Gets 18 Months for Call for 'Color Revolution'. *The Cambodia Daily*. www.cambodiadaily.com/news/ student-gets-18-months-for-call-for-color-revolution-109944
- 72 Chheng, N., & Turton, S. (2016, 8 November). Senator Sok Hour given seven years for forgery and incitement. *The Phnom Pen Post.* www.phnompenhpost.com/national/ senator-sok-hour-given-seven-years-forgery-and-incitement
- 73 Odom, S. (2017, 30 June). Court Upholds Sok Hour, Rainsy Border Treaty Convictions. *The Cambodia Daily*. www.cambodiadaily.com/ news/court-upholds-sok-hour-rainsy-border-treaty-convictions-131973

CASE STUDY 3: UM SAM AN

In October 2016, CNRP Member of Parliament Um Sam An was sentenced to two and a half years in prison for critical comments he made on Facebook about the government's demarcation of the Vietnam-Cambodia border. His comments were considered to constitute incitement.⁷⁴

CASE STUDY 4: SOURN SEREY RATHA

On 13 August 2017, the president of the Khmer Power Party, Sourn Serey Ratha, was arrested after issuing a Facebook post criticising the deployment of Cambodian troops to the Laos border. Sourn Serey Ratha wrote in his post: "The Cambodian children in the army will die horribly on the battlefield, but their commanders will be promoted, collect money and have fun with girls."⁷⁵ On 15 August 2017, Sourn Serey Ratha was detained and charged with inciting soldiers to disobey orders.

CASE STUDY 5: KEM LEY

As stated before, since the murder of the political commentator and activist Kem Ley, several people were arrested and convicted of incitement for accusing the Cambodian government of being responsible for his death. For instance, in July 2017, the anti-terrorism police arrested a woman, Heng Leakhena, for linking Prime Minister Hun Sen and his family to the murder of Kem Ley during a Facebook Live broadcast. The video was made in Kem Ley's childhood home in Takeo province, where a ceremony was held for the first anniversary of the death of Kem Ley.⁷⁶ She was charged with incitement.

⁶⁹ Ibid.

⁷⁰ OHCHR. (2009, 6 October). Comments on certain provisions of the Penal Code in relation to international human rights standards. cambodia.ohchr.org/~cambodiaohchr/sites/default/files/ OHCHR%20Comments%200n%20provisions%200f%20the%20 Penal%20Code,%20En,%20Ott%202009.pdf

⁷⁴ Sovuthy, K. (2016, 11 October). CNRP Lawmaker Guilty of Incitement for Facebook Posts. *The Cambodia Daily*. www.cambodiadaily.com/ news/opposition-lawmaker-sentenced-facebook-posts-119092

⁷⁵ Sokchea, M. (2017, 14 August). KPP head arrested for Facebook post criticising deployment of troops to Laos border. The Phnom Penh Post. www.phnompenhpost.com/national/kpp-headarrested-facebook-post-criticising-deployment-troops-laos-border

⁷⁶ Sokhean, B. (2017, 13 July). Woman Arrested for Linking Hun Sen to Kem Ley Murder. The Cambodia Daily. www.cambodiadaily.com/news/ woman-arrested-for-linking-hun-sen-to-kem-ley-murder-132449

Offences related to judicial decisions and investigations

Articles 522 and 523 criminalise publication of commentaries intending to put pressure on a court and to criticise a court decision, respectively. Article 522 provides that "any publication, prior to the final decision of the court, of any commentaries aiming at putting pressure on the court where a law suit is filed, in order to influence over the decision of the court" is punishable with up to six months imprisonment and a fine of up to one million riels (USD 240). Article 523 provides for the same penalties for "any act of criticizing a letter or a court decision aiming at creating disturbance of public orders or endangering institutions of the Kingdom of Cambodia." These provisions create a real risk that they will be used abusively to harass and punish associations that legitimately seek to analyse, comment on and criticise judicial processes and decisions. In particular, for associations working in the field of human rights and the rule of law, large areas of their work could potentially fall within these vague and broadly drafted provisions, which are neither narrowly defined, transparent, nor easy to understand.

Regulations and guidelines

The Ministry of Culture's 2010 Code of Conduct aims at promoting the "preservation, maintenance of arts, culture, tradition and the identity of the nation" and at preventing "any negative effects of the arts and tradition of the nation."⁷⁷ The most recent version of the Code has 12 guidelines.⁷⁸

The Ministry of Culture's Guidelines on Classification guide the Ministry in determining film ratings and whether or not a movie should be banned. One provision reads: "Movies which display lives of homosexual persons are clearly not in line with social values. Those movies should not promote or encourage homosexuality as appropriate."⁷⁹

77 Soumy, P. (2017, 27 April). Gov't bans actress for a year for violating "Code of Conduct". The Cambodia Daily, www.cambodiadaily.com/news/ govt-bans-actress-for-a-year-for-violating-code-of-conduct-128703

CASE STUDY: DENNY KWAN

In April 2017, the Cambodian actress Denny Kwan, who has more than 300,000 Facebook followers, was banned from appearing in any movie for a year. The Ministry of Culture found her clothes to have violated the 2010 Code of Conduct. She said she had only learned of the ban online.⁸⁰

Summary and conclusion

Certain trends can be identified from the analysis of the different laws involved in the criminalisation of expression online and from their implementation. These trends indicate a common purpose: reducing the scope of the right to freedom of expression in Cambodia.

Deterrence

Laws in Cambodia deter people from exercising their freedom of expression. Two deterrence strategies are recurring:

- *Vague terms:* Laws in Cambodia often use broad and vague terms without defining them. Terms like "national security", "immoral", "public order" and "good customs of society" are subject to subjective and possibly arbitrary interpretation and threaten freedom of expression. Case studies indicate that these vague terms are consistently interpreted broadly and in a discriminatory manner. Such sweeping interpretations in turn deter individuals from exercising their freedom of expression.
- High fines and prison sentences: The exercise of freedom of expression in a way that violates Cambodian laws can lead to heavy fines and prison sentences. With the exception of Article 502 of the Criminal Code (Insult of a Public Official), which provides for a fine from 1,000 riels (USD 0.2) to 100,000 riels (USD 24) and a prison sentence from one to six days, the fines mentioned in this report go from 100,000 riels (USD 24)⁸¹ to 300 million riels (USD 72,000)⁸² and the prison sentences from 10 days⁸³ to 15 years.⁸⁴ With a minimum wage of USD 153/ month in 2017 in Cambodia,⁸⁵ most Cambodians

- 81 See, for example, Articles 93 and 97 of the Law on Telecommunications.
- $82\$ See Articles 80 and 81 of the Law on Telecommunications.
- 83 See Article 525 of the Cambodian Code of Criminal Procedure.
- 84 See Articles 80 and 81 of the Law on Telecommunications.
- 85 tradingeconomics.com/cambodia/minimum-wages

⁷⁸ Sen David, S., & Maza, C. (2016, 28 September). Ministry's code of conduct for artists closer to reality. The Phnom Penh Post. www.phnompenhpost.com/national/ ministrys-code-conduct-artists-closer-reality

⁷⁹ Kijewski, L., & Meta, K. (2017, 9 May). Rules allowing censorship of depictions of homosexuality criticized. The Phnom Penh Post. www.phnompenhpost.com/national/ rules-allowing-censorship-depictions-homosexuality-criticised

⁸⁰ Soumy, P. (2017, 27 April). Op. cit.

would not be able to pay a heavy fine, which could lead to their imprisonment for up to two years according to Article 525 of the Cambodian Code of Criminal Procedure. The severity of this punishment combined with the vagueness of the offences are likely to deter people from exercising their freedom of expression.

Neutrality

The principle of neutrality appears in the LEMNA, the LANGO, the LPP and the Education Law. The neutrality restriction is valid on its face, but its vagueness can lead to abuses. In the name of neutrality, the government could decide to regulate only certain topics or viewpoints. In practice, it can be seen that these provisions are never used in respect of the ruling CPP, but rather they are applied to target opposition parties as well as independent civil society groups, who are painted as pro-opposition by the government.

State control

Having long ago exerted its control over the traditional media, the RGC is progressively extending its control over the internet as well. The Law on Telecommunications contains new surveillance powers for the RGC (embodied by the MPTC), which represent a troubling trend towards suppressing the freedoms of individuals in exchange for an increase in state control. The draft Cybercrime Law would only exacerbate this trend.

State control is becoming the norm. For example, according to a report from July 2017 by the National Police Chief Neth Savoeun at police headquarters in Phnom Penh, the National Police are monitoring Facebook to repress attempts to create a "rebel movement against the government" through negative posts and are working to better control civil society groups that have "opposition trends" and try to cause instability in society.⁸⁶

Targeting of high-profile individuals and human rights defenders

There is little evidence of a desire on the part of the Cambodian government to implement laws which criminalise expression on a systematic basis. Rather, targeted prosecutions of high-profile individuals and human rights defenders are preferred, in order to retain political control and to act as a deterrent for the general public. The government is aware of the prominent role these individuals play in mobilising people against human rights violations. Therefore, it imposes restrictions on freedom of expression to silence its most outspoken critics.

⁸⁶ Dara, M. (2017, 25 July). Cambodia's Facebook crackdown: Police are monitoring site for 'enemies' and 'rebel movements'. *The Phnom Penh Post*. www.phnompenhpost.com/national/ cambodias-facebook-crackdown-police-are-monitoring-siteenemies-and-rebel-movements

Criminal law and freedom of expression on the internet in India

Anja Kovacs and Nayantara R	
Internet Democracy Project	

Introduction

In July 2017, a Muslim man was arrested in the South Indian city of Chennai on charges of sedition, on the basis of WhatsApp messages that he had received on his phone. One of the messages had called on people to protest at Jantar Mantar, New Delhi's officially designated protest site, against those who disrespected the Koran. The man was released after a magistrate found no evidence of anti-national activity or calls for violence.¹

A few weeks later, on 8 August 2017, Indian internet users noticed that the Internet Archive, "a non-profit library of millions of free books, movies, software, music, websites, and more",² was no longer accessible in the country. Two days later, it emerged that internet service providers (ISPs) had taken down the page following a court order. The makers of two Indian films, *Jab Harry Met Sejal* and *Lipstick Under My Burkha*, had requested the court to block the Internet Archive as well as more than 2,600 file-sharing sites, in an effort to stop pirated copies of their films from being watched online.³

By the end of the month, the 47th internet shutdown of 2017 hit India – this time in the northern states of Haryana and Punjab. Mobile internet services were suspended because of growing tensions a day before a special court was to deliver its verdict in a rape case against high-profile godman⁴ Gurmeet Ram Rahim Singh. The shutdown lasted six days. Internet lease lines were suspended in a smaller geographical area.⁵ With four months left to go, India had already seen three times as many internet shutdowns in 2017 as in 2015.⁶

While the internet has often been hailed for its empowering impact on people's ability to express themselves, these incidents, recorded in a span of a mere six weeks, show that this potential can by no means be taken for granted. In India, as elsewhere, freedom of expression online is restricted in a number of ways. Focusing in particular on the criminalisation of freedom of expression but examining other barriers in law and policy as well, this report seeks to outline when and how laws in India are used to curtail the right to freedom of expression on the internet in ways that are overly broad.

The report consists of seven sections. Following this introduction, we will briefly discuss the methodology we have followed in researching and writing this report. For those not familiar with the Indian legal landscape, we will then describe the different types of law that affect the right to free speech and expression on the internet in India. Section four is the heart of this report and examines in detail the laws, policies and case laws that criminalise freedom of expression on the internet in India in ways that are overly broad. In section five, we analyse a number of other important threats to free speech online that further constitute the context in which the criminalisation of freedom of expression on the internet in India has to be understood - from government-mandated content restrictions to mass surveillance. Finally, we briefly highlight draft laws and policies which we believe give cause for concern over future violations of the right to freedom of speech and expression. We conclude the report with a summary and our conclusions.

Karthikeyan, D. (2017, 19 July). Arrest of Muslim Man for Receiving Phone Message Highlights Police Misuse of 'Sedition'. *The Wire*. https://thewire.in/159367/ sedition-whatsapp-chennai-anti-national/

² https://archive.org

³ Kelion, L. (2017, 9 August). Bollywood Blocks the Internet Archive. BBC News. http://www.bbc.com/news/technology-40875528

⁴ Godman is a colloquial term used in India for a type of charismatic guru. https://en.wikipedia.org/wiki/Godman_(India)

⁵ Indo Asian News Service. (2017, 27 August). Haryana, Punjab Suspend Mobile Internet Till Tuesday. NDTV News. http://www.ndtv.com/india-news/ haryana-punjab-suspend-mobile-internet-till-tuesday-1742656

⁶ https://internetshutdowns.in; Pahwa, N. (2017, 28 August). Government of India issues rules for Internet Shutdowns. *Medianama*. https://www.medianama. com/2017/08/223-internet-shutdowns-india

Methodology

To research and write this report, we examined three different types of sources. First, we looked at all the laws and related rules that have an impact on freedom of expression online. Second, we considered case law in higher courts that has had a profound influence on the promotion and protection of the right to freedom of expression in India, including as it relates to the internet, or that has the potential to do so in the future. Finally, we also took into account media reports of charges booked by the police – even if those cases did not eventually result in a conviction – to be able to flag chilling effects, heckler's vetoes,⁷ as well as implementation challenges.

We found that six grounds for restriction, in particular, are being used to criminalise free speech on the internet in ways that are not acceptable. These are defamation; sedition and the use of national symbols; contempt of court; hate speech; morality, obscenity and sexual expression; and intellectual property rights. In addition, we found five other legal and policy challenges relating to freedom of expression on the internet that are crucial to understand the broader landscape of digital censorship in India: government powers to block content; India's intermediary liability regime; the epidemic of network shutdowns in India; concerns around net neutrality; and digital surveillance in India. The substantive analysis of these challenges starts in the fourth section. However, for those not familiar with the Indian legal landscape, we want to first outline the different types of law that affect freedom of expression online in the country.8

Lay of the legal land

Legal foundations

The foundation for the freedom of speech and expression in India lies in Article 19(1)(a) of the Constitution of India, which states that all citizens shall have the right to freedom of speech and expression.

It was explicitly held in Secretary, Ministry of Information and Broadcasting, Government of India v. Cricket Association of Bengal⁹ that the right to freedom of speech and expression includes the right to impart and receive information via electronic media. Article 19(2) lays down exceptions to this fundamental right. This sub-section identifies certain heads under which there may be reasonable restrictions to the freedom of speech and expression: the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.

Laws that restrict freedom of speech and expression must be reasonable and fall within the contours of the subject matters listed in Article 19(2). Any legislation dealing with speech and expression on the internet can be challenged on the ground that it goes beyond the exceptions laid down in Article 19(2) of the Constitution.

Along with the right to equality (Article 14) and the right to life (Article 21), Article 19 forms the foundation for liberty and equality under the Constitution.

India's obligations towards the right to freedom of speech and expression also stem from being a signatory to the Universal Declaration of Human rights and the International Covenant on Civil and Political Rights (ICCPR).

The legislations that cover penal procedure and substantive law are the Code of Criminal Procedure, 1973, and the Indian Penal Code, 1860. The latter is a relic from the colonial period. These legislations continue to be used to book cases relating to speech on the internet as well.

Governance of online and networked spaces

Apart from the penal codes, the Information Technology Act, 2000 and the Amendment Act of 2008, as well as the rules framed under the Act, are other importants bases for the governance of electronic media, and consequently, for the criminalisation of speech and expression online.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, governs India's unique identity number project, which relies heavily on digital infrastructure and has ramifications not only for the right to privacy, but also for the right to freedom of speech and expression.

Legislations such as the Protection of Children from Sexual Offences Act, 2012, also specifically prohibit some forms of speech and expression on the internet. Other legislations, like the Contempt of Courts Act, 1971, the Prevention of Insults to National Honour Act, 1971, the Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989, and the Pre-Conception and Pre-Natal

⁷ In the strict legal sense, a heckler's veto occurs when the speaker's right is curtailed or restricted by the government in order to prevent a reacting party's behaviour. https://en.wikipedia.org/ wiki/Heckler%27s_veto

⁸ Our outline of the Indian legal landscape draws on the five-category framework of laws and regulations that affect online freedom of expression, developed by SMEX.

⁹ Government of India v. Cricket Association of Bengal. 1995 AIR 1236.

Diagnostic Techniques (Regulation and Prevention of Misuse) Act, 1994, do not specifically pertain to speech on electronic media, but they prohibit certain kinds of speech and are used to book charges against speech and expression on the internet as well.

Laws and policies on infrastructure

The Telecom Regulatory Authority of India (TRAI), established by the Telecom Regulatory Authority of India Act, 1997, has powers to regulate the telecommunications sector, with the mandate of protecting the interests of service providers and telecom subscribers while ensuring orderly growth of the sector. We will examine the connections between regulation of one aspect of this debate, that of network neutrality, and the right to freedom of speech and expression. Network neutrality is the principle that the internet is maintained as an open network, where network operators do not discriminate on the basis of origin or destination of traffic. Preserving network neutrality is central to making sure that the internet's potential of being a medium where freedom of speech and expression thrives can be realised.

Other laws

Laws on intellectual property rights (IPR) aim to strike a balance between protecting ownership and property rights, on the one hand, and not infringing on free speech, on the other. In copyright law, for example, fair use exceptions are forwarded as speech protecting where the public good is greater than the value derived from individual benefits of intellectual property. In the section on IPR, we look at the unique challenges that Indian laws on IPR pose to freedom of speech and expression.

Draft laws

Finally, a number of key bills and draft policies have been proposed on content and infrastructure regulation of electronic media which affect freedom of speech and expression. These include the Draft Prohibition of Indecent Representation of Women and Children Bill, 2012, the Draft Geospatial Information Regulation Bill, 2016, the Draft National Encryption Policy, 2015, and a forthcoming draft data protection policy. New provisions to address hate speech have been proposed as well, including to fill alleged gaps in the law that have emerged after the Supreme Court struck down as unconstitutional section 66A of the IT Act in 2015.¹⁰

Criminalisation of online freedom of expression

Because of their far-reaching consequences for the speaker, criminal charges to restrict speech and expression can be a powerful tool of censorship.

Between 2009 and 2015, one provision of Indian law in particular became notorious for its chilling effect on freedom of expression online. Section 66A of the IT (Amendment) Act, 2008, provided for punishments for messages that were "grossly offensive", had a "menacing character" or were sent "for the purpose of causing annoyance or inconvenience," among other overly broad grounds. Following a slew of high-profile cases that involved abuse of the section, the provision's constitutionality was challenged in *Shreya Singhal v. Union of India.*¹¹ On 24 March 2015, the Supreme Court of India ruled that section 66A IT Act was "violative of Article 19(1) (a)" and could not be saved under Article 19(2), and struck down the provision in its entirety.

For those concerned with freedom of expression online in India, the verdict provided tremendous relief. But many challenges remain. For one thing, even following the Supreme Court's ruling, section 66A IT Act continues to be invoked by the police and lower courts.¹² In addition, freedom of expression online continues to be threatened through criminalisation in other ways that are not acceptable, on six grounds in particular: criminal defamation; sedition and the use of national symbols; contempt of court; hate speech; morality, obscenity and expressions of sexuality; and intellectual property rights.

What connects these different challenges is the deep influence of a concern for law and order in free speech jurisprudence in India. In particular, in *State of U.P. v. Lalai Singh Yadav*,¹³ the Supreme Court upheld "ordered security" as a constitutional value, ensuring that where free speech and public order seem to clash, the latter is given precedence. Though there have been dissenting voices, this remains the dominant strand in free speech jurisprudence to this day and has led to a situation where, rather than the government having to ensure an environment in which everyone can speak freely, those who are speaking are expected to exercise

¹¹ AIR 2015 SC 1523.

¹² Mareedu, M. (2017, 8 April). Local court invokes annulled Sec 66A to convict a man. New Indian Express. www.newindianexpress. com/states/telangana/2017/apr/08/local-court-invokesannulled-sec-66a-to-convict-a-man-1591308.html; Jha, A. (2016, 1 September). 2,000 Arrests In 12 Months, 3,000 In Just 3? How Cops Use 66A Even After SC Scrapped It. Youth Ki Awaaz. https://www. youthkiawaaz.com/2016/09/66a-it-act-ncrb-crime-statistics

¹⁰ Shreya Singhal v. Union of India. AIR 2015 SC 1523.

¹³ AIR 1977 SC 202.

caution lest anyone gets outraged. Even truth is not accorded the same value as order. $^{\rm 14}$

In what follows, we examine relevant laws, case law and cases for each of the grounds mentioned above in detail. It is against the background of the precedence of order over speech that these analyses have to be read.

Defamation

Both civil and criminal remedies exist in Indian law for someone aggrieved of defamation, one of the eight exceptions to Article 19(1)(a) mentioned in the Constitution. Under the un-codified civil law remedy, one can obtain injunctive orders and/or claim damages for the publication of allegedly defamatory material. The criminal remedy to defamation, codified in sections 499 and 500 of the Indian Penal Code (IPC), punishes the crime with imprisonment and fines. Depending on the outcome desired, parties file for either a civil or criminal remedy, or for both. What is common among the two types of remedies is that they are routinely used by powerful players to strong-arm critics into silence.

The civil remedy is often used to obtain injunctive orders in the absence of respondents to the case, in addition to huge sums of money, as damages. Most recently, Baba Ramdev, a godman, politician and businessman, got an ex parte injunction against Juggernaut publishers, Flipkart and Amazon, stopping them from distributing a biography of him by Priyanka Pathak-Narain, on the grounds of it being defamatory.15 In another recent case, Member of Parliament Rajeev Chandrashekhar was seeking to prevent online news media outlet The Wire from publishing two stories about him that had a very clear public interest angle.¹⁶ The City Civil Court of Bangalore passed an ex parte order for temporary injunction against publication of the two articles, which highlighted the conflicts of interest between the political roles Chandrashekhar holds, on the one hand, and his investments in defence manufacturing firms and the news media outlet Republic TV, on the other. There are numerous such instances of ex parte injunctions that have been obtained in order to silence the publishing of material on the internet as well as in print media.¹⁷

The criminal remedy is especially useful for purposes of intimidation by politicians, actors, corporations and other powerful entities, as the offence is punishable with jail time and not just payment of monetary damages. The offence is bailable, non-cognisable and compoundable.

Sections 499 and 500 read as follows:18

499. Defamation. —

Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.

Explanation 1.—It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives. Explanation 2.—It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such. Explanation 3.—An imputation in the form of an alternative or expressed ironically, may amount to defamation.

Explanation 4.—No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful.

500. Punishment for defamation. --

Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.

The asymmetry of power between those who bring the charges and those who are charged for defamatory speech on the internet is frequently steep in

¹⁴ Law Commission of India. (2017). Report 267 Hate Speech. New Delhi: Law Commission. www.lawcomssionofindia.nic.in/reports/ Report267.pdf; Narrain, S. (2016). Hate Speech, Hurt Sentiment, and the (Im)Possibility of Free Speech. Economic and Political Weekly, 51(17). http://www.epw.in/journal/2016/17/specialarticles/hate-speech-hurt-sentiment-and-impossibility-freespeech.html

¹⁵ IANS. (2017, 11 August). Juggernaut restrained from distributing book on Ramdev, says will appeal. *Indian Express*. www. indianexpress.com/article/india/juggernaut-restrained-fromdistributing-book-on-ramdev-says-will-appeal-4792196

¹⁶ Scroll. (2017, 7 March). In highly unusual move, Bengaluru court orders The Wire to remove articles on Rajeev Chandrasekhar. *Scroll.* www.scroll.in/article/831159/in-highly-unusual-movebengaluru-court-orders-the-wire-to-remove-articles-on-rajeevchandrasekhar

¹⁷ Scroll. (2017, 17 October). 'Attempt to gag': The Wire criticises injunction against it in Jay Shah defamation case. *Scroll*. https:// scroll.in/latest/854371/attempt-to-gag-the-wire-criticisesinjunction-against-it-in-jay-shah-defamation-case

¹⁸ The illustrations and exceptions text in the section have not been included, in the interest of space.

the case of criminal defamation charges as well. For example, the Adani group issued a legal notice for criminal and civil defamation against media house The Wire for republishing an article that originally appeared in Economic and Political Weekly (EPW), titled "Modi Government's 500 Crore Bonanza to Adani Group Company", in June 2017. EPW also received a similar legal notice a few days later, in July. Bollywood actor Aamir Khan filed a defamation suit against a person for making comments against the actor's show Satvameva Javate on social media.¹⁹ And in another exemplary case of intimidation, a law student received a legal notice for charges of criminal and civil defamation for publishing a blog post on ongoing trademark litigation between the Financial Times Ltd. and Times of India.²⁰ Ironically, a media house was on the other side of the fence, issuing the legal notice.

A batch of petitions, including most prominently those by politicians Arvind Kejriwal, Subramanian Swamy and Rahul Gandhi, challenged the constitutionality of criminal defamation in the Supreme Court. The petitions contended that sections 499 and 500 IPC, and section 199(1) to 199(4) of the Code of Criminal Procedure, which lay down the procedure for prosecution for defamation, go beyond the reasonable restrictions to the right to freedom of speech and expression under Article 19(2). The petitions also held that the civil remedy of defamation is sufficient for safeguarding the right to reputation under Article 21 of the Constitution. In a case known by the name of one of the petitions, Subramaniam *Swamy v. Union of India*,²¹ the Supreme Court took up these petitions together to decide on the constitutionality of the criminal defamation provisions.

That the criminal remedy goes beyond the "reasonable" restrictions under Article 19(2) was argued on many grounds, which often sought to differentiate the criminal remedy from the civil remedy.²² For example, in contrast to the civil remedy, the criminal remedy involves the complainant bearing little costs, as state resources are spent on prosecuting the accused, to protect individual rights. This leads to greater chances of frivolous complaints being filed. In addition, the burden placed on the accused and the criminal nature of the complaint allows for harassment at the hands of the persons filing charges.

Ruling on the petitions, the Supreme Court of India paid lip service to the fundamental right to freedom of speech and expression and international covenants – before deciding that the sections were indeed not unconstitutional. Going against a global push away from criminal remedies for defamation, the Court ruled that there was a need to balance the right to reputation, which is part of the fundamental right to life, and therefore, the remedy of criminal defamation was a *reasonable* restriction under Article 19(2). This judgment of the Supreme Court received flak from many commentators for its regressiveness in free speech jurisprudence, for being needlessly wordy, and for not engaging satisfactorily with the arguments of petitioners.²³

Criminal defamation and publication on the internet

If the petitioners sought to distinguish the criminal from the civil remedy in *Subramaniam Swamy v. Union of India*, so, reportedly, did the Ministry of Home Affairs, albeit for a different reason: according to a news report, the Ministry submitted to the Supreme Court that because of the emergence of new technology, the criminal remedy is, in fact, required:²⁴

Civil remedy for defamation is not efficacious remedy per se. The civil remedies on an average take longer than criminal remedies. Furthermore, with the advent of new forms of technology, acts like online defamation cannot be adequately countered by means of civil remedies.

It is unclear on what grounds the government sought to create a distinction between "online defamation" and its print or broadcast counterpart. The ease of publication, the speed of transmission of statements, along with its duplicability seems to be the implicit basis for the distinction. However, this argument begs the question: are restrictions to free speech then to be higher for print media outlets that have a digital edition?

¹⁹ India Today. (2014, 19 April). Retired merchant navy officer Ajit Vadakayil arrested for defaming actor Aamir Khan. India Today. http://indiatoday.intoday.in/story/aamir-khan-man-held-fromkarnataka-for-defaming-actor-aamir-khan/1/356626.html

²⁰ Reddy, P. (2013, 21 May). The Times Publishing House threatens to sue our blogger for alleged defamation – we ain't going down without a fight! *Spicy IP*. https://spicyip.com/2013/05/the-timespublishing-house-threatens-to.html

²¹ WP (Crl) 184 of 2014.

²² Thomas, A. L. (2016, 27 May). Subramanian Swamy v. UoI: Unanswered Arguments. *Legally India*. https://www.legallyindia. com/blogs/subramanian-swamy-v-uoi-unanswered-arguments

²³ Acharya, B. (2016, 14 May). Criminal Defamation and the Supreme Court's Loss of Reputation. *The Wire*. https://www.thewire.in/36169/ criminal-defamation-and-the-supreme-courts-loss-of-reputation

²⁴ Mishra, P. (2015, 12 July). Online defamation cannot be countered by civil remedies, Centre tells Supreme Court. DNA News. http:// www.dnaindia.com/india/report-online-defamation-cannot-becountered-by-civil-remedies-centre-tells-supreme-court-2103811

Whether "new forms of technology" merit different treatment or not is not further discussed in the order of the Court in Subramaniam Swamy v. Union of India. However, the same court in 2009 had made statements that indicated that defamation on the internet had different effects, and therefore merited harsher consequences. In that case, a 19-year-old blogger was arrested for creating a group ("community") on social media site Orkut, that was allegedly defamatory to the political party Shiv Sena. The Supreme Court refused to quash the criminal proceedings against the boy and argued that restrictions to free speech on the internet should be higher. The judge noted that "any blogger posting material on the web should be aware of the reach of the internet and hence also be willing to face the consequences of such action."25

In a 2010 civil defamation suit, *Tata Sons Limited*. v. *Greenpeace International & Anr.*,²⁶ the Supreme Court made slightly different observations as to when it would be relevant that the publication of allegedly defamatory statement is made on the internet.

In this case, the petitioners moved the Court for a permanent injunction against Greenpeace along with damages for defamation under the civil remedy and trademark infringement. The facts of the case were that Tata Sons Limited was suing Greenpeace International, a not-for-profit organisation, for releasing a videogame through which it sought to publicise the harms that Tata Sons' business ventures would wreak on endangered olive ridley turtles.

The creators of the game defended their actions on the grounds of freedom of speech and exceptions under section 29(4) of the Trade Marks Act, 1999, which allows for the use of a trademark for criticism, fair comment and parody if it is with due cause. The Tata Group prayed for an injunction on the grounds that, as the "publication" happened on the internet, the likelihood of injury was greater if the injunction were refused, and that this should be a consideration for the court as it balanced convenience and irreparable hardship. According to the Tata Group, the damage to its reputation was "continuing and spreading every minute that the game stays online," and as a result, an injunction should be granted.

The Court ruled, however, that the nature of the medium of the internet may only be a consideration in assessment of damages. The Court held that the

term "publication" encompassed all forms and mediums, including the internet:

That an internet publication has wider viewership, or a degree of permanence, and greater accessibility, than other fixed (as opposed to intangible) mediums of expression does not alter the essential part, i.e. that it is a forum or medium.

In discussing the Canadian case relied upon by the petitioners, the Court drew attention to the detail that even in that case, a different standard for libel was not mooted for publication on the internet, and "suspected" that such a distinction (between the internet and other forms of publication) is not constitutionally sanctioned:

Formulating and adopting any other approach would result in disturbing the balance between free speech and the interest of any individual or corporate body in restraining another from discussing matters of concern, so finely woven in the texture of the Bonnard ruling.

Publication and republication in the digital age

Another matter to consider in the age of the internet is what constitutes "making or publishing imputations". According to section 499 of the IPC, the offence of criminal defamation would be committed if one "makes or publishes any imputation concerning any person [...] to defame that person."

Union Minister Arun Jaitley filed a criminal defamation complaint in December 2015 against the Chief Minister of Delhi, Arvind Kejriwal, for publishing a tweet that Jaitley alleges to be defamatory. He also arraigned a number of others who retweeted Kejriwal's original tweet, including the Aam Aadmi Party's Raghav Chaddha. Chaddha approached the Supreme Court to seek a direction that a retweet cannot form the basis of a criminal prosecution. The Supreme Court has directed the Delhi High Court to look into the matter. As noted by Devika Agarwal,²⁷ republishing a defamatory article constitutes defamation according to interpretation by Indian courts.²⁸ It remains to be seen whether a retweet will be considered as "publishing" by the Delhi High Court.

In the case of *Khawar Butt v. Asif Nazir Mir*²⁹ the plaintiffs instituted a civil suit for defamation

²⁵ Liang, L. (2009, 25 February). Bloggers and Defamation. Kafila. http://www.kafila.online/2009/02/25/bloggers-and-defamation

²⁶ CS(OS) 1407/2010.

²⁷ Agarwal, D. (2017, 25 September). Arun Jaitley's suit against AAP's Raghav Chadha: Does republishing of defamatory content amount to 'defamation'? *FirstPost*. www.firstpost.com/politics/ arun-jaitleys-suit-againt-aaps-raghav-chadha-does-republishingof-defamatory-content-amount-to-defamation-4058989.html

²⁸ Re: EVK Sampath, AIR 1961 Mad 318.

²⁹ CS (OS) 290/2010.

for republishing print material on Facebook. The question before the Delhi High Court was whether republication on the internet constituted a fresh offence, and whether the limitation period would begin afresh with the republishing. Arguing that the post on Facebook qualified as a fresh offence, and the suit cannot be barred by limitation, the plaintiffs sought to distinguish the internet as a medium from print on the ground that "a publication on a website can voluntarily be withdrawn by the publisher, unlike publication in print media, which, once published cannot be withdrawn."

This is only true, however, in so far as it does not consider archived versions of many websites. The Delhi High Court held against the plaintiffs, by holding against the Multiple Publication Rule:

I am of the view that the Single Publication Rule is more appropriate and pragmatic to apply, rather the Multiple Publication Rule. I find the reasoning adopted by the American Courts in this regard to be more appealing than the one adopted by the English Courts, prior to the amendment of the law by the introduction of the Defamation Act, 2013. It is the policy of the law of limitation to bar the remedy beyond the prescribed period. That legislative policy would stand defeated if the mere continued residing of the defamatory material or article on the website were to give a continuous cause of action to the plaintiff to sue for defamation/libel. Of course, if there is re-publication resorted to by the defendant-with a view to reach the different or larger section of the public in respect of the defamatory article or material, it would give rise to a fresh cause of action.

If the Court would not have held in favour of the Single Publication Rule, it would have been possible for a plaintiff to sue for every "hit" of the webpage.

Free speech online and the truth defence

One of the main issues with criminal defamation has been the burden placed on the accused, as truth is not a defence in itself without the accompanying requirement, noted in exception 1, of being in the public interest. This disproportionate burden creates a massive chilling effect on speech and expression on the internet. As noted by Shehla Rashid Shora and Anja Kovacs, explanation 2 to section 499, for example, could arguably be drawn on to penalise the authors of bad reviews given to products or services on the internet.³⁰ In the age of e-commerce and internet-mediated service delivery, such provisions can prove to be highly problematic for citizen journalists who, using only a cell phone and an internet connection, seek to expose shady business practices.

This is particularly noteworthy as corporations continue to be able to file complaints of criminal defamation. In 2014, Mahan Coal Limited, a corporation, filed a complaint against environmental rights campaigner Priya Pillai for allegedly defamatory remarks made by her.³¹ Her comments in a blog post questioning the speedy clearance of projects by the environment minister, benefitting corporations like the Essar Group at the expense of the forests, people and wildlife, were among the things that irked Mahal Coal Limited, a company promoted by ventures of the Essar Group.

Pillai filed a petition challenging the provisions of criminal defamation, along with challenging the ability of corporations to file criminal defamation complaints. The Supreme Court in *Subramaniam Swamy v. Union of India* locates the right to reputation under the right to life and personal liberty in Article 21, which is not a right available to corporations. Yet, a two-judge bench of the Supreme Court disposed of Pillai's petition, in the aftermath of the judgment in *Subramaniam Swamy v. Union of India*, saying nothing remained to be discussed.

Looking forward

In response to the misuse of the section by powerful actors to intimidate and chill free speech, the Supreme Court in *Subramaniam Swamy v. Union of India* unfortunately held that "an abuse of process or the potential for abuse of a law is no ground for repealing the law itself." As noted by Lawrence Liang, a solution to eliminating maliciousness may be to use more frequently the power of the courts under Section 250 of the Criminal Procedure Code, which provides for "compensation for accusation without reasonable cause."³²

A private member's bill has been presented to the Parliament by Member of Parliament Tathagatha Satpathy to repeal provisions on criminal defamation and codify the civil remedy to defamation.³³ It would be heartening if the Parliament ups its record of standing up for free speech, as the Supreme Court has in this instance failed to uphold citizens' rights.

³¹ Parthasarathy, S. (2016, 1 November). Blocked Out. Caravan Magazine. www.caravanmagazine.in/perspectives/ blocked-out-corporations-defamation

³² Liang, L. (2009, 25 February). Op. cit.

³³ See https://speechbill.in

Sedition and national symbols

Section 124A of the IPC concerns sedition: Section 124A.—

Whoever, by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Government established by law in India, shall be punished with imprisonment for life, to which fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine.

Explanation 1.—The expression "disaffection" includes disloyalty and all feelings of enmity.

Explanation 2.—Comments expressing disapprobation of the measures of the Government with a view to obtain their alteration by lawful means, without exciting or attempting to excite hatred, contempt or disaffection, do not constitute an offence under this section.

Explanation 3.—Comments expressing disapprobation of the administrative or other action of the Government without exciting or attempting to excite hatred, contempt or disaffection, do not constitute an offence under this section.

The colonial origins of Indian sedition law, its role in the independence struggles and its chequered history in the post-independence era are all well recorded.³⁴ In the last few decades, there has been strong speech-protecting jurisprudence in the courts when it comes to interpretation of the provisions on sedition: the objective criteria of "incitement"³⁵ to "imminent"³⁶ "violence" are required to be present for any speech to be curtailed. However, in practice, especially on the internet, we see a stark difference between law and implementation where sedition is concerned. Several trends deserve to be highlighted.

First, all too often the police book charges of sedition for speech and expression on the internet that very obviously does not meet the criteria under the section. For example, as mentioned earlier, according to news reports a man in Chennai was booked under section 124A for receiving an "anti-national" message on WhatsApp.³⁷ The alleged "anti-national" message was a voice note in Urdu, calling for a protest, but was nowhere close to inciting violence, let alone imminently. In Badaun, an individual was arrested for posting the caption "I love Pakistan" along with his picture.³⁸ Even a former judge of the Supreme Court has not been spared: Justice Markandey Katju was booked for sedition under section 124A for saying in a Facebook post that Pakistan can take Kashmir if it agrees to take Bihar too.³⁹

Second, phrases that gain currency on social media and subsequently in wider parlance, but that have no legal standing, become an informal lexicon to justify sedition charges. For example, "anti-national", which is neither a category defined under the section of sedition nor punishable under any legislative provision, is a term often used to refer to persons ostensibly liable for sedition, and is frequently bandied about in the filing of charges. Thus, in August 2016, a man was arrested and remained in judicial custody for several days for "liking, sharing and forwarding anti-India posts" on Facebook. The first information report (FIR)⁴⁰ reads:

An anti-national post, in which India is represented as a mouse swept away by a broom, has been brought to notice. [It] asks for freedom for Kashmiris and has the flags of Pakistan and China. It is shown that some people have black flags and black bands across their faces and are asking for Kashmir's freedom.⁴¹

Third, there have been cases in which electronic media evidence was manipulated to make a case for sedition. For example, students of Jawaharlal Nehru University (JNU), New Delhi, were arrested for allegedly shouting slogans considered seditious during a protest meeting to mark the anniversary of the death of a separatist leader who was hanged. A

³⁴ Dev, A. (2016, 25 February). A History of the Infamous Section 124A. The Caravan. www.caravanmagazine.in/vantage/section-124a-sedition-jnu-protests; Liang, L. (2016. 13 February). A Short Summary of the Law of Sedition in India. The Wire. https://www. thewire.in/21472/a-short-summary-of-the-law-of-sedition-in-india

³⁵ Shreya Singhal v. Union of India. AIR 2015 SC 1523.

³⁶ Arup Bhuyan v. State of Assam. (2011) 3 SCC 377.

³⁷ Pathak, P. (2017, 20 July). Chennai man arrested for receiving anti-national WhatsApp message. Yes, for receiving it. *India Today*. www.indiatoday.in/technology/story/chennai-manarrested-for-receiving-anti-national-whatsapp-message-yes-forreceiving-it/1/1005622.html

³⁸ Press Trust of India. (2017, 8 August). Badaun man booked for sedition for his 'I support Pakistan' Facebook post. *Times Now*. www.timesnownews.com/india/article/badaun-man-booked-forsedition-for-his-i-support-pakistan-facebook-post/70657

³⁹ The Wire. (2016, 28 September). Markandey Katju Faces Sedition Charge for Facebook Post about Bihar. The Wire. https://thewire. in/69547/markandey-katju-faces-sedition-charge-for-facebookpost-about-bihar/

⁴⁰ In criminal law, the first information report (FIR) is a report that provides information first in point of time about a crime. https:// www.lawnotes.in/First_Information_Report

⁴¹ Ghose, D. (2016, 6 August) Kashmiri held for sedition: Chhattisgarh cops probe who made 'anti-India' FB post. *Indian Express*. www. indianexpress.com/article/india/india-news-india/kashmiri-heldfor-sedition-chhattisgarh-cops-probe-who-made-anti-india-fbpost-2956483

forensic probe later found that two of the seven videos on the basis of which arrests were made were in fact doctored.⁴² In a separate incident of arrest of college students on charges of sedition, the Metropolitan Magistrate hearing the case said that the authenticity of the videos should be determined before the filing of an FIR.⁴³

But even if the contents of the videos of the JNU protests were known to be true, the speech in question would still not qualify as seditious.⁴⁴ It is established law in *Balwant Singh v. State of Punjab*⁴⁵ that raising separatist slogans once or twice by a few individuals does not amount to exciting or aiming to excite hatred or disaffection towards the government. In the landmark judgment of *Shreya Singhal v. Union of India*, the Supreme Court required that one differentiate between "advocacy" and "incitement" of violence, and that only the latter is punishable. Yet, across the country, public opinion continues to be mobilised around such doctored videos and police continue to book charges and arrest persons for the most innocuous of speech.

The misapplication of the section does not stop with the arrest of those making the speech, but bizarrely, extends even to those receiving it. For example, a WhatsApp group administrator was arrested in Karnataka for receiving a message insulting the prime minister.⁴⁶ Or in some cases, charges are brought against "unknown persons": Haryana police filed an FIR against "unknown persons" for a message shared on WhatsApp on the topic of the Jat agitation, which was "provoking".⁴⁷

It is common for the sedition provision to be used in conjunction with the Prevention of Insults to National Honour Act, 1971, to arrest persons even when no offences are made out. Section 2 of the Prevention of Insults to National Honour Act, 1971 states that:

Whoever in any public place or in any other place within public view burns, mutilates, defaces, defiles, disfigures, destroys, tramples upon or otherwise shows disrespect to or brings into contempt (whether by words, either spoken or written, or by acts) the Indian National Flag or the Constitution of India or any part thereof, shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.

Thus, a student was arrested in Kerala for altering the lyrics of the national anthem in a Facebook post and "insulting" India, in addition to refusing to stand up for the national anthem.⁴⁸ Another man, a writer, was taken into custody for a similar charge of showing disrespect to the national anthem in his book and in a Facebook post, in December 2016 – he was booked for sedition.⁴⁹ In an atmosphere of heightened performative nationalism, these legislations are seeing more use to target political speech on social media.

Common Cause, a not-for-profit organisation, observing widespread misuse of the sedition section, filed a writ petition in the Supreme Court.⁵⁰ The petition notes that according to the National Crime Records Bureau (NCRB) Report, 2014, 47 sedition cases were reported in the year across nine states; many of these cases did not satisfy the prerequisite of incitement of violence. Of the 58 people arrested for sedition, only one person was convicted. The figures continue to be similarly abysmal for 2015, the last year for which NCRB data is available as of the time of writing. Responding to a question raised in the Lok Sabha, the government said that 35 cases of sedition were registered across the country in 2016.⁵¹

The petition filed by Common Cause asked for the issuance of an appropriate writ, order or direction requiring certification from the Director General of Police or Commissioner of Police that the alleged seditious act either led to incitement of violence or had the tendency or intention to create public disorder, before the filing of an FIR. The Court issued an order that criticism against the government does not constitute sedition, but did not see it "necessary" to issue more specific directions.⁵²

⁴² Das, B. (2016, 19 February). Forensic experts say Kanhaiya video was doctored. *IndiaToday*. www.indiatoday.intoday.in/story/ forensic-experts-say-kanhaiya-video-was-doctored/1/600808.html

⁴³ Press Trust of India. (2017, 29 August). Ramjas College Ruckus: Can't Press Sedition on Basis of Unathenticated Videos, Says Delhi Court. News 18. www.news18.com/news/india/ramjas-ruckuscant-press-sedition-on-basis-of-unathenticated-videos-sayscourt-1504375.html

⁴⁴ Ibid.

^{45 1995 (1)} SCR 411.

⁴⁶ Express News Service. (2017, 3 May) Karnataka: WhatsApp group admin in jail over PM Narendra Modi post. *Indian Express.* www. indianexpress.com/article/india/karnataka-whatsapp-groupadmin-in-jail-over-pm-narendra-modi-post-4638071/

⁴⁷ Narrain, S., & Seshu, G. (2016, 19 August). Sedition goes viral. The Hoot. http://www.thehoot.org/free-speech/media-freedom/ sedition-goes-viral-9578

⁴⁸ The Hindu. (2014, 21 August). Insult to national anthem: Youth held. The Hindu. www.thehindu.com/todays-paper/tp-national/tpkerala/insult-to-national-anthem-youth-held/article6336783.ece

⁴⁹ Hindustan Times. (2016, 19 December). Kerala writer Chavara, held for 'insulting national anthem', on fast. *Hindustan Times*. www.hindustantimes.com/india-news/arrested-keralawriter-on-fast-seeking-withdrawal-of-sedition-case/story-7Uap5YaSugKiuY6VTdtmSO.html

⁵⁰ Common Cause and Anr. v. Union of India. WP (Civil) 683 of 2016.

⁵¹ Press Trust of India. (2017, 1 August). 35 sedition cases registered in 2016, govt tells Lok Sabha. *Hindustan Times*. http://www. hindustantimes.com/india-news/35-sedition-cases-registered-in-2016-govt-tells-lok-sabha/story-k5HUAkOZOHSYNCA30Z5A2H.html

⁵² Venkatesan, J. (2016, 5 September). Supreme Court Warns Police That Criticism of Government Is Not Sedition. *The Wire*. https:// thewire.in/64281/criticism-of-government-does-not-constitutesedition-says-supreme-court

Contempt of court

Contempt of court is one of the exceptions mentioned in Article 19(2) of the Constitution. The Contempt of Courts Act, 1971, is the legislation which details what may be considered an offence. The civil offence of contempt is defined in section 2(b) as "wilful disobedience to any judgment, decree, direction, order, writ or other process of a court or wilful breach of an undertaking given to a court."

The criminal offence of contempt is defined in section 2(c) as:

The publication (whether by words, spoken or written, or by signs, or by visible representation, or otherwise) of any matter or the doing of any other act whatsoever which

(i) scandalises or tends to scandalise, or lowers or tends to lower the authority of, any court; or(ii) prejudices, or interferes or tends to interfere with, the due course of any judicial proceeding; or

(iii) interferes or tends to interfere with, or obstructs or tends to obstruct, the administration of justice in any other manner.

Cases on contempt of court related to the internet are mostly filed under the criminal offence section. as the civil offence pertains to simple wilful disobedience towards a specific direction given by a court. As pointed out by constitutional scholar Gautam Bhatia,53 the section on the criminal offence of contempt can be interpreted either to mean that subsections (i), (ii) and (iii) have to be fulfilled, or that if merely sub-section (i) is fulfilled, the offence is made out. The court has over the years favoured the latter interpretation. There is no requirement that such scandalising or tendency to scandalise has to prejudice, interfere with or obstruct the administration of justice. The court has also not provided any guidelines to determine what constitutes scandalising the courts.

This has led to charges being filed for, among others, content that is criticism of judgment. For example, a man was sentenced to a month's jail time for "not only making scandalous statements against the judiciary, but also posting them on social networking websites"⁵⁴ – as if the latter action compounds the offence. In this case, the accused had simply made statements to the effect that he had lost faith in the judiciary, after a dispute over real estate was not working out in his favour. Similarly, a notice of contempt was sent to a former judge of the Supreme Court, Justice Katju, after he criticised the Supreme Court for its judgment on a case of rape and murder. The charges against the former judge were dropped after he delivered an apology.⁵⁵ In February 2017, the Bombay High Court issued a suo moto order against comments made by a person in a Facebook post against the court's order banning cell phones within the courtroom.⁵⁶ This is criticism of a policy of the Court which has implications for access to judicial process and, arguably, to justice.

Parody is affected as well. For example, "Bombay High Court" is a parody account on Facebook, offering a humorous take on goings-on in the Court. The creator of this account is reported to have been threatened for contempt.⁵⁷ According to a news report, the Ministry of Law and Justice similarly forwarded a complaint about certain Facebook pages to the Secretary General of the Supreme Court and the Registrar General of the Delhi High Court, with a request to take "further appropriate action". The complaint concerned satirical pages carrying the names of the Supreme Court and Delhi High Court: the pages were allegedly posting defamatory and contemptuous content that showed the judges and the judiciary in a poor light.⁵⁸

In still another instance, the Bombay High Court, in response to a petition filed by the Bombay Bar Association and the Advocates Association of Western India, ordered the takedown of videos of court proceedings on YouTube and directed YouTube to not allow such content to be posted.⁵⁹ This raises issues of intermediary liability, apart from whether criticism of the court's orders itself is enough to "scandalise" a court.

⁵³ Bhatia, G. (2016). Offend, Shock, or Disturb. Free Speech under the Indian Constitution. New Delhi: Oxford University Press.

⁵⁴ Mumbai Mirror. (2014, 2 December). Man gets one month in jail for contempt of court. *Mumbai Mirror*. www.mumbaimirror.indiatimes. com/mumbai/crime//articleshow/45342096.cms

⁵⁵ Indian Express. (2017, 6 January). Supreme Court accepts Justice Markandey Katju's apology, closes contempt proceedings. Indian Express. www.indianexpress.com/article/india/justice-markandeykatju-tenders-unconditional-apology-to-supreme-court-4461887

⁵⁶ Chaudhari, K. (2016, 23 February). Facebook may face contempt motion in case on secretly shot Bombay high court video. *Hindustan Times*. www.hindustantimes.com/mumbai-news/ facebook-may-face-contempt-motion-in-case-on-secretly-shotbombay-high-court-video/story-vhuYUU2oQSBYUSzlhkQ2JK.html

⁵⁷ Shukla, A. (2016, 31 December). Meet the man behind 'Bombay High Court' parody account on Facebook. *Midday*. www.mid-day. com/articles/meet-man-behind-bombay-high-court-parodyaccount-on-facebook-mumbai-news/17873159

⁵⁸ Nair, H. (2016, 23 January). Centre presses dislike on anti-court facebook pages. *India Today*. www.indiatoday.intoday.in/story/ centre-presses-dislike-on-anti-court-facebook-pages/1/577672. html

⁵⁹ Ibid.

Hate speech

India has a number of provisions on its books that seek to restrict speech that can negatively affect the relations between its diverse communities, hurt their religious feelings, or prejudice their integration into the national community. In light of India's size and diversity, it is quite understandable that the country's laws contain a number of provisions aimed at ensuring the peaceful coexistence of its peoples. In practice, however, the way in which some of these provisions in the Indian Penal Code in particular have been phrased and interpreted leads to easy misuse, and may well harm the relations between India's communities rather than helping them.

Among the sections in the Indian Penal Code that are frequently used to restrict freedom of expression online,⁶⁰ the wording of sections 153A and 505(2) IPC is quite similar:

153A. Promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.— (1) Whoever— (a) by words, either spoken or written, or by signs or by visible representations or otherwise, promotes or attempts to promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, disharmony or feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities [...] shall be punished with imprisonment which may extend to three years, or with fine, or with both.

505(2) Statements creating or promoting enmity, hatred or ill-will between classes.—

Whoever makes, publishes or circulates any statement or report containing rumour or alarming news with intent to create or promote, or which is likely to create or promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities, shall be punished with imprisonment which may extend to three years, or with fine, or with both.

Similarly, sections 295A and 298 IPC, too, resemble each other:

295A. Deliberate and malicious acts, intended to outrage religious feelings of any class by

insulting its religion or religious beliefs.-Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of citizens of India, by words, either spoken or written, or by signs or by visible representations or otherwise, insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both. 298. Uttering, words, etc., with deliberate intent to wound the religious feelings of any person.— Whoever, with the deliberate intention of wounding the religious feelings of any person, utters any word or makes any sound in the hearing of that person or makes any gesture in the sight of that person or places, any object in the sight of that person, shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

Under section 196 of the Code of Criminal Procedure, a court cannot take cognisance of a case under sections 153A or 295A without the previous sanction of the central government or state government. Before according sanction, the central government or state government may order a preliminary investigation by a police officer not being below the rank of inspector.

Perhaps the most notorious example of misuse of these sections is from November 2012, when a young woman, Shaheen Dada, was arrested for a Facebook post she wrote questioning the shutdown of Mumbai that followed the death of Bal Thackeray, the founder of the Shiv Sena. The Shiv Sena is a right-wing ethnocentric party with a particularly strong following in Mumbai. Following its leader's death, businesses throughout the city had been forced to shut and taxis went off the roads, all under the threat of violence. Shaheen Dada wrote:

With all respect, every day, thousands of people die, but still the world moves on. Just due to one politician died a natural death, everyone just goes bonkers. They should know, we are resilient by force, not by choice. When was the last time, did anyone showed some respect or even a two-minute silence for Shaheed Bhagat Singh, Azad, Sukhdev or any of the people because of whom we are free-living Indians? Respect is earned, given, and definitely not forced. Today, Mumbai shuts down due to fear, not due to respect.⁶¹

⁶⁰ For a more complete overview of hate speech provisions in Indian law, see Law Commission of India. (2017). Op. cit.

⁶¹ Quoted in The Telegraph India (2012, 21 November). Everyone Need Not Think the Same: Facebook Girl. *The Telegraph India*. https:// www.telegraphindia.com/1121121/jsp/nation/story_16221567.jsp

Shaheen's friend, Rinu Srinivasan, liked, shared and commented on the post on Facebook; she was arrested as well. While the FIR was initially filed under section 295A of the IPC ("deliberate and malicious acts intended to outrage religious feelings of any class by insulting its religion or religious beliefs"), in addition to section 66A of the IT Act, the former was later replaced by section 505(2) IPC as there was no actual mention of religious belief or religion in either of the girls' comments. Following a largescale uproar about the girls' arrest, the charges were dropped after about a month.

Years later, the use of India's hate speech sections to stifle political criticism continues. For example, in March 2017, a woman was arrested in Bangalore for Facebook posts she had written which allegedly put Uttar Pradesh Chief Minister Yogi Adityanath in a "poor light." Among the sections she was booked under was section 153A IPC.⁶² In April 2017, Prashant Bhushan, a senior advocate and social activist, saw a number of cases slapped on him under section 295A, for a tweet criticising a new policy of the government of Uttar Pradesh, in which he had, among other things, described Lord Krishna as an "eve-teaser".⁶³

There are several, intertwined reasons that explain why these sections are frequently used in such an overly broad manner. As mentioned earlier, in free speech jurisprudence in India, a dominant strand accords primacy to public order when free speech and public order seem to clash. In addition, where hate speech in particular is concerned, a close reading of both the hate speech sections in the IPC and of Supreme Court jurisprudence around these sections makes clear that the law gives considerable credibility to the idea that there is an excess of passion and emotion among the Indian people, because of which speech in unregulated or irrational form is believed to be dangerous: as the law states clearly, the feelings of the people need to be tended to. It is therefore that, for example, hate speech jurisprudence in India is deeply concerned not merely with the content of speech but with the form: while speech packaged in a rational form, for example in academic research, may be seen as acceptable, the same message in an artistic format that seeks to offend, shock or disturb might not.⁶⁴

The concurrent existence of these two aspects of Indian hate speech law and jurisprudence has two important consequences. The first is that the guestion of thresholds disappears into the background when the police receive complaints regarding hate speech. Supreme Court jurisprudence may have developed fairly high standards for the criminalisation of speech under these provisions.⁶⁵ For example, in Ramji Lal Modi v. State of UP, the Supreme Court, while upholding the constitutionality of section 295A, reconfirmed that the section only penalises insults or attempts at insult of religion or religious feelings that are perpetrated with a deliberate and malicious intent as well as having a tendency to disrupt public order.⁶⁶ Similarly, in Shreya Singhal v. Union of India, the Court distinguished discussion and advocacy from incitement and noted that only the latter could be limited. But once the feelings of a community are outraged, the question of whether or not the accused did so with deliberate and malicious intent, as required by section 295A IPC, frequently disappears into the background. As the cases of Prashant Bushan and Shaheen Dada mentioned above make clear, to placate the feelings of those outraged, the police come under tremendous pressure to register a case.

Consequently, each time the government gives in to threats of disruption of public order, those who have been outraged find new reason to do so again in the future, as – in a typical case of the heckler's veto - it is the author of the outrageous speech, not those who are threatening disruption, who is silenced. In other words, as Shehla Rashid Shora and Anja Kovacs have pointed out, the hate speech provisions in India's IPC "have allowed reference to a group identity, in combination with the orchestration of an actual or potential threat of group violence, to emerge as effective means for groups to impose their worldview on others."⁶⁷ Ironically, those who are most willing to revert to violence become the "custodians" of community identity, while other voices are marginalised.

These challenges are perhaps further heightened because the hate speech sections in the IPC do not take into account the unequal power relations between India's groups, races and religions.

⁶² Press Trust of India. (2017, 22 March). Bengaluru Woman Faces Police Case For Facebook Posts On Yogi Adityanath. *NDTV*. www. ndtv.com/bangalore-news/bengaluru-woman-booked-forobjectionable-facebook-posts-on-uttar-pradesh-chief-ministeryogi-adityan-1672010

⁶³ Hindustan Times. (2017, 4 April). Prashant Bhushan backs down, admits Krishna tweet was 'inappropriately phrased'. *Hindustan Times*. www.hindustantimes.com/india-news/prashant-bhushanbacks-down-admits-krishna-tweet-was-inappropriately-phrased/ story-iRORHk4DSKazaFrB98FkwL.html; Press Trust of India. (2017, 6 April). Fresh case against Prashant Bhushan for his tweet on Lord Krishna. *Deccan Chronicle*. www.deccanchronicle.com/nation/ politics/o60417/fresh-case-against-prashant-bhushan-for-histweet-on-lord-krishna.html

⁶⁴ Narrain, S. (2016). Op. cit.

⁶⁵ For an overview, see Law Commission of India. (2017). Op. cit.

⁶⁶ AIR 1957 SC 620.

⁶⁷ Shora, S. R., & Kovacs, A. (2013). Op. cit.

While Supreme Court jurisprudence might take into account incitement to discrimination as well as incitement to violence, the text of the law does not distinguish between slander directed at a powerful majority and abuse targeted at a marginalised community or individual.⁶⁸

The only law to fight hate speech in India that does recognise structural and historical discrimination is the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989, which applies to the internet space as well. The Delhi High Court has held that casteist slurs made on Facebook, for example, which target individuals belonging to a scheduled caste or scheduled tribe community, are punishable under this act – even when they are made in a closed group.⁶⁹

Provisions that do not recognise the historical and systemic marginalisation of specific groups of people based on their identity, such as section 153A and 505(2) IPC, are likely to "disproportionately benefit those who already are in a more powerful position than their adversaries, however relative that position might be."⁷⁰ As more and more Indians come online, this tension will likely be felt only more acutely.

In addition, the thresholds for the criminalisation of speech included in section 153A and section 505(2) in particular are arguably too low. Former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, has noted that to be criminalised, hate speech should be of a public nature, should at the very minimum present a real and imminent danger, and must contain an obvious intent to harm.⁷¹ Sections 153A and 505(2), however, allow speech to be censored merely because it promotes "disharmony" or "feelings of enmity [...] or ill-will" [italics ours]. In fact, in section 505(2), even the mere likelihood of this happening is considered sufficient for prosecution – there is no need to establish intent as well. Where sufficient tension is generated, as in the Shaheen Dada case, this provision, therefore, allows for the criminalisation of what may have been only an innocuous statement - or even a well-intended one - on the grounds that it is "likely" to promote class enmity.

Reform of the law might not always be sufficient. As section 295A comes close to a blasphemy law, it should arguably be scrapped. As Shora and Kovacs have argued:

While believers of all religious communities, as well as those who do not adhere to any religion, should indeed be protected, religious beliefs as such should not. Without the right to question, be it one's own religion or another, the right to religion becomes meaningless. Those who engage in violence because their own beliefs are questioned or challenged should not be protected by the law on that account.⁷²

The constitutional validity of sections 153A, 295A and 298 IPC, among others, is currently being challenged in the Supreme Court by Subramaniam Swamy.⁷³

Morality, obscenity and sexual expression

A number of provisions are used to curtail freedom of expression on the internet on the grounds of morality or obscenity. Most prominent among these is section 67 of the IT Act:⁷⁴

67. Punishment for publishing or transmitting obscene material in electronic form.—

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

The wording of this provision resembles closely that of section 292 of the IPC, which bans the sale, etc. of obscene publications or representations.

⁶⁸ Ibid.

⁶⁹ Garg, A. (2017, July 4). Social media slurs on SC/ST punishable: HC. *Times of India*. www.timesofindia.indiatimes.com/india/socialmedia-slurs-on-sc/st-punishable-hc/articleshow/59432794.cms.

⁷⁰ Shora, S. R., & Kovacs, A. (2013). Op. cit.

⁷¹ La Rue, F. (2012). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://www.un.org/en/ga/search/view_doc. asp?symbol=A/67/357

⁷² Shora, S. R., & Kovacs, A. (2013). Op. cit.

⁷³ Choudhary, A. (2015, 23 June). Subramanian Swamy challenges hate speech law in SC. *Times of India*. www.timesofindia. indiatimes.com/india/Subramanian-Swamy-challenges-hatespeech-law-in-SC/articleshow/47776651.cms?from=mdr

⁷⁴ Other provisions that can be and have been used in a similar vein include section 509 IPC (Word, gesture or act intended to insult the modesty of a woman) and provisions of the Indecent Representation of Women (Prohibition) Act, 1986. Their misuse seems, however, less widespread. For reasons of space, we have, therefore, not included a detailed discussion of these provisions in this paper.

In addition, section 294 of the IPC makes obscene songs and dance illegal. Moreover, both section 67 IT Act and section 292 IPC make an exception for material that is "in the interest of science, literature, art or learning or other objects of general concern" or has a "bona fide heritage or religious purpose."

The exceptions listed in the law do not, however, seem sufficient to curtail its misuse. In a groundbreaking study on the use of section 67 of the IT Act in India, Bishakha Datta found that section 67 has been slapped on people in a wide variety of situations, including for speech acts that consist of legitimate political speech.⁷⁵

In some of these cases, the charge of obscenity is completely misplaced, in others overdrawn. For example, in September 2012, Henna Bakshi was booked under section 67, among others, for using abusive language in messages she posted on the Chandigarh traffic police's Facebook page, following an unhappy series of interactions with the police after her car was stolen. While Bakshi did use unparliamentary language in her complaints to the police, only a total of two words used by her in the exchange could be considered to have a sexual connotation.⁷⁶ In another example, in November 2016, a Karnataka man was arrested on obscenity charges for allegedly posting on social media a photo of India's prime minister being urinated upon.⁷⁷

A complex mesh of reasons can explain the overuse of such sections. First, as Richa Kaul Padte and Anja Kovacs have noted elsewhere, laws focusing on obscenity and (in)decency in India are based on "the belief that [female] sexuality is an inherently corrupting force that serves to destroy the moral and social fabric of a culture, and therefore, something that needs to be suppressed."⁷⁸ Expressions of female sexuality are not only understood as violations of notions of "decency" and "morality" but also as against the broader interests of the state, as sexless, clothed female bodies have come to signify the purity of the nation.⁷⁹ Though often defended in the name of women's protection, such laws thus see expressions of female sexuality as a problem, a transgression, and control of women's bodies as essential. Not individual rights but "collective" values that are held dear by dominant groups really are considered the victims here. In other words, through morality, a particular set of power relations is sought to be protected.

Against this backdrop, the ambiguous phrasing of these laws becomes particularly problematic. Scientific or sociologically accepted definitions of what is "lascivious" or "appeals to the prurient interest," what is depraved or corrupting, remain absent. In fact, there is not even agreement on what constitutes "art". As a consequence, in interpreting what qualifies as obscenity, the personal perspectives and values of those making these decisions matter a great deal, and even judges do not always agree with one another when considering these matters. For example, when, in a 1986 case, a High Court judge ruled the description of the female body by a well-known writer obscene, this decision was overruled by the Supreme Court, which believed it to be for the advancement of art.⁸⁰ Moreover, Datta's research on the use of section 67 of the IT Act has shown that the situation is even worse on the ground: for many police officers, whose first language is often not English, words such as "prurient" or "lascivious" are simply meaningless.⁸¹

In addition, it is important to note that obscenity attracts a higher sentence when the offence is an electronic one. Under section 292 IPC, a first conviction only attracts a prison sentence of up to two years or a fine of up to 2,000 rupees, as against three years and 500,000 rupees under section 67 of the IT Act. While a second conviction may attract a term of up to five years under both sections, the IT Act allows for a fine of a whopping one million rupees, as against 5,000 rupees under the IPC. The IPC makes an exception to these relatively milder punishments only when the obscene material is shared with someone younger than 21 years of age.⁸²

The fact that the IT Act generally provides for higher sentences for obscenity offences than the IPC has important procedural consequences – and not merely for those convicted. While all the provisions discussed are bailable, the longer sentence

⁷⁵ Datta, B. (2017). *Guavas and Genitals: An exploratory study on* section 67 of the Information Technology Act, India. Mumbai: Point of View.

⁷⁶ For a detailed discussion of this case, see Shora, S. R., & Kovacs, A. (2013). Op. cit.

⁷⁷ The News Minute. (2016, 28 November). Karnataka Man Arrested for Posting Obscene Photo of PM Modi on Facebook. The News Minute. http://www.thenewsminute.com/article/karnataka-manarrested-posting-obscene-photo-pm-modi-facebook-53533

⁷⁸ Kaul Padte, R., & Kovacs, A. (2013). Keeping Women Safe? Gender, Online Harassment and Indian Law. New Delhi: Internet Democracy Project. https://internetdemocracy.in/reports/ keeping-women-safe-gender-online-harassment-and-indian-law/

⁷⁹ Bose, B. (2006). Introduction. In B. Bose (Ed.), *Gender and Censorship*. New Delhi: Women Unlimited.

⁸⁰ As noted in Jaising, I. (2006). Obscenity: The Use and Abuse of the Law. In B. Bose (Ed.), *Gender and Censorship*. New Delhi: Women Unlimited.

⁸¹ Datta, B. (2017). Op. cit.

⁸² Section 293 IPC makes illegal the sale, etc. of obscene objects to young persons, prescribing a jail term of up to three years and a fine of 2,000 rupees for a first conviction and of up to seven years and a fine of up to 5,000 rupees for repeat offenders.

under the IT Act makes obscenity under section 67 a cognisable offence, meaning that the police are allowed to start an investigation and make arrests without requiring the permission of a magistrate. In light of the many ambiguities surrounding obscenity laws, and of the widely reported misuse of the section, it deserves to be asked whether the threshold for arrests under the section should not be increased.

Although the Supreme Court's adoption in 2014 of the community standards test over the Hicklin test, in *Aveek Sarkar v. State of West Bengal*,⁸³ has been widely received as a positive evolution, it does not, so far, seem to have dramatically challenged either the assumptions that underlie the framing of the law or the way it has been applied by police forces across the country.

Established in the English case *Regina v. Hicklin*⁸⁴ in 1868, the Hicklin test as formulated by the presiding judge defined the test of obscenity as follows: "whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall."⁸⁵ For decades, this test was prominently used in Indian courts of law, most famously to ban *Lady Chatterley's Lover* in India. In *Aveek Sarkar v. State of West Bengal*, the Supreme Court for the first time formulated what it called a "contemporary community standards" test:

A picture of a nude/seminude woman, as such, cannot per se be called obscene unless it has the tendency to arouse feeling or revealing an overt sexual desire. The picture should be suggestive of deprave mind [sic] and designed to excite sexual passion in persons who are likely to see it, which will depend on the particular posture and the background in which the nude/semi-nude woman is depicted. Only those sex-related materials which have a tendency of "exciting lustful thoughts" can be held to be obscene, but the obscenity has to be judged from the point of view of an average person, by applying contemporary community standards.

As Gautam Bhatia has noted, the judgment was significant for its emphasis on the importance of the background and context in which nude imagery is placed: nudity as such is finally no longer necessarily deemed obscene. Also important is that the Court notes, following the 1957 US Supreme Court case of *Roth v. United States*, that the community standards to be applied should be contemporary: not the standards from India's idealised, mythical golden age, but of today's real-life fleshand-blood people, should be determining.⁸⁶

Where the judgment remains weak, however, is that it allows for the criminalisation of speech on the grounds of obscenity merely because, following the application of contemporary community standards, an image that contains nudity or semi-nudity is believed to arouse sexual desire or passion. While Roth v. United States also required the material to be "patently offensive" and "of no redeeming social value", these additional standards were not referenced in the Indian Supreme Court's ruling.87 As a consequence, in a country where even mere suggestion is often believed to be inducing passion, much power remains with the eye of the beholder where the right to sexual expression is concerned as the continuing arrests under this provision make clear.

Perhaps the Court's decision should not be surprising, however. After all, more stringent standards might have run contrary to section 67A of the IT Act, which explicitly criminalises depictions of sexually explicit acts:

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form. —

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

The limitations that apply to section 67 of the IT Act apply here as well, i.e. material that is "in the interest of science, literature, art or learning or other objects of general concern" or has a "bona fide heritage or religious purpose" cannot be criminalised. However, all other depictions of sexually explicit acts are criminalised by section 67A, whether or not

^{83 (2014) 4} SCC 257.

⁸⁴ L.R. (1868) 3 Q.B. 360.

⁸⁵ Quoted in Mazzarella, W. (2011). The Obscenity of Censorship: Rethinking a Middle-class Technology. In A. Baviskar and R. Ray (Eds.), *Elite and Everyman: The Cultural Politics of the Indian Middle Classes*. New Delhi: Routledge.

⁸⁶ Bhatia, G. (2014, 7 February). Obscenity: The Supreme Court Discards the Hicklin Test. *Indian Constitutional Law and Philosophy*. https://indconlawphil.wordpress.com/2014/02/07/ obscenity-the-supreme-court-discards-the-hicklin-test

they are "patently offensive" or "of no redeeming social value" and whether or not those involved have consented.

Moreover, where those under 18 years old are concerned, sexual expression is always criminalised in India. Section 67B of the IT Act and sections 13 and 14 of the Protection of Children from Sexual Offences Act, 2012, seek to fight the production, circulation and consumption of child sexual abuse images. Unfortunately, however, the sections in their current wording also criminalise images of a sexual nature that are shared with consent by young people who are in a relationship with each other; none of the provisions provides for an exception in these cases.

Such provisions criminalising all sexual expression further contribute to the portrayal of sexuality as inherently corrupting, while disregarding the importance of consent in any sexual act or in the creation, circulation and publication of images of such acts. In this way, they help to keep existing power relations and their associated conceptions of morality intact. If the writ petition of Kamlesh Vaswani currently under consideration in the Supreme Court is successful, this will only further exacerbate this situation: Vaswani has asked the court not only to ensure that all pornography will be blocked in India, but also that even watching pornography in a private place will be criminalised and will, in fact, be made a non-bailable, cognisable offence.⁸⁸ For the moment, while creating, circulating or publishing pornography is illegal, its consumption in private is deemed not to be.

It is notable that section 67A IT Act does not have an equivalent under any other law book in India, meaning that this crime, with its severe sentences, exists only when electronic media are used. Moreover, section 67A IT Act, too, is non-bailable and cognisable, meaning that the barriers to be charged with this crime are few. Perhaps this is what explains why the provision was slapped on a man who had tweeted a 2012 picture of Maharashtra Chief Minister Devendra Fadnavis holidaying on a yacht with his family to suggest that the Chief Minister was squandering taxpayers' money while on an official tour to the United States in 2015.89 Where sexual expression remains largely taboo, tools to censor it lend themselves easily to misuse indeed.

Intellectual property rights

Intellectual property rights are governed under dedicated legislations such as the Indian Copyright Act, 1957, the Trademarks Act, 1999, the Patents Act, 1970, and amendments to these Acts.

Issues of intermediary liability as they relate to intellectual property rights infringement will be addressed in the sub-section on intermediary liability, below. There have also been attempts, on occasion, to use these Acts to directly penalise speech and expression online. We earlier referred to *Tata Sons Limited. v. Greenpeace International & Anr.*,⁹⁰ for example, in which the Tata Group sued Greenpeace, an NGO, for defamation and trademark violation when Greenpeace released an online videogame called *Turtles v. TATA* as part of a campaign against Tata's port on beaches in Orissa, as the port was harming olive ridley turtles. The suit was not successful.

A more common concern for free speech on the internet where India's intellectual property rights regime is concerned is the passing of "John Doe" orders by courts. Exercising powers under section 151 of the Civil Procedure Code, courts order the blocking of named and unnamed parties, often for copyright infringement.

For example, as noted earlier, when the producers of Bollywood movies *Lipstick Under My Burkha* and *Jab Harry Met Sejal* approached the Madras High Court in 2017, more than 2,600 websites were blocked as part of an injunction order for copyright infringement. The order required blocking of entire websites, and not just specific URLs that have infringing content.⁹¹

This is common in the case of "John Doe" or "Ashok Kumar" orders, in which copyright holders (often producers of Bollywood movies or owners of broadcasting rights for large-scale events) approach courts to pass blocking orders, ex parte, against named and unnamed parties who may be publishing copyrighted works of the petitioners.⁹² These orders have been found to affect legitimate online businesses and non-infringing websites.⁹³

⁸⁸ Kamlesh Vaswani v. Union of India & Ors. WP (Civil) 177 of 2013.

⁸⁹ Bose, A. (2015). A Man Just Got Arrested for Tweeting Chief Minister Devendra Fadnavis' Family Photograph. *Huffington Post*. http://www.huffingtonpost.in/2015/07/11/mumbai-fadnavistwitter_n_7774592.html

⁹⁰ CS(OS) 1407/2010.

⁹¹ Joshi, D. (2017, 10 August). Madras High Court Issues 'Ashok Kumar' Order to Block the Internet Archive + 2649 Websites. *Spicy IP*. https:// www.spicyip.com/2017/08/madras-high-court-issues-ashok-kumarorder-to-block-the-internet-archive-2649-websites.html

⁹² The principles and procedures evolved and the justification for arraigning unnamed defendants has been argued in a series of posts by the Centre for Internet and Society. See, e.g. Padmanabhan, A. (2014, 30 January). Can Judges Order ISPs to Block Websites for Copyright Infringement? (Part 1). Centre for Internet and Society. https://cis-india.org/azk/blogs/ john-doe-orders-isp-blocking-websites-copyright-1

⁹³ Basheer, S. (2016, 24 August). Of Bollywood "Blocks" and John Does: Towards an IP Ombudsman? Spicy IP. https://spicyip. com/2016/08/of-bollywood-blocks-and-john-does-towards-aneutral-ombudsman.html

In the first such case in India, *Tej Television Ltd. v. Rajan Mandal*,⁹⁴ a Court Commissioner was appointed to make an inventory of infringing material, equipment used, etc., with the help of technical staff and the police, and to produce a report to be used by the Court. Nowadays, it is common for producers to sub-contract the job of combing through infringing or potentially-infringing websites to external agencies, who tend to err on the site of caution and list more websites for blocking than strictly necessary. As Kian Ganz has noted:

[U]ntil now, such agencies have had little incentive to get it right. Their bill is usually paid by the copyright holder, who has filed the John Doe order in court and usually doesn't mind if overblocking of websites takes place. And courts realistically do not have enough time to manually check hundreds of file-sharing websites.⁹⁵

Intellectual property rights professor Shamnad Basheer has also noted that it is not practical to require the judges to determine whether the links pertain to specific pages containing the infringing copies:

[I]s it reasonable of us to expect an overworked and underpaid judge (hit with the pendency pressures and all that) to wade through all 800 links and ascertain infringement for himself/ herself? What then is to be done? How are these competing concerns to be balanced out?⁹⁶

The Bombay High Court's Justice Gautam Patel has in the past pointed to the disproportionate nature of blocking and has required a three-step verification before the blocking of URLs, so that the blocking orders are narrowly tailored.⁹⁷

State laws touching on intellectual property rights and their infringement provide an additional challenge where freedom of speech and expression is concerned: going above and beyond what the Indian Copyright Act allows for, they consider copyright infringement as a violation worthy of preventive detention. States like Tamil Nadu, Maharashtra and Karnataka have made amendments to the respective states' preventive detention laws, to make it possible to arrest "audio and video pirates" and "digital offenders".⁹⁸

For example, in August 2014, the Karnataka Prevention of Dangerous Activities of Bootleggers, Drug-Offenders, Gamblers, Goondas, Immoral Traffic Offenders and Slum-Grabbers Act, 1985, was amended to include offences under the Indian Copyright Act, 1957 and the Information Technology Act, 2000. The amendments also brought new categories of "video or audio pirates" and "digital offenders" under the purview of the Act. Section 2(f) of the Act defines "digital offender" as:

[A]ny person who knowingly or deliberately violates for commercial purposes any copyright law in relation to any book, music, film, software, artistic or scientific work and also includes any person who illegally enters through the identity of another user and illegally uses any computer or digital network for pecuniary gain for himself or for any other person or commits any of the offences specified under section 67, 68, 69, 70, 71, 72, 73, 74 and 75 of the Information Technology Act, 2000.

Further, per Section 2 (vii):

(vii) In the case of a Video or Audio pirate, when he is engaged or is making preparations for engaging in any of his activities as a Video or Audio pirate habitually for commercial gain, which affect adversely, or are likely to affect adversely, the maintenance of public order.

In the explanation to the section, the meaning of the phrase "video or audio pirate" is further defined:

(k) "Video or Audio pirate" means a person who commits or attempts to commit or abets the commission of offences of infringement of copy right habitually for commercial gain, in relation to cinematograph film or a record embodying any part of the sound track associated with the film, punishable under the Copy Right [sic] Act, 1957 (Central Act XIV of 1957).

Section 13 of the Act allows the state government to undertake preventive detention of suspects, without the requirement to be produced before a magistrate for up to 90 days (which may extend up to a year). By allowing for preventive detention of

^{94 [2003]} FSR 22.

⁹⁵ Ganz, K. (2016, 2 August). The messy battle against online piracy. *Livemint*. http://www.livemint.com/Consumer/ YtbRNgfv6ZgZCZOexcsWMI/The-messy-battle-against-onlinepiracy.html

⁹⁶ Basheer, S. (2016, 27 June). Udta Punjab: Of Courts, Cuts, Copyrights and Conflicted Counsels. Spicy IP. https://spicyip. com/2016/06/udta-punjab-linking-courts-cuts-copyrights-andconflicted-counsels.html

⁹⁷ Bajaj, R. (2016, 28 July). Bombay HC Effectively Transforms John Does from Swords to Shields – Delineates Most Robust Safeguards to Date. *Spicy IP*. https://spicyip.com/2016/07/bombay-hceffectively-transforms-john-does-from-swords-to-shieldsdelineates-most-robust-safeguards-to-date.html

⁹⁸ Chari, M. (2014, o6 August). Why many states are using the 1923 Goondas Act to curb digital piracy. Scroll. http://scroll.in/ article/673042/Why-many-states-are-using-the-1923-Goondas-Act-to-curb-digital-piracy

persons suspected of pirating audio or video material for purposes outside of commerce, the Act goes well beyond the scope of liability under the Indian Copyright Act, 1957. Many intellectual property rights and free speech scholars have argued that the provisions are unconstitutional.⁹⁹

Other limitations of freedom of expression

In the previous section, we saw how a variety of grounds are used in India to criminalise speech and expression in ways that are not acceptable. However, free speech is not only curtailed through problematic criminal charges against those who speak; it is also frequently restrained in other objectionable ways. In this section, we will examine five such methods that have had a significant impact on free speech online in India.

Government powers to block content

A first provision of immediate relevance here is section 69A of the IT Act, which provides the central government with the "power to issues directions for blocking for public access of any information through any computer resource," when it is "necessary or expedient to do so, in the interest of sovereignty and integrity of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to the above."

While the IT Act of 2000 also allowed the central government to block content on the grounds of obscenity, this is no longer the case under the amended Act of 2008. Seeing that the likelihood of political abuse of censorship powers is considerably smaller when censorship grounds are narrowly and clearly defined, the removal of obscenity from this provision is a most welcome evolution.

As required by the IT Act, the procedures and safeguards subject to which such blocking may be carried out have been detailed in the Information Technology (Procedures and Safeguards for Blocking Access of Information by Public) Rules, which were notified in October 2009.

Under these Blocking Rules, every ministry or department of the government of India as well as state governments and union territories and any agency of the central government have to appoint a Nodal Officer to which "any person may send their complaint." If the organisation in question is satisfied that there is indeed reason to take action, it can then forward the complaint, through its Nodal Officer, to the Designated Officer. The Designated Officer is an officer not below the rank of Joint Secretary and may "on receipt of any request from the Nodal Officer of an organisation or a competent court, by order direct any Agency of the Government or intermediary to block for access by the public any information or part thereof generated, transmitted, received, stored, or hosted in any computer resource" for any of the reasons specified in section 69A of the IT Act and listed above.

However, where the request comes through a Nodal Officer, the Designated Officer can only do so after the request has been examined by a committee "consisting of the Designated Officer as its chairperson and representatives, not below the rank of Joint Secretary in Ministries of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency Response Team."

Where possible, the Rules stipulate, the person or intermediary hosting the information will be informed of the inquiry and will get the chance to submit their replies and clarifications; the Rules require the person or intermediary to be given at least 48 hours' notice. In addition, the committee's recommendation to block has to subsequently be approved by the Secretary in the Department of Information Technology under the Ministry of Communications and Information Technology. A Review Committee is supposed to meet at least once every two months to re-examine the legitimacy of all blocking orders.

While the blocking regime under section 69A of the IT Act and its attendant rules is, thus, fairly well circumscribed, requiring a range of approvals and recognising the right to be heard of the owner of the content in question, there are a few aspects of the regime that remain open to improvement.

Allowing content to be blocked simply because it is expedient to do so violates international standards which require that censorship should be necessary and the least restrictive means required to achieve the purported aim. In the absence of these qualifications, the provision has the potential to open the door to censorship that is overly broad.

The inclusion of incitement to the commission of a cognisable offence as a ground for blocking is arguably problematic for the same reason: in established international human rights jurisprudence, incitement is recognised as a ground for censorship specifically when it concerns a clear, demonstrable and immediate incitement to *violence*, or sometimes, discrimination. These qualifications are absent in section 69A and the Blocking Rules.

⁹⁹ Bhatia, G. (2014, 5 August). Goondagiri Of The Goonda Act. Outlook India. www.outlookindia.com/website/story/goondagiriof-the-goonda-act/291593; Chaudhary, N. (2014, 13 August). Karnataka's 'Goondas Act' - An examination. Spicy IP. https:// www.spicyip.com/2014/08/guest-post-karnatakas-goondas-actan-examination.html

Further adding to these concerns is the fact that the last clause of the Blocking Rules explicitly makes transparency in the blocking regime an impossibility. The clause reads: "strict confidentiality shall be maintained regarding all the requests and complaints received and actions taken thereof." In other words, while the phrasing of section 69A of the IT Act and the attendant rules raise a range of concerns regarding their impact on freedom of expression, those same rules also make it impossible for us to assess whether such concerns are indeed justified or whether the purposes for which content is restricted are in fact wholly legitimate.

Moreover, at no point in the process do the section or the rules require the intervention of a judicial body. The crucial role that courts should play, and have played, in democratic societies in decisions that curtail the right to freedom of speech has been disregarded.

While content bans in the offline world have generally been made public in India, it thus becomes almost impossible for the public to challenge online censorship undertaken under this section in court if so desired. The only time at which a challenge becomes possible is when a blocking order is leaked. For example, earlier this year, the government used its powers under this section to ask Twitter to block 115 handles for "propagating objectionable contents." The handles included a range of accounts that allegedly take controversial positions regarding the conflict in Kashmir. The government's request became public knowledge after Twitter, in disregard of the Blocking Rules under section 69A. emailed all account holders involved to inform them that "an official correspondence" was received which claimed that the content of their accounts violates Indian law. When journalists followed up on the incident with Twitter, Twitter linked to a copy of the request that was available on the internet. According to this document, the request for blocking was done in "the interest of public order as well as for preventing any cognisable offence relating to this referred in section 69A of the IT Act."100

The constitutional validity of section 69A of the IT Act and the validity of the rules made under that section were challenged in *Shreya Singhal v. Union of India*. The petitioners questioned, among other things, the absence of a guaranteed hearing of the author of the content before a decision is made; the limited procedural safeguards when compared

to those provided in the case of offline bans (under section 95 and 96 of the Criminal Code of Procedure); and the confidentiality provision. However, the court rejected the petitioners' arguments, on the grounds that the provision is narrowly framed and that a number of procedural safeguards are foreseen, even if those are different from safeguards for offline content. The constitutionality of both the provision and rules was upheld.

Intermediary liability

The Indian authorities do not always draw on section 69A to block content. Figures reported by Google in its Transparency Report indicate that the company receives a substantial number of takedown requests from Indian government officials. In 2016, the Indian government made 575 such requests, asking for 5,370 pieces of content to be taken down.¹⁰¹ Only 52 of those requests, relating to 196 items, were made by the judiciary. The rest came from the executive branch of government. Google complied in 14% of cases. Requests such as those reported by Google in its transparency reports are frequently made under section 79 of the IT Act and its attendant rules, the Intermediary Guidelines Rules 2011, both of which concern intermediary liability and safe harbour.

Intermediary liability in the IT Act

The IT Act defines an intermediary as:

[A]ny person who on behalf of another person receives, stores or transmits that record or provides any service with regard to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

The current version of section 79 was included in the IT Act in 2008; following a number of controversies, section 79 was reframed at that time to more clearly define and circumscribe the circumstances under which intermediaries could become liable. According to the section in its current form, intermediaries are not liable for content they provide access to, provided they do not initiate or select the receiver of the transmission; do not select or modify the information contained in the transmission; and do delete content "expeditiously when receiving actual knowledge or when being notified by the appropriate government or its agency." When this

¹⁰⁰ Saha, A. (2017, 4 September). Citing official complaint, Twitter tells Kashmiri handles they are breaking laws. *Hindustan Times*. http://www.hindustantimes.com/india-news/twitter-tellskashmiri-handles-they-are-breaking-indian-laws-points-to-officialcomplaint/story-u33dt3gtkkvUjZtpld13fl.html

¹⁰¹ Google Transparency Report: Government requests to remove content. https://www.transparencyreport.google.com/ government-removals/by-country/IN

amendment to the IT Act was first approved, this phrasing was considered a substantial improvement over the earlier version of this section in the IT Act of 2000, and was as such welcomed.

But the additional guidelines that the central government prescribed in April 2011, as it is authorised to do under section 79 of the Act, undid much of the protection and clarity the section was intended to provide. Known as the Intermediary Guidelines Rules 2011, these made it obligatory for intermediaries to inform their users, by means of their terms of service, not to host, display, upload, modify, publish, transmit, update or share a broad range of types of content. In addition to content prohibited by article 19(2) of India's Constitution, this included content deemed "grossly harmful", "harassing", "blasphemous", "hateful", "racially, ethnically objectionable", "disparaging" or that "impersonate[d] another person" or "harm[ed] minors in any way." As many of the grounds for censorship included in the latter group go beyond the grounds of reasonable restrictions established by India's Constitution and are not defined under any other Indian statute, intermediaries were left without any guidelines to judge content. Moreover, under the Intermediary Guidelines Rules, anyone could file a complaint with the intermediary, who then had to act within 36 hours. The intermediary did not have to inform the party who posted the content, and the Intermediary Guidelines Rules did not provide for an automatic right to respond for the aggrieved party, nor for an appeals mechanism.

The privatisation of censorship that the Indian intermediary liability regime thus put into place had the potential to have a deeply chilling effect on free speech in the country. In informal conversations, representatives of several major intermediaries indicated over several years that the number of takedown requests by both government and private parties had grown substantially since the Rules were notified. Moreover, at least in some cases these requests were accompanied by significant political pressure that might have affected intermediaries' decisions. For example, on 5 December 2011, The New York Times reported that the then Minister of Communications and Information Technology, Kapil Sibal, had, over a stretch of several months, had a string of meetings with some of the major intermediaries in which he had tried to convince them to manually pre-screen content and remove any objectionable material.¹⁰² Content that Sibal showed to the intermediaries is said to have included both religiously sensitive material that he believed could potentially cause riots and political speech that he deemed unacceptable – including a Facebook page that maligned the president of the Congress Party, Sonia Gandhi.

In the same year, a study conducted by Rishabh Dara, then Google Policy Fellow at the Centre for Internet and Society, clearly brought out that intermediaries tend to err on the side of caution when faced with government requests to take down content.¹⁰³ Dara sent rather frivolous takedown notices to seven major intermediaries. Six of them complied, with some even taking down *more* content than Dara had requested. Strictly speaking, affected parties could have gone to the courts in response. Yet as the notice-and-takedown system that was put into place under section 79 lacked transparency, they in many cases might not even have become aware that their rights had been violated.

In Shreya Singhal v. Union of India, concerns about the potential for misuse of these provisions, and the weakening of the protections for freedom of expression that they therefore entail, were brought to the Supreme Court. The privatisation of censorship that the Intermediary Guidelines Rules and its parent section entailed, as well as the lack of safeguards in the Rules, were all called into question by the petitioners. In addition, the petitioners argued that the grounds on which both the rules and parent section allowed for censorship were vague and over-broad and went well beyond the subjects specified under Article 19(2) of the Indian Constitution.

The Supreme Court was receptive to the petitioners' arguments, and while stopping short of striking down the section and rules, it read down both. From here onwards, intermediaries have been only obliged to take down content upon receiving "a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to article 19(2) are going to be committed." In such cases, intermediaries are expected to remove content expeditiously. Where the content in question does not fall within the reasonable restrictions mentioned in Article 19(2) of the Constitution and/ or where an intermediary has not received a court order or a notification from a relevant government agency, it is not obliged to act.

While the Supreme Court's judgement may have strengthened the legal certainty for both

¹⁰² Timmons, H. (2011, 5 December). India Asks Google, Facebook to Screen User Content. *The New York Times*. www.india.blogs.nytimes.com/2011/12/05/ india-asks-google-facebook-others-to-screen-user-content

¹⁰³ Dara, R. (2012, 27 April). Intermediary Liability in India: Chilling Effects on Free Expression on the Internet. *Centre for Internet* and Society. https://www.cis-india.org/internet-governance/ chilling-effects-on-free-expression-on-internet

intermediaries and authors of content, it is not clear to what extent it has reduced takedowns. Google, for example, received the highest number of requests for the highest number of items ever in 2016; its compliance rate was only marginally higher than that in 2014, before the judgement in Shreva Singhal v. Union of India was pronounced.¹⁰⁴ In the case of Facebook, however, a drastic reduction can be observed: in 2016, the year that Facebook started to implement the judgement, it took down 2,753 pieces of content, compared to more than 30,000 the year before, and more than 10,000 in 2014. Facebook takes down content mostly under India's laws protecting religious beliefs and the sentiments of communities, as well as the protection of national symbols.105

Whether or not government-requested takedowns have decreased, it deserves to be pointed out that big tech companies in India, such as Amazon, reportedly also resort to tremendous amounts of self-censorship. "Nobody wants bad PR or government ire in an important market over a little nudity or a dead cow," as Pranav Dixit has reported.¹⁰⁶

Intermediaries and copyright

While section 79 of the IT Act might govern intermediary liability in general, additional provisions for intermediary liability are included in the Copyright (Amendment) Act, 2012. For those who seek to quickly remove material that they disagree with from the internet, this amended version of the Indian Copyright Act, 1957, might in many cases provide an all-too-easy route through which to do so.

At the heart of the regime around intermediary liability and copyright that has emerged in India is the case of *Super Cassettes Industries Ltd. v. Myspace Inc.*¹⁰⁷ In this case, the former sought to hold social network MySpace liable for copyright infringement. In his judgment, Justice Singh referred to section 81 of the IT (Amendment) Act, 2008, to argue that the safe harbour provisions in the IT Act did not apply in this case. Section 81 of the IT Act states that "nothing in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957." With this, Justice Singh pointed out a crucial lacuna in the law.

The gap was partially resolved in 2012 when several amendments to the Copyright Act of 1957 were passed in Parliament. Two of these entail a limited safe harbour provision, and thus have direct import for internet intermediaries.

The first amendment, section 52(1)(b) in the new Act of 2012, absolves intermediaries from liability for copyright infringement where the storage of infringing content is "transient or incidental" and part of a purely technical process of transmission or communication.

The second amendment, section 51(1)(c) in the amended Act, does the same when the transient or incidental storage of content is "for the purpose of providing electronic links, access or integration," on the condition that doing so "has not been expressly prohibited by the rights holder" and "unless the person responsible is aware or has reasonable grounds for believing that such storage is of an infringing copy."

The amendment further states that "if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work" claiming copyright infringement, the former is obliged to disable access to the content in question for a period of 21 days, or until receiving a court order. "In case no such order is perceived before the expiry of such period of 21 days, [the person responsible for the storage of the copy] may continue to provide the facility of such access."

As Sunil Abraham has pointed out,¹⁰⁸ the amendment clearly privileges the concerns of intellectual property rights-holders, as the intermediary is obliged under the law to remove the content in question even before the validity of the complaint has been proved. Because of this, the mechanism provided for under the amended Copyright Act is likely to have a chilling effect on free speech. Moreover, the likelihood of ISPs automatically and voluntarily reinstating content once the legal waiting period of three weeks has passed and no court order has been received, is low.

Abraham's colleague Pranesh Prakash goes even a step further. If the complaint turns out to be false – either because the complainant is not the rights-holder or because the content does not entail a violation of the rights-holder's copyright – there

¹⁰⁴ Google Transparency Report: Government requests to remove content. https://www.transparencyreport.google.com/ government-removals/by-country/IN

¹⁰⁵ Facebook (2016). Government requests report. https://www. govtrequests.facebook.com/country/India/2016-H2/

¹⁰⁶ Dixit, P. (2017, 12 July). American Tech Companies Are So Afraid Of Offending Indians That They're Censoring All Their Products. *Buzzfeed News*. https://www.buzzfeed.com/pranavdixit/whysilicon-valley-is-censoring-itself-as-it-expands-in?utm_term=. ry6qKDEboD#.jcApR71bJ7

¹⁰⁷ Super Cassettes Industries Ltd. v. Myspace Inc. 2011 (48) PTC 49 (Del).

¹⁰⁸ Abraham, S. (2012, 10 June). Copyright amendment: bad, but could have been much worse. Smart Investor. www. smartinvestor.business-standard.com/market/Compnews-120087-Compnewsdet-Sunil_Abraham_Copyright_amendment_bad_but_ could_have_been_much_worse.htm#.WaZ9h98xDec

is no punishment for the person who filed the complaint. Given this lack of punishment, Prakash has argued, the law is open to widespread abuse: it allows anyone "to remove content from the internet without following any 'due process' or 'fair procedure'."¹⁰⁹

Clearly, this amendment to the Copyright Act therefore violates the principles of necessity and proportionality that are integral to the validity of any action that seeks to censor content online.

But there are two further aspects of the judgment that were remarkable and also deserve attention here. First, when determining whether MySpace had knowledge of the presence of copyright-infringing content on its platform, Justice Singh highlighted the mechanisms instituted by MySpace to trail and curtail copyright infringement, as well as efforts by MySpace to cooperate with industry in this area, as one indication that MySpace did indeed have such knowledge (the Justice was not convinced they also authorised such actions though). With this, the lustice went against the grain of what is increasingly considered best practice in this area in the international community, where such proactive measures on the part of intermediaries generally have been lauded. Justice Singh's pronouncements on this issue were of importance because having actual knowledge was a ground on which intermediaries can lose the safe harbour provided to them by section 79 IT Act as well.

Finally, the Justice also argued that "if the defendants are put to notice about the rights of the plaintiff in certain works, the defendants should do preliminary check in all the cinematograph works relating Indian titles before communicating the works to the public rather than falling back on post infringement measures." He further stated:

if there is any due diligence which has to be exercised in the event of absence of any provision under the Act, the said due diligence must be present at the time of infringement and not when the infringement has already occurred so that the infringement can be prevented at the threshold and not when the same has already occurred.

Various aspects of MySpace working practices convinced the Justice that it should be technically feasible to do so. Although Justice Singh made his pronouncements in a case relating to copyright, with this, he was the first to put the supposed need for a pre-screening mechanism on the table.

Fortunately, in December 2016, following an interlocutory appeal, a two-judge bench of the Delhi High Court overturned the 2012 order, and ruled that pre-screening requirements cast an enormous burden on intermediaries.¹¹⁰ This welcome order cited the challenges that inhere in requiring intermediaries to regulate speech on the internet.

Ongoing challenges to India's intermediary liability regime

Challenges to India's intermediary liability regime, nevertheless, continue. Two separate, ongoing cases in the Supreme Court are of particular importance.

In Sabu Mathew George v. Union of India & Ors.,¹¹¹ the petitioner seeks to ensure that advertisements for services related to sex selective abortions do not show up in search engine results – be they paid results or organic results – as they violate section 22 of India's Pre-Conception and Pre-Natal Diagnostic Techniques (Regulation and Prevention of Misuse) Act, 1994 (henceforth PCPNDT Act). Section 22 reads:

22. Prohibition of advertisement relating to pre-conception and pre-natal determination of sex and punishment for contravention.—

(1) No person, organisation, Genetic Counselling Centre, Genetic Laboratory or Genetic Clinic, including Clinic, Laboratory or Centre having ultrasound machine or imaging machine or scanner or any other technology capable of undertaking determination of sex of foetus or sex selection shall issue, publish, distribute, communicate or cause to be issued, published, distributed or communicated any advertisement, in any form, including internet, regarding facilities of pre-natal determination of sex or sex selection before conception available at such Centre, Laboratory, Clinic or at any other place. (2) No person or organisation including Genetic Counselling Centre, Genetic Laboratory or Genetic Clinic shall issue, publish, distribute, communicate or cause to be issued, published, distributed or communicated any advertisement in any manner regarding pre-natal determination or pre-conception selection of sex by any means whatsoever, scientific or otherwise.

¹⁰⁹ Prakash, P. (2012, 23 May). Analysis of the Copyright (Amendment) Bill 2012. *Centre for Internet and Society.* www.cis-india.org/a2k/ blog/analysis-copyright-amendment-bill-2012

¹¹⁰ Nair, B. (2016, 25 December). Breaking News: Del HC Division Bench Rules in Favour of Safe Harbour for Intermediaries in MySpace-T Series Copyright Dispute. *Spicy IP*. https://www. spicyip.com/2016/12/breaking-news-division-bench-rules-infavour-of-safe-harbour-for-intermediaries-in-myspace-t-seriesdispute.html

¹¹¹ WP (Civil) 341 of 2008.

(3) Any person who contravenes the provisions of sub-section (1) or sub-section (2) shall be punishable with imprisonment for a term which may extend to three years and with fine which may extend to ten thousand rupees.

Explanation.—For the purposes of this section, "advertisement" includes any notice, circular, label, wrapper or any other document including advertisement through internet or any other media in electronic or print form and also includes any visible representation made by means of any hoarding, wall-painting, signal, light, sound, smoke or gas.

In response, the Court directed Google, Yahoo! and Microsoft, in September 2016, to block results for a number of keywords and keyword strings provided by the Court. In April 2017, the Court clarified that only results that violate section 22 PCPNDT Act should be blocked. It noted:

It is made clear that there is no need on the part of anyone to infer that it creates any kind of curtailment in his right to access information, knowledge and wisdom and his freedom of expression. What is stayed is only with regard to violation of Section 22 of the Act.¹¹²

However, it remains unclear how intermediaries can ensure that only illegitimate content will be blocked if content is blocked based on keywords and keyword strings. This is even more so as it is not clear how the word "advertisement" is to be interpreted by the intermediaries in this case: while the intermediaries are arguing for a narrow definition, the Solicitor-General has argued for a broad understanding, in which case the distinction between legitimate and illegitimate content becomes even more difficult to discern and a much wider range of content may be affected. The debate on what constitutes an "advertisement" in this case is still ongoing in court.

In addition, in September 2016, the court ordered the three intermediaries to develop an "auto-block" mechanism: an in-house procedure or method to ensure that advertisements or searches that are introduced into the system but are violating the PCPNDT Act will not be shown in the results even when they are not included in the results for the keyword searches mentioned above. The intermediaries protested this interim order, arguing that it runs counter to section 79 of the IT Act and the Court's judgement in *Shreya Singal v. Union of India*. Rather than rescinding its interim order, however, the Court further ordered the intermediaries, in February 2017, to appoint an "In-House Expert Body", which will be responsible for ensuring that any words or keywords that are in violation of the PCPNDT Act will be deleted immediately. Where the Expert Body has any doubt, it can seek guidance from the Nodal Agency appointed by the Union of India on directions of the Court. The Nodal Agency will also intimate the intermediaries of any violating content that has been brought to its notice by the public. For the moment, the burden on intermediaries to proactively prevent violating content from appearing online remains.

A second case in which intermediaries have been requested to prevent content from being uploaded is *In Re: Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendation.*¹¹³ The case concerns a request to the Supreme Court by NGO Prajwala to stop the circulation of videos depicting child sexual abuse, rape and gang rape. The report of a court-ordered Expert Committee to make recommendations on how to address this problem was put on record on 6 July 2017 and all recommendations on which there was consensus were subsequently adopted by the Court on 23 October 2017.

This included a recommendation that content-hosting platforms, search engines and the government work together "in formulating [a] process for proactively verifying, identifying and initiating take down" of all such content. Though it was recognised that effective implementation of this recommendation requires further research, the Court also noted that in developing such mechanisms to enable real-time filtering at the time content is uploaded, techniques based on artificial intelligence, deep learning and machine learning should be used.

The Court's interim order contains no indication of what kind of safeguards will be used to prevent censorship that is overly broad when implementing these mechanisms, nor is there an explicit recognition that such safeguards are important. Seeing that, as explained earlier, legitimate sexual expression is controversial in India as well, this is cause for concern. Unless clear safeguards are put in place, this case, while laudable in its aims, might inadvertently end up undermining the progressive intermediary liability regime that *Shreya Singhal v. Union of India* had put into place.

¹¹² WP (Civil) 341 of 2008, order dated 13 April 2017. http:// supremecourtofindia.nic.in/pdf/cir/2017-04-13_1492086489.pdf

¹¹³ SMW (Crl.) 3 of 2015.

Social media group administrators and intermediary liability

If the big intermediaries might have benefited from the greater legal clarity around India's intermediary liability regime to some extent, the pressure may simply have shifted to a different set of actors: the authorities' alleged concern for public order has led them to expect special vigilance on the part of WhatsApp group administrators.

With more than 200 million users, India is WhatsApp's biggest market, and it one of the most popular forms of digital communication in the country. It is also considered a prime means to spread fake news and disinformation.¹¹⁴ For example, when a Muslim man was murdered in Bisara village near Dadri, in September 2015, on suspicion of storing beef in his fridge, this was followed by an apparently planned rumour-mongering campaign on WhatsApp and Twitter.¹¹⁵ In another case that same year, in Solapur, Maharashtra, rumours about thefts, looting and possible child kidnapping that circulated in WhatsApp groups led to widespread fears.¹¹⁶

The authorities have attempted to contain the spread of such rumours by putting the burden of vigilance on group administrators, even though such administrators arguably are intermediaries. In 2016, two state governments issued directives holding WhatsApp group administrators liable for any message circulated in the group. In Jammu and Kashmir, the circular issued by the District Magistrate of Kupwara additionally required new WhatsApp groups to be registered with the district social media centre by the administrator. In Jharkhand, the circular released by government officials in Dumka held that social media group administrators would be held liable wherever they did not remove group members who had shared incorrect, misleading or seditious information or did not report such an incident to the authorities in cases where this information could affect peace in society.117

In April 2017, an order issued jointly by the District Magistrate and Senior Superintendent of Police in Varanasi, Prime Minister Modi's constituency, noted that where fake information or rumours or statements that could cause religious disharmony were circulated in a social media group, such messages needed to be refuted by the group administrator and the poster of the message would need to be removed from the group. In addition, the order also required all such posts to be reported to the nearest police station. "In the event of inaction from the group admin, he or she will be considered guilty and action will be taken against the group admin," the order said.¹¹⁸

Some relief seemed to arrive when in December 2016, in *Ashish Bhalla v. Suresh Chawdhury & Ors*, ¹¹⁹ the Delhi High Court noted that it could not see how a WhatsApp group administrator could be held liable for allegedly defamatory messages that were circulated in the group about one of the group's members – especially since messages do not require the administrator's approval before being posted. However, as these remarks were merely made by the Court in its rejection of a complaint on the grounds of non-disclosure of cause of action, the judgment cannot be considered a conclusive judicial determination on the matter of liability of social media group administrators in India.

And indeed, arrests of WhatsApp group administrators have continued since then. For example, in Karnataka, in May 2017, the administrator of a WhatsApp group on which "ugly and obscene" images of the prime minister were circulated, was arrested.¹²⁰ And in July 2017, two WhatsApp group administrators were arrested in Chennai because objectionable images of the state finance minister and a female actress were posted in their group by a member.¹²¹

Network shutdowns

The number of internet shutdowns in India has been steadily increasing over the past five years. While the Software Freedom Law Centre, which has been

¹¹⁴ Singh, M. (2017, 24 February). WhatsApp hits 200 million active users in India. Mashable India. www.mashable.com/2017/02/24/ whatsapp-india-200-million-active-users/#F569eCmwisqG

¹¹⁵ The Hindu. (2016, 6 October). Dadri lynching: Police identify rumour-mongers. The Hindu. www.thehindu.com/news/national/ other-states/dadri-lynching-police-identify-main-accused/ article7727750.ece

¹¹⁶ Anima, P. (2015, 28 August). The new tattler in town. *The Hindu Business Line*. www.thehindubusinessline.com/blink/know/the-new-tattler-in-town/article7587041.ece

¹¹⁷ Dan, S. (2016, 28 December). Are WhatsApp Group Administrators Liable For Members' Statements? *The Wire*. https://www.thewire. in/89903/whatsapp-group-administrators-liability

¹¹⁸ Press Trust of India. (2017, 21 April). WhatsApp admins beware: Offensive posts can land you in jail. *Hindustan Times*. www. hindustantimes.com/tech/whatsapp-admins-beware-offensiveposts-can-land-you-in-jail/story-iddtcX54taNah8o3ZllwxJ.html 119 CS (OS) No. 188/2016.

¹¹⁹ CS (US) NO. 188/2016.

¹²⁰ Deccan Chronicle. (2017, 3 May). WhatsApp group admin in Karnataka arrested for sharing offensive posts on PM. Deccan Chronicle. www.deccanchronicle.com/technology/in-othernews/030517/whatsapp-group-admin-in-karnataka-arrested-forsharing-offensive-posts-on-pm.html; ANI. (2017, 3 May). Beware! Here's why a WhatsApp group admin was arrested. DNA India. www.dnaindia.com/india/report-k-taka-whatsapp-admin-arrestedfor-offensive-posts-on-pm-modi-2425854

¹²¹ Thirumurthy, P. (2017, 27 July). WhatsApp group admins and member arrested for posting obscene images of TN Minister. *The News Minute.* www.thenewsminute.com/article/whatsappgroup-admins-and-member-arrested-posting-obscene-images-tnminister-65848

tracking internet shutdowns in the country, found reports of three such crackdowns in 2012, by late August the number for 2017 was already 47.¹²² In addition, the Indian government has had no qualms about blocking SMS and/or voice in various parts of Kashmir and the North-Eastern states of India at different points in time, even before internet shutdowns became a regular occurrence, as well as restricting SMS across the country on several occasions.

The internet is shut down in India for a wide range of, sometimes trivial, reasons. For example, between February 2016 and March 2017, an ongoing agitation by the lat community for reservations led to mobile internet services being suspended eight times in parts of Haryana, in addition to one complete block of internet services. In February 2016, mobile internet services were also suspended across Gujarat for four hours to prevent cheating in the Revenue Accountants Recruitment Exam. In March 2015, all internet services were stopped for 48 hours in Nagaland after a video of the lynching of an accused rapist went viral. In August 2016, mobile internet services were disrupted for two days in parts of Arunachal following the death of the state's former Chief Minister, Kalikho Pul. And in June 2017, mobile internet services, and later also broadband services, were stopped for at least a week, following violent clashes between the Gorkha Janmukti Morcha (GIM) and security forces after the GIM called for a complete strike in its agitation for a separate Gorkhaland. With 49 shutdowns since 2012, the state that has seen the greatest number of internet suspensions in India is Jammu and Kashmir. Many of these shutdowns are precautionary and seek to prevent the spreading of information or rumours.123

As section 69A of the IT Act, discussed above, allows the government to block content on a number of grounds, it could be argued that this section also provides the Indian authorities with the legal ability to switch off, under particular circumstances, access to all or parts of the internet in India. Rule 9 of the Blocking Rules that accompany section 69A explicitly allows for the Secretary of the Department of Information Technology to order intermediaries to block access "in any case of emergency nature, for which no delay is acceptable" without giving such intermediaries an opportunity of hearing. Within 48 hours, this order has to be brought for consideration and approval to a larger committee, which includes representatives of the Ministries of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency

Response Team. However, the rules do not specify within which time period the committee has to provide a recommendation with regard to the order, nor for that matter do the Rules or the IT (Amendment) Act specify anywhere under which conditions a situation can be considered an "emergency" in the first place.

In practice, however, internet shutdowns in India have happened under section 144 of the Criminal Code of Procedure, which reads:

144. Power to issue order in urgent cases of nuisance of apprehended danger. -

(1) In cases where, in the opinion of a District Magistrate, a Sub- divisional Magistrate or any other Executive Magistrate specially empowered by the State Government in this behalf, there is sufficient ground for proceeding under this section and immediate prevention or speedy remedy is desirable, such Magistrate may, by a written order stating the material facts of the case and served in the manner provided by section 134, direct any person to abstain from a certain act or to take certain order with respect to certain property in his possession or under his management, if such Magistrate considers that such direction is likely to prevent, or tends to prevent, obstruction, annovance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquility, or a riot, of an affray.

(2) An order under this section may, in cases of emergency or in cases where the circumstances do not admit of the serving in due time of a notice upon the person against whom the order is directed, be passed ex parte.

(3) An order under this section may be directed to a particular individual, or to persons residing in a particular place or area, or to the public generally when frequenting or visiting a particular place or area.

This provision has been used to shut down the internet in various states, including on the order of police commissioners, who can exercise the powers of executive magistrates in emergencies. Any order issued under this section can be in force for no more than two months from the time of its making, unless it is extended by the state government for a further six months.

These powers were first used in 2004 by the Mumbai police, to block the website hinduunity.org; anti-Islamic material accessible on this website was thought to be potentially inflammatory. In the following years, the Mumbai and Pune police in particular have used their power to block internet content on

¹²² SFLC.in. Internet Shutdowns Tracker. www.internetshutdowns.in 123 Ibid.

several occasions.¹²⁴ The content in question generally related to Shivaji, the Marathi warrior-hero, or to political figures, including Bal Thackeray and B. R. Ambedkar. In one such instance, an Orkut community containing supposedly "objectionable and derogatory" comments about Shivaji was blocked; at the time of blocking, the one-month old community had a mere 101 members.¹²⁵

In recent years, however, section 144 has been used more and more often to shut down the internet altogether, especially in times of social or political controversy or tension. This use of the section, earlier called on predominantly to restrict the right to assembly offline where such assembly could lead to a potentially volatile situation, massively expanded the censorship capacities of the authorities, providing them with a blunt instrument to silence people that they could wield like a sledgehammer. Further adding fuel to the worry is the state government's ability to extend such orders by an additional six months, without the intervention of a court or other independent body. Such provisions open the door to political misuse.

Despite these concerns, in February 2016, the Supreme Court dismissed a plea challenging the power of state governments to shut down internet services using section 144. The plea argued that only section 69A of the IT Act should be used to shut down the internet; section 69A provides only the central government with the powers to block. The Supreme Court dismissed the plea on the ground that internet shutdowns at times are necessary to maintain law and order. A Gujarat High Court order had earlier upheld a ban on mobile internet services imposed by the Gujarat government in August 2015 on the same grounds. The unsuccessful plea in the Supreme Court had sought to challenge that order.

Irrespective of the Court's verdict, network shutdowns in India have drawn international attention. In May 2017, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, and UN Special Rapporteur on the situation of human rights defenders, Michel Forst, called upon India to restore internet and social media networks in Jammu and Kashmir in particular. In April 2017, the state government had blocked 22 social media sites/apps, including Facebook, WhatsApp, YouTube and Skype. "The internet and telecommunications bans have the character of collective punishment," stressed Kaye, "and fail to meet the standards required under international human rights law to limit freedom of expression."¹²⁶

The ban on social networking sites, which was issued under section 5(2) of the Indian Telegraph Act, 1885, was challenged before the Srinagar High Court for being arbitrary, ineffective and amounting to excessive delegation as it focuses on the medium rather than on the content of messages.¹²⁷ Section 5(2) reads as follows:

On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may. if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.

Though the High Court refused to stay the ban, it noted that such a ban could only ever be temporary and required periodic review.¹²⁸ The state government lifted the ban after a month; it allegedly had not been very successful, as users used virtual private networks (VPNs) to circumvent the

¹²⁴ OpenNet Initiative. (2012). India. www.opennet.net/research/ profiles/india

¹²⁵ Press Trust of India. (2006, 18 November). Orkut forum blocked over Shivaji comments. DNA India. http://www.dnaindia.com/ india/report-orkut-forum-blocked-over-shivaji-comments-1064711

¹²⁶ Office of the United Nations High Commissioner for Human Rights. (2017, 11 May). India must restore internet and social media networks in Jammu and Kashmir, say UN rights experts. www.ohch.org/EU/NewsEvents/Pages/DisplayNews. aspx?NewsID=21604&LangID=E

¹²⁷ Parray, M. A. (2017, 9 May). Social media ban challenged; HC declines stay. Kashmir Reader. www.kashmirreader. com/2017/05/09/social-media-ban-challenged-hc-declines-stay; Peerzada, A. (2017, 10 May). Plea challenges social media ban in J&K. The Hindu. www.thehindu.com/todays-paper/tp-national/ plea-challenges-social-media-ban-in-jk/article18417526.ece

¹²⁸ Tantry, I. (2017, 17 May). Social media ban likely to continue in Kashmir. The Tribune. www.tribuneindia.com/news/jammu-kashmir/ social-media-ban-likely-to-continue-in-kashmir/408099.html

restrictions¹²⁹ even though the government reportedly had tried to block VPNs as well.¹³⁰

On 7 August 2017, the Government of India released, quietly and without any preceding public consultation, the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017. The rules have been framed under section 7 of the Indian Telegraph Act, 1885, which reads:

7. Power to make rules for the conduct of telegraphs.—

1) The Central Government may, from time to time, by notification in the Official Gazette, make rules consistent with this Act for the conduct of all or any telegraphs established, maintained or worked by the Government or by persons licensed under this Act.

(2) Rules under this section may provide for all or any of the following among other matters, that is to say: [...]

(b) the precautions to be taken for preventing the improper interception or disclosure of messages; [...]

(k) any other matter for which provision is necessary for the proper and efficient conduct of all or any telegraphs under this Act.

Rule 2(1) of the new rules reads:

Directions to suspend the telecom services shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India or by the Secretary to the State Government in-charge of the Home Department in the case of a State Government (hereinafter referred to as the competent authority), and in unavoidable circumstances, where obtaining of prior direction is not feasible, such order may be issued by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorised by the Union Home Secretary or the State Home Secretary, as the case may be:

Provided that the order for suspension of telecom services, issued by the officer authorised by the Union Home Secretary or the State Home Secretary, shall be subject to the confirmation from the competent authority within 24 hours of issuing such order: Provided further that the order of suspension of telecom services shall cease to exist in case of failure of receipt of confirmation from the competent authority within the said period of 24 hours.

Any directions for suspension of services in addition need to be reviewed within five days by a Review Committee set up by the union or state government.

Insofar as the rules provide a clearer procedure for network shutdowns and limit the authorities that can impose them, taking this power away from district-level authorities, they seem a step forward. However, seeing that both the authority who can order a shutdown and the Committee that reviews that order are from within the executive, there remains cause for concern. As the rules do not specify what can be considered a "public emergency" or a "threat to public safety", broad concerns around public order and public safety will likely continue to trump concerns for freedom of expression and other human rights, at enormous cost to the latter. As they can rarely be considered a solution that is necessarv and proportionate, internet shutdowns should only be resorted to in the most extreme of circumstances. It is unlikely, however, that these rules will ensure that shutdowns will indeed become such an exception. Rather, they seem to legitimise the practice, even if they may perhaps help to somewhat reduce the number of shutdowns in the future. Moreover, while the rules regulate "temporary" shutdowns, they do not provide any restrictions on the time period for which an order for suspension can be valid. In addition, while the reasons for an order of suspension of services need to be recorded in the order, the rules do not make it mandatory for the government to make those reasons public.

ISPs are committed to follow government orders to shut down services as per their licence agreements. For example, the Unified Licence Agreement states explicitly that the government has:

the right to take over the service, equipment and networks of the Licensee (either in part or in whole of the service area) in case any directions are issued in the public interest by the Government of India in the event of a National emergency/war or low intensity conflict or any other eventuality.

Conflicts such as those in Kashmir and the North-East are of the low intensity variety. In addition, ISP licence agreements note explicitly that the government reserves the right to keep any area out of the operation zone of the service if implications of security so require.

¹²⁹ Hindustan Times. (2017, 27 May). J-K government lifts ban on social media in Kashmir. *Hindustan Times*. www.hindustantimes. com/india-news/j-k-government-lifts-ban-on-social-media-inkashmir/story-UgdfX6tswZhmrqTYFITk5J.html

¹³⁰ Kashmir Post. (2017, 4 May). Cyber Cell begins snapping VPN's: Blocking the blocked. Kashmir Post. www.kashmirpost.org/2017/05/04/ cyber-cell-begins-snapping-vpns-blocking-the-blocked

Concerns related to net neutrality

The terms of access to media and communications infrastructure are a crucial element in the exercise of freedom of speech and expression. However, fundamental rights are applicable against the state, but media and communications infrastructure is often privately owned. To what extent, then, can the state justify infrastructure regulation?

Matters of infrastructure regulation were agitated under the protection of freedoms under Article 19 of the Constitution as far back as 1962, in the case of Sakal Papers (P) Ltd. & Oth. v. Union of India.¹³¹ In this case, the editor of a newspaper and its readers challenged the validity of the Newspaper (Price and Page) Act. 1956, which empowered the central government to fix prices of newspapers according to the number of pages and allocation of space for advertising. One of the questions before the court was whether the regulation of prices of newspapers by the government was an infringement on the right to freedom of speech and expression of the press. The court ruled that the legislation affected the right to freedom of the press, which forms part of Article 19(1)(a). Regulation of advertising space, and its indirect impact on circulation, was found to be an infringement on the right to freedom of speech and expression.

In the context of the internet, the Telecom Regulatory Authority of India (TRAI) consultation on discriminatory pricing of data services brought in sharp focus the question of whether or not, and to what extent, to regulate service offerings of telecom service providers in the larger public interest.

This consultation happened against the background of the emergence of "zero-rated" internet plans in India – such as telecom operator Bharti Airtel Ltd.'s Zero plan and Facebook's Internet.org-turned-Free Basics. Network operators on their own, or in partnership with internet companies, were offering data plans which would provide selective access to the internet for a lower price or for free. One of the issues before the authority was: what principles should guide the decision to regulate such plans (or to abstain from regulating)? Or in other words, what are the first principles towards which any policy on differential pricing should be aimed?

TRAI noted that the consultation was initiated because two key principles of tariff regulation were being affected: non-discrimination and transparency.¹³² Many additional considerations were forwarded in the comments made by stakeholders, including innovation, competition, non-discriminatory access to users and, crucially in the context of this report, the right to freedom of speech and expression. The consultation paper acknowledged this:

Several responses have drawn a critical link between the internet and its role in preserving the constitutional guarantees of right to free speech and expression under Article 19(1)(a) of the Constitution. As observed by the Supreme Court, in the Secretary, Ministry of Information and Broadcasting v. Cricket Association of Bengal, (1995) 2 SCC 161, para 201 (3)(b) allowing citizens the benefit of plurality of views and a range of opinions on all public issues is an essential component of the right to free speech. This includes the right to express oneself as well as the right to receive information as observed by the Supreme Court in the Indian Express Newspapers (Bombay) Put. Ltd. v. Union of India, (1985) 1 SCC 641 (para 68) case. Both of these components viz., right to express oneself as well as the right to receive information are critical elements in the use of the internet. The Authority is of the view that use of internet should be in such a manner that it advances the free speech rights of the citizens, by ensuring plurality and diversity of views, opinions, and ideas.133

Arguments in favour of zero-rating included that there was no stopping a customer to avail of the full internet by paying for data; that platforms (at least in the case of Free Basics) would be open to any app, content or service; that such regulating is paternalistic; and that disallowing zero-rating would kill business models and affect the freedom of these companies to conduct trade, etc.

Following several rounds of public consultations, TRAI passed a regulation in February 2016 that prohibited discriminatory pricing of data services on the basis of content.¹³⁴

Given the value that the public internet has provided for economic, social, political and cultural ends, allowing a selection of applications, content and services to be accessed for a negligible amount or for free would likely have led to the exclusion of a large section of the population from being able to make use of the medium to the fullest. It would also have undone the relatively "permission-less" nature of innovation by applications developers and content and service providers on the internet,

^{131 1962} AIR 305.

¹³² Telecom Regulatory Authority of India. (2016, 08 February). Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 (20 f 2016). www.trai.gov.in/sites/default/files/Regulation_ Data_Service.pdf. Para 2 of Explanatory Memorandum.

¹³³ Ibid. Para 24.3 of Explanatory Memorandum. 134 Ibid.

including where these are regular citizens or notfor-profits rather than commercial entities, arguably affecting their freedom of speech and expression.

Without going as far as to provide a definitive list of characteristics which justify regulation of private commercial entities, the explanatory memorandum to the TRAI regulation notes that changes to business models and commercial arrangements should pay heed to the unique architecture of the internet, including its "end-to-end design principle", according to which features specific to an application reside in the communicating end nodes, rather than in the intermediary nodes of the network. This principle is central to net neutrality.

The internet has become the most active public square, where political speech is discussed, and public opinion mobilised. The state has a role to play in ensuring that such a space is not unduly controlled by gatekeepers. As private players mediate access to a public good, the internet, they have an obligation to ensure that there is no discrimination on the grounds of who the service is being offered to. As observed in several submissions to the above-mentioned consultation, the Supreme Court has previously held that when private parties discharge what amounts to a public function, they must be held to a public law standard.¹³⁵

Consultations on a broader framework for net neutrality, with similar potential ramifications for the right to freedom of expression online, have also been held by TRAI since then, as well as by the Department of Telecommunications. The outcome of these consultations is awaited.

Surveillance

It has been established by courts¹³⁶ as well as by research¹³⁷ that mass surveillance has a chilling effect on speech and expression. In India, such concerns have arisen especially in the context of mass surveillance programmes. Some of these, such as the Central Monitoring System (CMS) and National Intelligence Grid (NATGRID), have been designed for the specific purpose of mass communications surveillance; others, such as the Unique Identity Project (Aadhaar) and the seeding of Aadhaar numbers in other databases, have tremendous potential for mass surveillance but were not developed explicitly for this purpose.

The CMS has been operationalised through a mere executive order. In addition, the licence terms of

135 Unnikrishnan v. State of Andhra Pradesh, 1993 SCC (1) 645.

Unified Access Services (UAS) Licensees and Unified Service Licensees were amended in 2013 to require the setting up of interception store and forward (ISF) servers and integration with the Lawful Interception Systems at the licensee's premises.¹³⁸ These servers were to be connected to Regional Monitoring Centres, which are in turn connected to the CMS. The CMS infrastructure, operated by Telecom Enforcement Resource and Monitoring (TERM) cells, enables interception of all communications over the networks in a systematic way such that authorities do not have to interface with the nodal officers of telecom service providers for interception requests.

As per section 4 of the Telegraph Act, all ISPs and telecom companies require a licence from the central government to do business. While licences contain a number of clauses requiring ISPs to safeguard the privacy and confidentiality of the information of their customers, they also require ISPs to maintain extensive logs of user activity, which need to be available in real time to the telecom authority, and to cooperate with government agencies when required to do so. In practice, however, ISPs only kept a log of customers' internet protocol addresses, as well as selectively monitoring specific users' activity at the government's request.¹³⁹ With the establishment of the CMS, the government now no longer needs to rely on telecom companies' cooperation.

NATGRID is an initiative of the Ministry of Home Affairs. According to the Ministry's website, NAT-GRID "has been conceived to develop a cutting edge framework to enhance India's counter-terror capabilities." The project, started in 2011, seeks to connect 21 databases held by different agencies of the government like the Customs Department, Income Tax Department, etc., through agreements. The Central Board of Direct Taxes issued a notification earlier this year to share "bulk information" including Permanent Account Numbers (PAN), taxpayers' names and demographic and biometric details like photographs and thumbprints with NATGRID.¹⁴⁰ Such all-round access by intelligence agencies to

¹³⁶ Shreya Singhal v. Union of India, AIR 2015 SC 1523.

¹³⁷ Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. Berkeley Technology Law Journal, 31(1). https:// www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

¹³⁸ Ministry of Telecommunications and Information Technology. (2013, 11 October). Amendment 2 of 13. www.dot.gov.in/sites/ default/files/DOC231013.pdf?download=1

¹³⁹ Philip, J. T. (2010, 30 December). Intelligence bureau wants ISPs to log all customer details. *Economic Times*. https:// economictimes.indiatimes.com/tech/internet/intelligence-bureauwants-isps-to-log-all-customer-details/articleshow/7187899. cms?intenttarget=no

¹⁴⁰ Central Board of Direct Taxes, Department of Revenue, Ministry of Finance. (2017, 21 June). Notification 54 of 2017. www.incometaxindia.gov.in/communications/notification/ notification54_2017.pdf; Press Trust of India. (2017, 22 June). NATGRID to get PAN, taxpayer data access. *Economic Times*. www. economictimes.indiatimes.com/news/economy/policy/natgrid-toget-pan-taxpayer-data-access/articleshow/59270998.cms

citizens' data exists without external accountability mechanisms or independent oversight.

News reports indicate that several ministries¹⁴¹ and police departments¹⁴² have also begun or plan to start operations to monitor social media. Such programmes are likely to have a chilling effect on speech on the internet as well, and the question of reasonability arises when these are ongoing programmes, seeking to gauge the "public's moods".

As legal scholar Gautam Bhatia has noted, if surveillance is an issue that affects freedom of speech and expression, then it needs to have statutory backing according to Article 19 of the Constitution, and such a law should pass the test of reasonability. He observes that the determination of whether programmes like the CMS are reasonable restrictions in the interests of "security of the state" and "public order" would depend upon what line of precedent the court would take:

Under the Ramji Lal Modi line of cases, with their broad understanding of the phrase "in the interests of", the surveillance regime will be easy to justify (it is hardly deniable that it bears some relation to public order and security). If, on the other hand, the narrower test of Lohia is followed, then the burden upon the government will be much greater.¹⁴³

Indeed, even though government officials maintain that the requirements under section 5(2) of the Indian Telegraph Act, 1885, read with Rule 419A will continue to apply at least in the case of the CMS, the development of these mass surveillance programmes through executive orders seems to be the apex of a continuous hollowing out of checks and balances in India's surveillance regime that protect freedom of speech and expression as well as privacy.¹⁴⁴

Two acts are central to this regime: the Indian Telegraph (Amendment) Act 2006, which governs

telecom service providers (including ISPs), and the IT (Amendment) Act 2008, which has wider application. Both Acts penalise the unlawful interception of communications (e.g. sections 24 and 25 of the Telegraph Act; sections 43 and 66 of the IT Act). They also permit interception by the state under specific conditions.

Section 5(2) of the Indian Telegraph (Amendment) Act 2006 allows for such interception "on the occurrence of any public emergency, or in the interest of the public safety," provided that "it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence."

The Indian Telegraph Rules 2007 specify, in rule 419A, that in normal circumstances, such interception can only be ordered by officers of the rank of Secretary, either in the Ministry of Home Affairs, where the central government is concerned, or in the Home Department, where a state government is concerned. Moreover, such an order can only be issued "when it is not possible to acquire the information by any other reasonable means" and has to contain reasons. The rule further includes a range of safeguards to be observed during interception, as well as imposing limits on periods of both data collection and retention.

Most of the provisions made under the Indian Telegraph Act and its attendant rules have been retained in the IT Act. However, there is one significant difference: section 69 of the IT (Amendment) Act 2008 has done away with the requirement for "a public emergency" or "the interest of the public safety", while adding "the defence of India" and "for investigation of any offence" to the list of grounds on which surveillance is allowed.

As Prashant lyengar has pointed out, the requirement of "a public emergency" or a clear threat to "public safety" as preconditions had earlier put a clear damper on the Indian government's ability to legally intercept communications.¹⁴⁵ In *PUCL v. Union of India*, referring to the Indian Telegraph Act, the Court had observed:

[E]ven if the Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India or the security of the State or friendly relations with sovereign States or in public order or for preventing incitement to the commission of

¹⁴¹ Press Trust of India. (2017, 23 June). Government plans a new social media policy to check anti-India activities. *Economic Times*. www.tech.economictimes.indiatimes.com/news/internet/ government-plans-a-new-social-media-policy-to-check-anti-India activities/59276445; Hindustan Times. (2016, 24 February). Govt to monitor social media 24x7 to counter negative comments, blogs. *Hindustan Times*. www.hindustantimes.com/india/govt-tomonitor-social-media-24x7-to-counter-negative-comments-blogs/ story-6Phot5wXXtMbzTYTKpmgkl.html

¹⁴² Puri, N. (2013, 9 March). India sets up social media monitoring lab. *ZDNet*. www.zdnet.com/article/ india-sets-up-social-media-monitoring-lab

¹⁴³ Bhatia, G. (2016). *Offend, Shock, or Disturb*. New Delhi: Oxford University Press.

¹⁴⁴ Xynou, M. (2017, 30 January). India's Central Monitoring System (CMS): Something to Worry About? Centre for Internet and Society. https://www.cis-india.org/internet-governance/blog/ india-central-monitoring-system-something-to-worry-about

¹⁴⁵ Iyengar, P. (2011). Privacy in India - Country Report - October 2011. Bangalore: Centre for Internet and Society. https://ssrn.com/ abstract=2302978

an offence, it cannot intercept the message, or resort to telephone tapping unless a public emergency has occurred or the interest of public safety or the existence of the interest of public safety requires.¹⁴⁶

This important constraint has been done away with in the case of digital communications.

At the same, by allowing for interception of communications in the course of the investigation of any offence, the range of communications that have the potential to legally come under the state's radar has increased exponentially. While interception in the case of an economic offence, for example, generally would not have been possible under the Indian Telegraph Act, it is very much so under the new IT Act.

The considerable expansion of the state's powers to intercept communications within its borders is particularly worrying in the light of reports that even telephone tapping, regulated by the far more stringent Telegraph Act, is widespread. For example, in February 2011, telecom service provider Reliance Communications told the Supreme Court that it had tapped, on order of the authorities, 151,000 phone numbers between 2006 and 2010. This amounts to 30,000 telephone interceptions every year - or 82 every day – by a single service provider.¹⁴⁷ As safeguards such as the Review Committee, which has to meet at least once every two months to assess the legality of all orders, are unlikely to work effectively under such circumstances, this has raised serious questions about the extent to which the law is being followed, in letter or in spirit.

Legislative amendments have been proposed to the Telegraph Rules for the insertion of Rule 419B, which would give legislative authority to conduct mass interception of communications. As per Access Now's report to the UN Special Rapporteur on freedom of speech and expression:

Besides the deployment of the infrastructure and operations for the CMS programme, the Union Government also proposed amendments to the legal environment on interception in India, in the form of a proposed Rule 419B to the Telegraph Rules. This would have provided legal cover for the CMS programme and real time surveillance operations on Indian licensed network operators. Proposed in 2013, this amendment to the Telegraph Rules has not yet been advanced.¹⁴⁸

While the Indian Telegraph Act regulates only interception, section 69 of the IT Act applies to monitoring and decryption as well.

Since its inception, the Aadhaar project has raised concerns for its potential for mass and pervasive surveillance. Only in 2016, the government enacted legislation to govern the different aspects of the project: the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016. With subsequent notifications by the government requiring the Aadhaar number of individuals to be linked to everything from government benefits to mobile numbers and bank accounts, it has created an unprecedented infrastructure with huge surveillance potential.

Section 33 provides for the disclosure of this information, including identity information and authentication records, when it is required in the interest of "national security" in pursuance of a direction of an officer who is Joint Secretary to the Government of India or a higher rank, on behalf of the central government. Every such direction is to be reviewed by an Oversight Committee. Such orders will be valid for a period of three months from the date of issue, and may be extended for three more months after the Oversight Committee reviews it.

Further, the purpose of use of the information and the terms of sharing, publication and display of the information are not fixed, and may be specified through regulations.¹⁴⁹ This means that the scope of use of the information held by the Unique Identification Authority of India can be expanded at the executive's will, without the Act having any further checks and balances.

Future violations through draft laws

In March 2017, the Law Commission of India submitted Report No. 267 on Hate Speech to the central government, in pursuance of a request to do so by the Supreme Court in March 2017.¹⁵⁰ This report suggests

¹⁴⁶ PUCL v. Union of India. AIR 1997 SC 568.

¹⁴⁷ Mahapatra, D. (2011, 15 February). Over 1 lakh phones are tapped every year. *Times of India*. www. articles.timesofindia.indiatimes.com/2011-02-15/ india/28545822_1_lakh-phones-subscriber-base-provider

¹⁴⁸ Access Now. (2016). Access Now submission to the UN Special Rapporteur on the protection of the right to freedom of opinion and expression study on Telecommunications and Internet Access Sector. www.ohchr.org/Documents/Issues/Expression/ Telecommunications/AccessPart_II.docx

¹⁴⁹ Section 23(2)(k) of the Act allows the Unique Identification Authority of India (UIDAI) to share information about individuals in such manner as may be specified by regulations. Section 29(2) permits the sharing of identity information other than core biometric information, in such manner as may be specified by regulations. Section 29(4) permits the publication and display of an individual's core biometric information or Aadhaar number for purposes as may be specified by regulations.

¹⁵⁰ Law Commission of India. (2017). Op. cit.

amendments to the Indian Penal Code by the insertion of Sections 153C and 505A, expanding the scope of hate speech laws in India, including by explicitly recognising hate based on sex, gender identity, sexual orientation or disability, among others.

In October 2017, the Internet Freedom Foundation released a leaked copy of another report: the recommendations of an expert committee headed by TK Visvanathan, which was formed after section 66A of the IT Act was struck down as unconstitutional.¹⁵¹ This report proposes further changes to both draft provisions proposed in the Law Commission report on hate speech, including to make explicit that these sections apply to communications on the internet as well. While these changes overall are improvements over the proposals by the Law Commission, its proposed new section 505A of the IPC, in particular – and contrary to what the report claims – continues to suffer from the same issues of vagueness and overbreadth that afflicted section 66A of the IT Act.

For example, many of the terms used to describe communication that would be criminalised under the section are imprecise and nebulous. Similarly, although the proposed section specifies that there needs to be an "intention to cause fear of injury" or an "intention to cause alarm", this qualification arguably does not pass the "clear and present danger" test. In *Shreya Singhal v. Union of India*, the Supreme Court had ruled that discussion or even advocacy of a cause was not sufficient to justify any restriction on the right to freedom of speech and expression; only when this reaches the level of incitement does Article 19(2) apply.

A number of other laws and policies that are currently in the drafting stage have the potential to negatively impact the right to freedom of speech and expression on the internet in the future as well.

The Draft Prohibition of Indecent Representation of Women and Children Bill, 2012,¹⁵² sought to widen the scope of its parent act to include communications made over electronic media. The bill proposed new definitions for "indecent representation of women", "electronic form" and "publish". This bill released by the Ministry of Women and Child Development is still pending.

The Ministry of Home Affairs released the Draft Geospatial Information Regulation Bill¹⁵³ in 2016,

and called for comments from all stakeholders. The bill sought to regulate the acquisition, publication, modification and dissemination of any representation of spatial attributes of India. After business interests and user groups across the country sent comments against the proposed bill, there have been no developments. This bill would have affected several internet-age businesses involved in logistics management, humanitarian relief efforts and, of course, users, and would limit freedom of speech by limiting their use of maps.

The Draft National Encryption Policy 2015¹⁵⁴ released by the Department of Electronics and Information Technology sought to increase the security of the internet and related information systems by regulating the strength of encryption that may be used. However, the policy if implemented would have imposed great burdens on users and businesses to store in plaintext any information exchanged via electronic media for up to 90 days after the communication was made. Contrary to the stated objectives, such a policy would have been disastrous to the security of communications and information networks, and to user privacy.

At present, although this does not seem to be enforced, telecom licences disallow ISPs from using bulk encryption, as well as prescribing a maximum 40-bit encryption for individuals, groups or organisations without obtaining permission from the government. For stronger encryption, prior permission from the government is required and the decryption key, split into two parts, is to be deposited with the government.

Following the unanimous verdict by the nine judges of the Supreme Court in *KS Puttaswamy v. Union of India*, ¹⁵⁵ we can expect legislation on data protection in the near future. The judgment also affirms that the right to privacy, which is enshrined in the right to life, affects the enjoyment of the right to freedom of speech and expression under Article 19(1)(a).

Summary and conclusions

While the Shreya Singhal judgement might have signified an important victory for freedom of expression in the digital space in India, many challenges remain. Criminal defamation is used all too often by powerful actors to silence critical voices. Laws regarding sedition and the protection of national symbols are misused to curtail political dissent. Provisions regarding hate speech often reward those who respond with threats of violence to

¹⁵¹ TK Visvanathan Committee. (n/d). Recommendations of TK Visvanathan Committee. New Delhi: TK Visvanathan Committee. https://internetfreedom.in/files/documents/recommendations. of.t.k.visanathan.committee.pdf

¹⁵² www.prsindia.org/billtrack/the-indecent-representation-ofwomen-prohibition-amendment-bill-2012-2576/

¹⁵³ www.prsindia.org/uploads/media/draft/Draft%20Geospatial%20 Bill,%202016.pdf

¹⁵⁴ www.netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf 155 KS Puttaswamy v. Union of India. WP (CIVIL) 494 of 2012.

speech they do not agree with, rather than ensuring a safe space to speak for all. Expressions of sexuality are frequently penalised irrespective of consent or intent; women's agency rarely seems to matter here. Even copyright laws are applied in ways that disregard freedom of expression and criticism of court decisions is all too easily seen as contempt.

Even where there is no threat of arrest, freedom of expression is frequently hampered through overly broad government blocks, limited protections of intermediaries and sledgehammer methods such as network shutdowns. In addition, concerns around network neutrality and surveillance can further silence many voices, including, in the latter case, through self-censorship.

As the country has such a solid reputation as a democracy, this long list of challenges to freedom of expression that can be found in India may come

as a surprise. A central tension that runs throughout almost all of these challenges, however, is that between public order and freedom of expression – a tension that was debated as early as during the time of India's Constituent Assembly. It is because many lawmakers as well as government officials continue to believe that public order trumps freedom of expression wherever the two clash that restrictions can be imposed in India with relative ease - and the judiciary provides only limited relief. Only when the courts, too, start to see a need to carve out space for freedom of expression even when public order is in disorder, will stronger protections of the right to freedom of expression likely emerge. Especially in the age of the internet, hecklers should not be allowed to veto speech, if the potential of the internet to allow a voice to even the most marginalised in the country is really to bloom.

Malaysia: A study on the criminalisation of free expression online

Chew Chuan Yang Suara Rakyat Malaysia (SUARAM) www.suaram.net

Introduction

Malaysia has a long history of curtailment of the right to freedom of expression. Prior to the inception of Malaysia as a nation-state, the Sedition Act 1948 was introduced by the British to curtail alleged subversive messages by individuals and groups who opposed British colonial rule. The repression of freedom of expression in that era was not only through the Sedition Act 1948, but also through security laws that were applied broadly against individuals who were not in agreement with Britain's proposition on the Federation of Malava. Despite achieving independence in 1957, the pre-existing laws that curtailed freedom of expression were not repealed but gradually strengthened over the years. Similarly, abuse of security laws in restricting freedom of expression remains prevalent throughout the country's history.

Closer to the 21st century, Malaysia was rocked by the political divide created by former deputy prime minister Datuk Seri Anwar Ibrahim¹ at the height of the Asian financial crisis in 1998. When Anwar Ibrahim broke ranks with Tun Dr. Mahathir Mohamad, the prime minister of the day, demonstrations and protests calling for the resignation of the prime minister followed. The debacle ended with the imprisonment of Anwar Ibrahim for alleged corruption charges and a politically motivated sodomy charge. It was also in those turbulent years that Malaysia was first introduced to the internet and enjoyed the first taste of free flow of information and independent news.

Moving forward to 2017, statistics in the past few years show rapid internet adoption throughout the country. With constantly improving accessibility due to low entry costs and widespread availability of service providers, Malaysia is now estimated to have roughly 24.1 million internet users – representing close to 70% of the nation's population. While there is limited access to the internet in selected parts of Malaysia, access and adoption rates have been relatively even and equal throughout the country.²

Unfortunately, the expansion of a civil space due to the prevalence of the internet was not without challenges. The spread of political opposition and popular mass movements through the internet was noted by the government. With this recognition came a response by the government and the ruling political party, which embarked on social media campaigns through trolls and "cybertroopers", punitive legal measures to legally restrict and silence dissent, and disproportionate use of force to intimidate those involved and others that voice dissent.

The purpose of this report is to map the laws that affect online freedom of expression in Malaysia. In addition to the Sedition Act 1948, the Communications and Media Act 1998 (CMA) and the Malaysian Penal Code incorporate sections that have been used to criminalise online expression activities. In addition to the laws themselves, the report seeks to study legal judgments and draft legislation insofar as they relate to online freedom of expression. As the internet is a fast-evolving medium – and the law is always lagging to catch up – we also study recent incidents as an indication of governmental interpretation and use of laws to curtail and violate freedom of expression online.

We will begin by elaborating on the methodology for research, followed by a detailed look at the laws that are most often utilised to criminalise freedom of expression.

¹ Deputy prime minister of Malaysia from 1993 to 1998.

² Department of Communications and Multimedia. (2016). Internet Users Survey 2016: Malaysian Communications and Multimedia Commission.

www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS2016.pdf

Methodology

This report will analyse the criminalisation imposed upon freedom of expression online and whether there is any difference between general restrictions applied to freedom of expression and criminalisation of the same. This report will adopt legal analysis of court judgments on the criminalisation of freedom of expression and whether there are any distinctions on how the state perceives an offence under laws such as the Sedition Act 1948 when it applies online and offline.

However, there are some technical gaps in the study, as the criminalisation of freedom of expression online through the Communications and Multimedia Act 1998 is relatively new in Malaysia.³ As such, there are limitations in terms of reported court judgments on this matter. As of the time of writing, there are only three published high court judgments relating to the Communications and Multimedia Act 1998 and they do not address the crux of the issue of freedom of expression.

As such, with regard to examination of the criminalisation of freedom of expression under this law, an assessment will be made through media reports of cases and pre-trial treatment of those suspected of an offence.

The Malaysian legal framework for freedom of expression

Malaysia is a federation comprising 13 states and three federal territories. The Federal Constitution of Malaysia serves as the foundation of the country's laws and establishes the scope of powers for the three arms of government and the basic rights guaranteed to its people. In general, the direction of Malaysia as a nation-state is determined by the federal government, with the introduction of most if not all policies for the country driven by the political party that dominates the parliament.

Furthermore, Malaysia's system of parliamentary democracy is largely based on the Westminster system with two houses of parliament, an independent judiciary and an executive (cabinet), which is appointed by the prime minister who commands support in the parliament. While this system has largely worked well in the United Kingdom, in Malaysia the system's flaws manifest themselves through the upper house in parliament, which is overwhelmingly dominated by the ruling political party; a judiciary whose independence has been in

3 Documented use to regulate social media abuses online emerged around 2013, with the first high court case reported only in 2015. question since 1988⁴ and resurfaced recently;⁵ and an executive that utilises all arms of government (including but not limited to the Election Commission,⁶ law enforcement agencies, and other civil services)⁷ for political dominance.

In terms of rights, Article 10 of the Federal Constitution of Malaysia lays the foundation for freedom of speech, assembly and association. Article 10(1) (a) stipulates that every citizen has the right to freedom of speech and expression.⁸ In many situations, this article has been interpreted in a narrow manner which results in excessive power for the state to restrict and curtail freedom of speech and expression.⁹

State governments are usually not afforded any power to regulate and restrict freedom of expression. However, state governments have a degree of monopoly with regards to the establishment and enforcement of Islamic or Sharia laws.¹⁰ Traditionally, these laws held little repercussion for freedom of expression. However, there have been recent developments, such

⁴ The concern for the Malaysian judiciary's independence first surfaced in 1988 during the constitutional crisis where the chief justice of the day was sacked. Pakrisamy, S. (2008, 29 April). Comment: Tun Salleh and the judiciary. *The Malaysian Bar.* www. malaysianbar.org.my/members_opinions_and_comments/ comment_tun_salleh_and_the_judiciary.html

⁵ Following the extension of the current chief justice's term after he has reached the age of retirement stipulated by the Federal Constitution of Malaysia, former judges, the bar council and activists have been criticising the chief justice's decision to accept the extension. Anbalagan, V. (2017, 26 June). Say 'no' to extension for chief justice, urges ex-top judge. *Free Malaysia Today*. www.freemalaysiatoday.com/category/nation/2017/06/26/ say-no-to-extension-for-chief-justice-urges-ex-top-judge

⁶ Palansamy, Y. (2017, 20 January). Selangor lists six 'supersized' seats as examples of EC's alleged gerrymandering. Malay Mail Online. www.themalaymailonline.com/malaysia/article/selangorlists-six-supersized-seats-as-examples-of-ecs-alleged-gerrymande ri#GrgijaigjsTlhH6l.97

⁷ School teachers were in the past given show-cause letters for criticising government. See: Anbalagan, V. (2017, 30 March). Lawyer: Civil servants criticising govt can be charged with misconduct. *Free Malaysia Today*. www.freemalaysiatoday.com/category/ nation/2017/03/30/lawyer-civil-servants-criticising-govt-can-becharged-with-misconduct; Borneo Post Online. (2013, 16 June). Masing: Wrong for civil servants to oppose govt. *Borneo Post Online*. www.theborneopost.com/2013/06/16/masing-wrong-forcivil-servants-to-oppose-govt; Malay Mail Online. (2015, 15 June). Racism can unite a race 'for good', BTN says. *Malay Mail Online*. www.themalaymailonline.com/malaysia/article/racism-can-unite-arace-for-good-btn-says#RkxPwS5GocRuSpIL.97 (The National Civics Bureau or BTN is a government agency which has in the past been known for espousing a neo-apartheid ideology of racial supremacy.)

⁸ Subject to clauses that refer to Article 149, which deals with legislation against subversion, action prejudicial to public order, etc. www.agc.gov.my/agcportal/uploads/files/Publications/FC/ Federal%2oConsti%2o(Bl%2otext).pdf

⁹ PP v Azmi bin Sharom, Para 37. www.kehakiman.gov.my/directory/ judgment/file/GOJ_-_PP_v_Azmi_Sharom.pdf

¹⁰ Article 74(2) outlines the power of state legislatures in terms of law making, and Islamic law is one of the items which state assemblies still have power to determine with limited oversight by the federal government. In practice, the power to legislate religious law is far more complex, with influence from the respective state monarch and institutions.

as where a translator of publications deemed to be Islamic in nature has been subjected to local state laws as opposed to federal law.¹¹ The development suggests that elements of Islamic or Sharia laws may impact on freedom of expression on par with federal laws passed by the parliament.

Laws which restrict freedom of expression are common in Malaysia and the application of the laws is largely supported and backed by legal jurisprudence which tends to interpret civil liberties enshrined in the Federal Constitution in a conservative or restrictive manner. An example of this can be seen in the cases involving Anwar Ibrahim, where the burden of proof and presumption of innocence were disregarded and elements of rule of law were violated.¹² A more recent example can be seen in the case of *PP v Azmi bin Sharom*, where the Federal Court ruled that the court has no power to determine whether a restriction imposed by the parliament is reasonable or otherwise.¹³

Examples of laws restricting freedom of expression in Malaysia include, but are not limited to:

- Sedition Act 1948, which renders comments, speeches, selected statements or publications as seditious, potentially resulting in a fine or imprisonment for offenders.
- Communications and Multimedia Act 1998, a broad law covering all aspects of telecommunication and multimedia which contains provisions that have been interpreted in manners that punish "hurtful" comments made online.
- Printing Presses and Publications Act 1984, a law that imposes criteria and requirements for print media which has been utilised to ban books, outlaw t-shirts related to civil activism and shut down print media.
- Selected sections of the Penal Code with explicitly repressive provisions such as Section 124B and other more innocuous sections such as Section 298,¹⁴ 298A¹⁵ and 499.¹⁶

16 Criminal defamation.

In terms of the interpretation of the law, the Federal Court of Malaysia serves as the apex court. Due to the nature of most criminal cases relating to freedom of expression, the Federal Court only hears and decides on cases if there was an appeal or challenge on constitutional issues. For cases where no such challenges were filed by the defendant or the prosecutor, the case usually ends at the Court of Appeal, which has in the past ruled in favour of acquitting or discharging the defendant in line with a more progressive interpretation of freedom of expression.¹⁷

Curtailment of freedom of expression online

In the past, freedom of expression has been largely restricted through the use of security laws. One of the laws that coloured Malaysian history in this aspect would be the Internal Security Act 1960 (ISA). Since its inception, there were documented incidents where political opponents were alleged to have been detained under the ISA.¹⁸ Over the years, the ISA was also used to silence civil dissent, notably in 1987 under "Ops Lalang", where 106 individuals including NGO activists and intellectuals were arrested and detained.¹⁹ The pattern of suppression of freedom of expression was also seen in 1998 during the height of the Reformasi movement seeking to oust the prime minister of the day, Tun Mahathir Mohamad, following the fallout and persecution of Anwar Ibrahim,²⁰ and yet again in 2008 when political blogger Raja Petra Kamaruddin.²¹ MP Teresa Kok and journalist Tan Hoon Cheng were arrested and detained.²² Officially they were arrested for being a threat to security, peace and public order under Section 73(1) of the ISA. When inquired, the deputy inspector-general of police of the day reported that the journalist, Tan, was arrested for reporting a racist remark made by a politician from the ruling party; Teresa Kok was arrested for alleged involvement with a resident's petition over a mosque; while Raia Petra was only alleged to be involved with activities that could cause unrest.

19 https://aliran.com/oldsite/hr/js3.html

- 21 One of the few known cases where an individual was detained under the ISA solely for his commentaries online. Raja Petra Kamaruddin is a controversial political blogger who has been active since far before the rise of the internet in Malaysia.
- 22 The Star Online. (2008, 13 September). Raja Petra, Teresa Kok and Sin Chew reporter arrested under ISA. *The Star Online.* www.thestar.com.my/news/nation/2008/09/13/ raja-petra-teresa-kok-and-sin-chew-reporter-arrested-under-isa

¹¹ The case of Zaid Ibrahim, which will be further explored later in this report.

¹² Anwar Ibrahim's first trial in 1998 was met with a series of controversies and reversal of the rule of law; a similar turn of events was witnessed yet again in his more recent conviction for sodomy. See Thomas, T. (2008, 29 July). Comment: A second prosecution of Anwar Ibrahim – is it in the national interest? *The Malaysian Bar.* www.malaysianbar.org.my/members_opinions_ and_comments/comment_a_second_prosecution_of_anwar_ ibrahim_is_it_in_the_national_interest_.html?date=2017-06-01

¹³ PP v Azmi bin Sharom, op. cit.

¹⁴ Uttering words, etc., with deliberate intent to wound the religious feelings of any person.

¹⁵ Causing, etc., disharmony, disunity, or feeling of enmity, hatred or ill will, or prejudicing, etc., the maintenance of harmony or unity, on grounds of religion.

¹⁷ In Safwan Anang's sedition case, the Court of Appeal maintained a high threshold for a statement to be deemed seditious by the court and acquitted Safwan Anang, www.kehakiman.gov.my/directory/ judgment/file/W-09-7-2016.pdf

¹⁸ Hansard, 30 July 1971. www.parlimen.gov.my/files/hindex/pdf/DR-30071971.pdf

²⁰ BBC. (1999, 15 November). A crisis unfolds: Timeline. (1999, 15 November). BBC News. news.bbc.co.uk/2/hi/special_ report/1998/10/98/malaysia_crisis/204632.stm

Following the repeal of the ISA in 2012,²³ the Government of Malaysia no longer has access to this legislation and uses other laws such as the Sedition Act 1948, the Communications and Multimedia Act 1998, etc.²⁴ While the repeal of the ISA may have broadened the perceived space for civil discourse in Malaysia, the reality does not necessarily reflect this sentiment. As noted in the comment by the prime minister of the day, Najib Tun Razak, the abolition of the ISA was a political move aimed at recovering support²⁵ for the ruling coalition and the law itself was not "helping" the ruling coalition but actually enhancing the opposition's progress. With this in mind, the "expansion" of space should be viewed with scepticism.

It should be noted that the repeal of the ISA took place in tandem with the introduction of new security laws such as the Security Offences (Special Measures) Act 2012 (SOSMA), which grants police similar power to detain individuals without trial.²⁶ The suspicion that SOSMA would be used in a similar manner was affirmed in 2015, following the arrest and detention of Khairuddin Abu Hassan and Matthias Chang.²⁷ In 2016, SOSMA was yet again used to arrest and detain the prominent chairperson of the Bersih 2.0 committee, Maria Chin Abdullah.²⁸

In addition to the liberal interpretation of security laws, it is also noted that in Malaysia there is rarely any distinction made for "offences" committed online and offline. It is common for laws that are applied offline to be applied online as well without any adjustments. Individuals arrested or detained for allegedly seditious posts online are often arrested and investigated for both an offence under the Sedition Act 1948 and under the Communications and Multimedia Act 1998.²⁹ This makes it possible and highly likely that the laws described below could be applied online at any juncture.

Security Offences (Special Measures) Act 2012

SOSMA is not a law that outlines specific crimes or punishment; it is technically a procedural law that replaces the Criminal Procedure Code if an individual is arrested for offences under Chapters VI, VI(A), VI(B) and VII of the Penal Code. These four chapters of the Penal Code cover, respectively, offences against the state, offences relating to terrorism, organised crime, and offences relating to the armed forces.

Some of the more controversial offences are located in Chapter VI of the Penal Code. Notable sections include Section 124B which outlines the offence of activity detrimental to parliamentary democracy; Section 124C which outlines the attempt to commit activity detrimental to parliament democracy; and others which address publications that are detrimental to parliamentary democracy (Section 124D) and possession of such publications (Section 124E).

In practice, under SOSMA, a police officer can, without warrant, detain an individual whom he has reason to believe to be involved in security offences for 24 hours.³⁰ A police officer with the rank of a superintendent or above may extend the detention for an additional 28 days³¹ for the purpose of investigation. An important point to note is that under SOSMA, individuals charged for an offence are not granted bail by default³² and there are no recorded cases where the court found the use of the law legitimate and granted bail; therefore, anyone charged would only be released at the conclusion of all legal proceedings. While Section 4(3) of SOSMA outlines that no person shall be detained for his political belief or activity, this law has still been utilised against civil society and political dissent.

Notable examples are those mentioned before, namely, the arrest and detention of Khairuddin Abu Hassan and Matthias Chang. Khairuddin Abu Hassan was arrested under Section 124K and 124L of the Penal Code following the reports he filed against 1 Malaysia Development Bhd (1MDB).³³ His lawyer, Matthias Chang, was subsequently arrested under Section 124K and 124L when he acted as a counsel for him.³⁴ While the two are no longer

²³ The Star Online. (2012, 10 April). New Bill to replace ISA. The Star Online. www.thestar.com.my/news/nation/2012/04/10/ new-bill-to-replace-isa

²⁴ As noted by the SUARAM report for 2015, documented use of the Sedition Act 1948 and Communications and Multimedia Act 1998 increased substantially. See: www.suaram.net/wordpress/ wp-content/uploads/2015/12/SUARAM-HR-OVERVIEW-2015combined-ver1.pdf

²⁵ Syed Jaymal Zahiid. (2012, 9 July). Repeal of ISA politically driven, says Najib. *Free Malaysia Today.* www. freemalaysiatoday.com/category/nation/2012/07/09/ repeal-of-isa-politically-driven-says-najib

²⁶ Soong, K. K. (2016, 21 November). Sosma is the new ISA. *Free Malaysia Today.* www.freemalaysiatoday.com/category/ opinion/2016/11/21/sosma-is-the-new-isa

²⁷ More details of the case are available in the subsection on SOSMA.

²⁸ More information on their arrest will be further explored later in this report.

²⁹ Notable cases include those of Khalid Ismath and Zunar.

³⁰ Section 4(1) SOMSA.

³¹ Section 4(5) SOSMA.

³² The law itself classifies all charges made in line with SOSMA to be non-bailable and extension of remand after the trial of first instance remains at the sole discretion of the public prosecutor.

³³ Malay Mail Online. (2015, 23 September). Khairuddin rearrested under Sosma moments after court orders his release. Malay Mail Online. www.themalaymailonline.com/malaysia/article/ khairuddin-rearrested-under-sosma-moments-after-court-ordershis-release#EKQ9prz7Ojzebtmu.97

³⁴ Hamudin, N. (2015, 8 October). Matthias Chang arrested under Sosma. The Sun Daily. www.thesundaily.my/news/1576303

detained under SOSMA,³⁵ their case brought back the old spectre of repression of political dissent and criminalisation of freedom of expression under the ISA for members of civil society and the public.³⁶

The use of SOSMA to silence political dissent and criminalise freedom of expression was once again witnessed in the arrest and detention of Maria Chin Abdullah, the chairperson of Bersih 2.0.³⁷ On the eve of the Bersih 5 rally on 18 November 2016,³⁸ Maria Chin Abdullah and Mandeep Singh³⁹ were arrested at the Bersih office. During the raid of the office, lawyers were denied access to Maria Chin Abdullah and Mandeep Singh, and were also not allowed to witness the search. On the day of the rally itself, the police informed the counsels that Maria Chin Abdullah was detained under SOSMA in relation to an alleged offence under Section 124C of the Penal Code (124C outlines the offence of threat to parliamentary democracy).⁴⁰

It should be noted that thus far, the use of SOS-MA has not applied to any issues that deal with freedom of expression online directly. However, the manner in which it has been applied suggests that it may be interpreted and utilised the same way as its predecessor the ISA. Furthermore, it is also noted that unlike the ISA, SOSMA is a procedural law by nature and its utilisation is dependent on the interpretation of an offence under Chapter VI of the Penal Code. On that note, there is no distinction or definition made in the relevant section that restricts it to "offline" events and incidents only, and thus it can be applied to any offence that surfaces online.

Sedition Act 1948

Since the abolition of the ISA, the Sedition Act 1948 is a popular go-to law for the silencing of political dissent by the government. As noted in the Suara Rakyat Malaysia (SUARAM) Annual Human Rights

36 Doraisamy, S. (2015, 24 September). The spectre of ISA: Broken promises and freedom forgone. SUARAM. www.suaram. net/?p=7250; see also: Thiru, S. (2015, 15 October). Press Release: Respect the rule of law and release Dato' Sri Khairuddin and Matthias Chang. The Malaysian Bar. www.malaysianbar.org.my/ press_statements/press_release. %p7C_respect_the_rule_of_law_ and_release_dato_sri_khairuddin_and_matthias_chang.html

- 37 A popular mass movement demanding free and fair elections in Malaysia. www.bersih.org/about/background
- 38 Free Malaysia Today. (2016, 18 November).Police arrest Maria Chin after Bersih raid. Free Malaysia Today. www. freemalaysiatoday.com/category/nation/2016/11/18/ police-arrests-maria-chin-after-bersih-raid
- 39 The manager of Bersih 2.0.
- 40 Brown, V. (2016, 19 November). Bersih 5: Maria Chin detained under Sosma. *The Star Online*. www.thestar.com.my/news/ nation/2016/11/19/bersih-5-maria-chin-detained-under-sosma

Report in 2015 and 2016, the use of the Sedition Act 1948 hit a record high⁴¹ in the years that followed the repeal of the ISA.

In general, the crime of sedition is a colonial offence that was established in Malaysia prior to its independence.⁴² The law itself has been amended on several occasions in the past. However, coming into the digital age, the Government of Malaysia has not made any distinction in the application of the Sedition Act 1948. Human rights defenders (HRDs) and political dissenters have been arrested and charged for allegedly seditious speeches made during public forums, and also for articles written and published online.

A notable example where the Sedition Act 1948 was applied to online articles would be the case of Azmi Sharom in 2014. Azmi Sharom, a respected academic at the University of Malaya, was first charged for sedition over an article relating to an ongoing political crisis in Perak, which was published online.⁴³ He was charged under Section 4(1) (b) with an alternative charge under Section 4(1)(c) of the Sedition Act 1948 that outlines an offence of uttering any seditious statements and printing, publishing, selling, offering for sale, distributing or reproducing any seditious publications, respectively. After 17 months of delays, the public prosecutor requested for Azmi Sharom to be given a discharge not amounting to an acquittal.⁴⁴

In Azmi Sharom's case, there was an attempt by his counsels to have the Sedition Act 1948 declared as unconstitutional and void. Unfortunately, the Federal Court rejected the counsels' motion and further restricted the interpretation of freedom of expression in its decision. In Azmi Sharom's decision, the Federal Court deemed the requirement for restriction of freedom of expression based on the concept of reasonableness would amount to "re-writing" Article 10(2) of the Federal Constitution and effectively sought to remove the need for reasonableness.⁴⁵

Apart from Azmi Sharom's case, another notable case where the Sedition Act 1948 was applied

³⁵ The Star Online. (2017, 28 April). Duo will not be tried under Sosma. The Star Online. www.thestar.com.my/news/ nation/2017/04/28/duo-will-not-be-tried-under-sosmakhairuddin-chang-will-instead-face-banking-sabotage-charge

⁴¹ The use of the Sedition Act 1948 in 2015 and 2016 is reported to be 220 and 12 times, respectively. See: www.suaram.net/wordpress/ wp-content/uploads/2016/12/Overview-2016-Digital-Edition.pdf

⁴² The Sedition Act was passed in 1948 but Malaysia only achieved independence in 1957.

⁴³ Free Malaysia Today. (2014, 1 September). Azmi Sharom next up for sedition charge. Free Malaysia Today. www. freemalaysiatoday.com/category/nation/2014/09/01/ azmi-sharom-next-up-for-sedition-charge

⁴⁴ Fadzil, F. (2016, 19 February). Court acquits Azmi Sharom of sedition charge. *The Star Online*. www.thestar.com.my/news/ nation/2016/02/19/court-acquits-azmi-sharom-of-sedition-charge

⁴⁵ PP v Azmi Sharom [2015] 8 CLJ 921 [37]-[40].

against HRDs can be seen in the arrest of Eric Paulsen in March 2015. Paulsen was arrested and subsequently charged for sedition for a tweet on the implementation of Hudud law in Malaysia.⁴⁶ Similar to the case before, Paulsen was charged under Section 4(1)(c) of the Sedition Act 1948 and was also briefly remanded.

Zulkiflee Anwar, better known as Zunar, was similarly arrested and subsequently charged for nine counts of sedition following his tweets criticising the judiciary for its alleged bias in the second sodomy trial of Anwar Ibrahim in 2015.⁴⁷ Since then, Zunar has consistently been "in trouble" with the law for his cartoons on current politics.⁴⁸

Besides political dissenters and HRDs, the Sedition Act 1948 has also been applied against controversial online personalities Viven Lee May Ling and Alvin Tan Jye Yee. The two posted on Facebook a controversial photo of them dining on a local dish, *bak kut teh*, that was well known to be non-halal – since pork is its main ingredient – during the month of Ramadan. The photo was accompanied by the caption "Selamat Berbuka Puasa [the greeting used when breaking the fast at the end of the day during Ramadan] (with Bak Kut Teh... fragrant, delicious and appetising)" alongside a halal logo.⁴⁹ On top of the charge of sedition, they were also charged under the Film Censorship Act⁵⁰ and Section 298A(1) of the Penal Code.⁵¹

Communications and Multimedia Act 1998

When it comes to online comments and internet-related items, the go-to provision for criminal action would be under Section 233 of the Communications and Multimedia Act 1998 (CMA). Section 233 is an ambiguous provision that can potentially cover any

- 48 Zolkepli, F., & Divakaran, P. (2016, 17 December). Zunar arrested at fan event. The Star Online. www.thestar.com.my/news/ nation/2016/12/17/zunar-arrested-at-fan-event 7
- 49 Lim, I. (2016, 27 May). Vivian Lee jailed six months over 'bak kuh teh' Ramadan photo. Malay Mail Online. www.themalaymailonline. com/malaysia/article/vivian-lee-jailed-six-months-over-bak-kut-tehramadan-photo#gP74mmWkkB3ppGX.97
- 50 Naidu, S. (2016, 14 April). Malaysian 'sex blogger' acquitted of charge under censorship act. *Channel News Asia*. www. channelnewsasia.com/news/asiapacific/malaysian-sex-bloggeracquitted-of-charge-under-censorship-act-8055984
- 51 Causing, etc., disharmony, disunity, or feelings of enmity, hatred or ill will, or prejudicing, etc., the maintenance of harmony or unity, on grounds of religion.

comments made online that are interpreted as hurting someone's feelings.⁵² The application of this law in this area is still relatively new. For most of its existence, it has had little to no role in the ongoing discourse on freedom of expression.⁵³

Unfortunately, in the last two years, this law has been applied broadly, with more than 180 cases of alleged social media abuse⁵⁴ reported by the Malaysian Communications and Multimedia Commission (MCMC) for the year 2016 alone. Offences that have surfaced under this law include *lèse majesté*, alleged fake news, satire, graphics that are perceived as insulting the prime minister, and a wide variety of other "affronts".

Political activist and HRD Khalid Ismath was one of the earlier cases under the CMA. He was detained for comments allegedly insulting the members of the royal family and was subsequently charged for nine counts of sedition and four under the CMA, for tweets and Facebook posts. He was later kept in solitary confinement for almost three weeks before he was released on bail of MYR 70,000 (over USD 16,500).⁵⁵

After this case in late 2015, a myriad of other cases began to surface under Section 233 of the CMA. Malaysia witnessed mass arrests under this law in May 2016, when a group of football fans were arrested for comments that allegedly insulted a member of the royal family, who was also a manager of a football team.⁵⁶ The individuals detained were subjected to extended remand and held in detention for close to two weeks in the state of Johor.

Among the best-known cases under the CMA are those relating to Fahmi Reza, a well-known activist in Malaysia. His satirical depiction of Malaysia's prime minister and of the "block notice" issued by the MCMC⁵⁷ online incurred the ire of the government, which led to his being subjected to

- 53 The first reported case was in its early stages as of 2017, with the first case reported at High Court in 2016 (Zaid Ibrahim's case).
- 54 Which usually falls under the purview of Section 233.
- 55 Malaysia Kini. (2015, 22 October). Amnesty declares Khalid Ismath 'prisoner of conscience.' Malaysia Kini. www.malaysiakini.com/ news/316782
- 56 #NetMerdeka. (2016, 6 June). Net freedom coalition condemns arrests under the CMA. SUARAM. www.suaram.net/?p=8051
- 57 Tzu Ging, Y. (2016, 10 June). Fahmi Reza charged again over clown face sketch. *Malay Mail Online*. www.themalaymailonline.com/ malaysia/article/fahmi-reza-charged-again-over-clown-facesketch#b1C3fMzwvmAQ8I56.97

⁴⁶ Tan, S. (2015, 23 March). Lawyer Paulsen to be detained until 6pm in sedition probe over hudud tweets. *Malay Mail Online*. www.themalaymailonline.com/malaysia/article/lawyer-paulsento-be-detained-until-6pm-in-sedition-probe-over-hududtweets#HJ5uweyAJilsCQs.97

⁴⁷ Mei Lin, M. (2015, 3 April). Cartoonist Zunar slapped with nine counts of sedition over Anwar tweets. *Malay Mail Online*. www.themalaymailonline.com/malaysia/article/cartoonistzunar-slapped-with-nine-counts-of-sedition-over-anwartweets#GfuXobcElLcrigt5.97

^{52 233(1)(}a) "... any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; 233(1)(b) - initiates a communication using any application service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity with intent to annoy, abuse, threaten or harass any person at any number or electronic address."

investigations and criminal prosecutions for creating and sharing the content in question.

Apart from activists and political dissenters who have been charged, an online news editor has also been charged for uploading a video of coverage of a press conference.⁵⁸ In this case, KiniTV Sdn Bhd, a media company, was charged under Section 233(1) (a) of the CMA while the editor-in-chief, Steven Gan, was charged under Section 244(1), which carries a similar punishment if found guilty.⁵⁹

Reflecting on the cases that Malaysia has witnessed in recent years, it is difficult to say how far-reaching this law can be in the criminalisation of freedom of expression. This law has shown itself to be highly flexible in its utilisation by the state, and also a law that can be utilised by non-state actors to push for government action even when the police report lodged has no merits or is false in nature.⁶⁰ This flexibility is interpreted by the communications and multimedia deputy minister as applicable for punishing WhatsApp group administrators if they failed to curb the spread of false information.⁶¹

In terms of the application of the law, there are also substantial concerns on the manner of application itself, which may create additional human rights violations on top of the criminalisation of freedom of expression. On the lighter end of the spectrum, there have been cases where individuals were harassed through persistent calls for questioning and investigations and were finally released with no further actions. At the other end, there have been cases where individuals were found guilty and faced fines and prison terms. One individual was fined MYR 120,000 (over USD 28,000) and sentenced to 30 months imprisonment in default; another individual was sentenced to 14 years imprisonment for 14 charges of allegedly insulting a member of royalty on Facebook.⁶² Fortunately, in the case of the 14 counts, the person in question was allowed to serve his sentences concurrently.

Apart from the direct impact posed by Section 233 of the CMA, Section 263 also plays a substantial role in the criminalisation of freedom of expression in Malaysia. Unlike Section 233, Section 263 is targeted towards network service providers. The law itself technically compels network service providers to follow government directives in enforcing the law and requires the providers to enforce all Malaysian laws as part of their services. While the law itself may be innocuous, the provision is often cited by the government and utilised to compel internet service providers (ISPs) to block websites that have been deemed as illegal.⁶³

Penal Code offences

On top of the crime of sedition and the myriad of other possible offences under Section 233 of the CMA, the criminalisation of freedom of expression includes the application of selected sections of the Penal Code. Selected aspects of the Penal Code offences⁶⁴ used to criminalise freedom of expression have been addressed in the earlier portion of this report. On top of those provisions, there are other sections such as Section 298, Section 298A and Section 499.

Notable cases under Section 298⁶⁵ include the case of Aishah Tajuddin, a radio DJ who made a video highlighting the peculiarity that would result from the proposal by the Islamic Party regarding the implementation of Hudud law in the state of Kelantan.⁶⁶ On top of the attacks and threats posed against her by anonymous internet users (an issue to be further covered later in this report), she was called for investigation by the police under Section 298 of the Penal Code,⁶⁷ and was also reportedly investigated by the MCMC for causing mischief online.⁶⁸

More recently, a local English newspaper which published a controversial front page was called

⁵⁸ Yatim, H. (2016, 18 November). M'kini editor-in-chief charged over AG videos. Malaysia Kini. www.malaysiakini.com/news/363282

⁵⁹ Section 244(1) states that a senior officer (director, CEO or similar individual) can be jointly charged with the corporate body unless he or she is able to prove that the offence was committed without his or her knowledge, consent or connivance and he or she had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.

⁶⁰ Yen, H. K. (2017, 24 May). Alibi given by man over charges he 'insulted Najib, Rosmah'. Free Malaysia Today. http:// www.freemalaysiatoday.com/category/nation/2017/05/24/ alibi-given-by-man-over-charges-he-insulted-najib-rosmah/7

⁶¹ CNA. (2017, 27 April). Malaysia may take action against WhatsApp admins for spreading fake news: Report. *Channel News Asia*. www. channelnewsasia.com/news/asiapacific/malaysia-may-takeaction-against-whatsapp-admins-for-spreading-8796344

⁶² The Straits Times. (2016, 7 June). Youth sentenced to 1-year jail for insulting Johor royalty on Facebook. *The Straits Times*. www. straitstimes.com/asia/se-asia/youth-sentenced-to-1-year-jail-forinsulting-johor-royalty-on-facebook

⁶³ BBC. (2016, 14 March). Blocked Malaysian insider news website shuts down. BBC News. www.bbc.com/news/world-asia-35800396

⁶⁴ Chapter VI offences relating to threat to parliamentary democracy and its peers.

⁶⁵ Uttering words, etc., with deliberate intent to wound the religious feelings of any person.

⁶⁶ The video contains a scene where a hijab or headscarf mysteriously appears on the DJ upon entry to the state.

⁶⁷ The Jakarta Post. (2015, 23 March). Cops to probe Malaysian station and journalist over hudud satire video. *The Jakarta Post*. www. thejakartapost.com/news/2015/03/23/cops-probe-malaysianstation-and-journalist-over-hudud-satire-video.html

⁶⁸ Free Malaysia Today. (2015, 22 March). Blasphemy probe into BFM video. Free Malaysia Today. www.freemalaysiatoday.com/ category/nation/2015/03/22/blasphemy-probe-into-bfm-video

for investigation under Section 298A and the Sedition Act 1948.⁶⁹ Following a show-cause letter from the Home Ministry and a follow-up meeting, the editor-in-chief and chief executive office were suspended indefinitely.⁷⁰ It is noted that while the investigation was made in relation to a print publication, there was no demarcation that would suggest that the front page would have avoided similar punishment if it were published online.⁷¹

On the one hand, civil society has traditionally advocated for the use of these sections in lieu of the Sedition Act 1948 and the Communications and Multimedia Act 1998, as they are far more defined and not easily subjected to the whimsical interpretation of law by the government. However, unrestricted use of this legislation may well place it among the list of laws that unjustly and disproportionately criminalise freedom of expression.

Other laws

The Printing Presses and Publications Act 1984 (PPPA) is another law that is often utilised to criminalise and restrict freedom of expression in Malaysia. Traditionally, this law was invoked to restrict or criminalise print publications. However, there is no guarantee that this law would not be interpreted to restrict online publications (e-books, etc). When we consider that the Sedition Act 1948 was not differentiated in its application to articles published online or in print media, there is a substantial possibility that the PPPA may be interpreted in a similar manner that could cut across the online and offline realms in the future.

On the eve of the Bersih 4 rally in 2015, the t-shirts and logo of Bersih 4 were declared illegal under the PPPA on the grounds of national security. At the same time, the Bersih website⁷² was also blocked by the MCMC through its powers under the CMA.⁷³ The joint application of laws in such a manner also raises the possibility that the act of criminalisation of publications under the PPPA may be used as a "legitimate" excuse to compel ISPs to

- 69 Malaysia Kini. (2017, 30 May). IGP: The Star investigated for sedition, inciting religious enmity. *Malaysia Kini*. www. malaysiakini.com/news/383967
- 70 The Star Online. (2017, 31 May). Two top editors of 'The Star' suspended. The Star Online. www.thestar.com.my/news/ nation/2017/05/31/two-top-editors-of-the-star-suspended
- 71 The news which was published on the front page was similarly published online.
- 72 Malaysia Kini. (2015, 28 August). MCMC blocks four websites for promoting Bersih. *Malaysia Kini*. www.malaysiakini.com/ news/310322
- 73 Malaysia Kini. (2015, 28 August). Bersih website blocked ahead of rally? *Malaysia Kini*. www.malaysiakini.com/news/310207

block or remove the offending items from access under the CMA.

However, it is noted that while the PPPA may have a strong influence that would easily compel print publications to follow an invisible line set by the government, the law itself may have very little repercussion for consumers and activists. For example, the novel 50 Shades of Grey has been subjected to a ban under the PPPA, but can still be found in bookshops across the country. Similarly, a quick search online would show that the book is still easily available in e-book format on Google Play and other distribution channels.

In addition to the PPPA, another worrying aspect arising in recent years is related to the Islamic laws and principles that have been gaining traction in the Malaysian legal system.

With regard to Islamic or Sharia law, there is relatively wide power to regulate and criminalise freedom of expression. There are three identified manners in which Islamic or Sharia law has been applied to curtail freedom of expression. First, it can be used directly to criminalise freedom of expression, similarly to how the Sedition Act 1948 functions. This is seen in the case of Dr. Kassim Ahmad⁷⁴ where he was charged for insulting Islam⁷⁵ during a speech he delivered at a seminar.

Furthermore, Islamic or Sharia law has been and can be used to restrict publications, as seen in the case involving Ezra Zaid,⁷⁶ which raised substantial questions as to the scope of power afforded to Islamic law and whether these laws can affect, curtail and criminalise freedom of expression. Ezra Zaid and ZI Publications were charged under Section 16 of the Syariah Criminal Offences (Selangor) Enactment 1995.⁷⁷ At the time of this report, the constitutionality of this section is still pending hearing in the civil courts.

On top of the potential power to restrict publications, the power of the state religious authorities to issue a fatwa, which is not legally binding, raises an additional point of concern. While a fatwa does not necessarily hold legal sway, it can greatly affect public perception, which may lead to increasing

⁷⁴ Siti Aziela Wahi. (2014, 27 March). Kassim Ahmad didakwa di mahkamah pagi ini. *Sinar Online*. www.sinarharian.com.my/ semasa/kassim-ahmad-didakwa-di-mahkamah-pagi-ini-1.264386

⁷⁵ Section 7(b) of Shariah Criminal Offences (Federal Territories) Act 1997.

⁷⁶ Lim, I. (2017, 26 April). Ezra Zaid allowed to continue challenge of Jais arrest, prosecution over book. *Malay Mail Online*. www. themalaymailonline.com/malaysia/article/ezra-zaid-allowed-tocontinue-challenge-of-jais-arrest-prosecution-over-boo

⁷⁷ Section 16 deals with religious publication contrary to Islamic law. https://goo.gl/bzUxBa

threats by non-state actors.⁷⁸ In addition, the recent debacle where the National Registration Department (NRD) refused to register a child with his father's name as his surname due to an existing fatwa⁷⁹ suggests that these decrees may indirectly influence the execution of secular legal provisions and become a basis for restriction of freedom of expression under secular law.

On a more positive note in terms of freedom of expression, Dr. Kassim Ahmad's case was heard by the Federal Court and the court affirmed the decision made by the Court of Appeal, which had ruled that his arrest was invalid. The grounds of judgment for his case were that an inappropriate law had been used to apprehend him. His arrest should have been made by local religious authorities, as opposed to the federal religious authority.⁸⁰

At this point, there is very little developed legal jurisprudence and precedents that chart the powers and the scope of the jurisdiction of Islamic or Sharia law, especially with regard to the influence of these laws on freedom of expression. In an ideal scenario, the civil courts would hear and adjudicate on the powers and scope of Islamic or Sharia law in regard to these issues in line with the Federal Constitution. Unfortunately, the development of the law in this area will unlikely be completed in the foreseeable future, and as such this report must conclude that Islamic or Sharia law can potentially be utilised in a manner that criminalises freedom of expression of the Muslim community.

Distinction in application between comments in the "real" and "online" world

Apart from offences under the CMA, which is exclusively used against online comments, most of the Malaysian laws are interpreted to apply to both online and offline offences without any additional distinction.⁸¹ The current state of affairs in terms of interpretation and implementation raises the possibility that a comment made online can potentially result in a greater punishment when compared to a statement uttered in a physical public forum.

Khalid Ismath's case serves as an excellent illustration of this danger. As internet posting can potentially cut across various platforms and channels, an individual may be slapped with several charges despite the comments or posts being essentially the same, due to automated sharing between Facebook and Twitter, for example. The comments made by him would have traditionally been bound to an offence under the Sedition Act 1948. However, due to the online nature of his posting, some of his posts were subjected to charges that crossed into the CMA. In essence, not only was he technically placed under criminal action for an allegedly seditious statement, he was also charged for social media abuse.

Furthermore, the punitive measures under the CMA can be more onerous when compared to the Sedition Act 1948 and other laws. While the maximum prison sentence may not be as extraneous as those under the Sedition Act 1948, the MYR 50,000 (USD 11,800) fine that could be imposed may be far more damaging than a short prison sentence. For example, student activist Adam Adli⁸² and wellknown activist Hishamuddin Rais⁸³ were both found guilty of sedition and fined MYR 5,000 (USD 1,180) respectively, whereas in the case of Wan Fatul Johari, who was charged under the CMA, he was fined for MYR 120,000 (USD 28,400) and underwent a 30-month prison sentence in default.84 The difference in penalties under different laws is further illustrated in Table 1.

Extralegal state actions in criminalisation of dissent

Another concerning aspect with regard to the criminalisation of freedom of expression online arises from the manner in which an "offender" is arrested, detained and prosecuted. As an example, in the case described earlier relating to comments on football, the individuals arrested were taken into custody from various parts of Malaysia and subsequently brought for remand and detention at Johor Bahru, a practice which contradicts the Criminal

⁷⁸ Blog posts condemning Sisters in Islam as a deviant group in line with the fatwa issued can be easily found and accessed online, which raises the question as to whether the fatwa itself galvanised attacks and threats against the group led by non-state actors.

⁷⁹ The Star Online. (2017, 27 July). NRD D-G not bound by fatwa to decide surnames of illegitimate Muslim kids. *The Star Online*. www. thestar.com.my/news/nation/2017/07/27/nrd-dg-not-bound-by-fatwa-to-decide-surname-of-illegitimate-muslim-child

⁸⁰ Astro Awani. (2015, 21 December). Mahkamah Rayuan putuskan pendakwaan ke atas Kassim Ahmad tidak sah dan batal. Astro Awani. www.astroawani.com/berita-malaysia/mahkamah-rayuan-putuskanpendakwaan-ke-atas-kassim-ahmad-tidak-sah-dan-batal-86091

⁸¹ An issue that has been noted by this report on various accounts especially in cases highlighting the use of law in criminalisation of freedom of expression

⁸² Mei Lin, M. (2016, 18 February). Youth activist Adam Adli gets RM5,000 fine in place of jail term in sedition sentence. Malay Mail Online. www.themalaymailonline.com/malaysia/article/ youth-activist-adam-adli-gets-rm5000-fine-in-place-of-jail-term-insedition#FTISEeJXXTD6f80e.97

⁸³ The Star Online. (2016, 16 May). Hishamuddin Rais' jail term overturned by Appeals Court. *The Star Online.* www.thestar.com.my/news/nation/2016/05/16/ hishamuddin-raiss-jail-term-overturned-by-appeals-court

⁸⁴ www.utusan.com.my/berita/mahkamah/wan-fatul-johari-kanandibawa-keluar-dari-mahkamah-selepas-didapati-1.152543

TABLE 1. Comparison of penalties under different laws*				
Sedition Act 1948	3 (or 5)****	5,000	Yes	
Section 233 of CMA	1	50,000	Yes	
Section 124C of Penal Code	15	-	No	
Section 298 of Penal Code	1		Yes	
PPPA – Possession of material	_	5,000	No	
PPPA – Production, publication, sales and distribution of material	3	20,0000	No	
Section 7(b) of Syariah Criminal Offences (Federal Territories) Act	2	3,000	Yes	

* This is not a comprehensive comparison but only highlights some of the laws discussed in this report. "Refers to the possible maximum sentence. "" Could be sentenced to both imprisonment and fine. "" In the event of a subsequent offence."" Not listed in the Penal Code, but read in line with Section 283(1)(a) Criminal Procedure Code, there is technically no limit but it shall not be excessive.

Procedure Code. Curiously, the arrests made in this case included those of a fisherman and his son, who were allegedly owners of the offending Facebook account.⁸⁵ The two were arrested off the coast of Malaysia while they were out fishing.⁸⁶

Furthermore, the practice of chain remand⁸⁷ was also utilised against those detained in this case. Some of the detainees were subjected to a detention period of close to two weeks, when their remand period should not be more than seven days.

On top of the peculiarities mentioned above, the Royal Malaysian Police maintains a Twitter watchdog account that occasionally calls out online users whom they deem offensive.88 Similarly, the former Inspector-General of Police of Malaysia is also an avid user of Twitter and often makes comments praising the police force or calling out individuals whom he finds "offensive" or who have supposedly made "seditious" comments online. A good example of this can be seen when a well-known human rights lawyer and activist. Michelle Yesudas, commented on the rape threats made by non-state actors and members of the public in relation to the Aishah Taiuddin case. In that incident, the former Inspector-General of Police tweeted a demand for the activist to explain her tweet to the Royal Malaysian

Police and accused her of causing restlessness and panic among the public.⁸⁹

While there is limited repercussion on those who are called out by the former Inspector-General of Police, there are concerns that the public call-out and the threat of investigation posed by the Inspector-General of Police's scrutiny on Twitter may eventually have a chilling effect on the rest of the internet users in Malaysia.⁹⁰

An interesting point to note is that the former Inspector-General of Police has in the past considered applications such as WhatsApp as part of social media as opposed to messaging applications.⁹¹ While the law does not discriminate between the platforms in which a message is delivered, the stance of the former Inspector-General may open up new avenues in which the state may intervene, with the presumption that private spaces, such as closed chat groups, form part of the public sphere of social media.

Non-state actors

In recent years, non-state actors have nurtured a growing role in the "enforcement" of morality in Malaysia. Many of the cases referred to below were initiated by individuals as opposed to government agencies. In addition to cases involving

⁸⁵ My Metro. (2016, 1 June). Izlaily Nurul Ain Hussein. 'Minah Pendek' direman empat hari. My Metro. www.hmetro.com.my/node/141948

⁸⁶ Malaysia Kini. (2016, 31 May). Polis cekup 'Minah Pendek' hina TMJ di tengah laut. *Malaysia Kini*. www.malaysiakini.com/ news/343641#MO4VUz5lFoViXesm.97

⁸⁷ Chain remand is where an individual is repeatedly re-arrested at the end of the remand period. SUARAM has in the past documented cases where individuals were remanded in this way for 80 days. Free Malaysia Today. (2016, 15 March). Six men allege torture during 80-day remand. Free Malaysia Today. www.freemalaysiatoday.com/category/nation/2016/03/15/ six-men-allege-torture-while-in-80-day-remand

⁸⁸ PCIRC Official @OfficialPcirc (Police Cyber Investigation Response Centre). https://twitter.com/officialpcirc

^{89 &}quot;Mohon @chelle_yesudas jelas kan kpd @PDRMsia, apa yg dimaksudkan dgn tweet di bawah, jgn timbul kan keresahan rakyat" – rough translation: "Please @chelle_yesudas, explain to the Royal Malaysian Police what you mean by the tweet below, don't cause worry (unrest) among the people." https://twitter. com/KBAB51/status/579854384235827200

⁹⁰ A phenomenon that has yet to manifest, as individuals are still more than happy to criticise and challenge political authorities on social media.

⁹¹ Rodzi, N. H. (2016, 12 January). IGP: Police targeting 'immature Malaysians' on social media. *The Star Online*. www.thestar.com. my/news/nation/2016/01/12/igp-police-to-monitor-social-media

unidentifiable non-state actors, there are cases such as that of Khalid Ismath, in which the report against him was made by an individual who serves in the Royal Palace.⁹²

Until the recent case of an arrest for online threats against Siti Kassim,⁹³ a prominent human rights lawyer and activist, internet users were largely allowed to threaten activists and other internet users with impunity. Comments calling for individuals like women human rights defenders (WHRDs) to be raped, killed or subjected to acid attacks⁹⁴ were common, with no actions taken against those issuing the threats. In some cases, the threat goes beyond social media posts in the public sphere and extends to private messages sent to HRDs. In the run-up to the Bersih 5 rally in 2016, several individuals affiliated with Bersih were sent a series of images based on a video of an execution by the socalled Islamic State.⁹⁵

Without a substantial change to the status quo relating to WHRDs, they will constantly be subjected to this additional element of danger and threats from non-state actors due to their gender, on top of the criminalisation of freedom of expression by the state.

It is noted that the Royal Malaysian Police is seemingly altering its stance on the matter and investigating reports made by activists regarding online comments that threaten their personal safety. It remains to be seen whether the initial actions of arresting individuals making death threats online will be followed by legal actions and sanctions.

Beyond the threats made against activists or other individuals, targeted attacks against communities are growing more common in Malaysia. One example would be the attacks faced by Sisters in Islam, such as frequent blog posts that demonise them or classify them as deviants.⁹⁶ Other common forms of attack are those faced by LGBTIQ activists. Recent examples include the online witch-hunt against the organiser of a pride event in May 2017. An individual perceived as the organiser had his photo shared on a website that was notorious for demonising LGBTIQ communities.⁹⁷

Another activist who has in the past spoken up against the attacks against and demonisation of LGBTIQ activists also had his information listed publicly on the website, which resulted in individuals approaching his family home and threatening his personal safety. Due to the threats posed against him, the activist was forced to temporarily relocate out of fear for his own safety.

Apart from attacks against known or perceived activists, other individuals are also often exposed to online violence. In March 2017, a teenage girl was attacked online for a sign she had carried in a march, expressing her aspiration to become the first woman prime minister of Malaysia.⁹⁸

Unfortunately, there is a trend of cyberbullying and online violence that is growing in Malaysia, with little to no criminal action taken against perpetrators. The predicament faced at this juncture is a curious one, as Section 233 of the Communications and Multimedia Act 1998 was initially implemented to prevent and criminalise such behaviours, but has not been utilised in a manner conducive to reducing and mitigating cyberbullying and online violence.

Future violations through draft laws

At the time of writing in August 2017, there were two known laws affecting freedom of expression in Malaysia. Amendments to the Sedition Act 1948 were passed and gazetted in June 2015. Fortunately, the amendments are not yet in force, despite having appeared in the Federal Gazette.⁹⁹ While there has been no resistance or challenges against the legitimacy of applying the Sedition Act 1948 online, the amendments included the addition of the term "by electronic means" among other additions to the law, such as as heavier penalties and an alteration of the definition of "seditious" statements under the Act.

On finer inspection, the Sedition Act 1948 now criminalises propagation of a seditious comment or causing a seditious comment to be published as an offence. Furthermore, in the event where a seditious comment is published through electronic

⁹² An office that traditionally does not have any executive power but exercises substantial influence on selected matters.

⁹³ Zack, J. (2017, 26 July). Cops arrest man who threatened to behead Kasim. *The Star Online*. www.thestar.com.my/news/nation/2017/07/26/ cops-arrest-man-who-threatened-to-behead-siti-kasim

⁹⁴ Malay Mail Online. (2017, 24 July). Lawyer Siti Kasim says getting death, rape threats. *Malay Mail Online*. www.themalaymailonline. com/malaysia/article/lawyer-siti-kasim-says-getting-death-rapethreats#x5TUO90ezOyZml8J.97

⁹⁵ Alhadjri, A. (2016, 18 October). Maria Chin, Ambiga to lodge report over death threat, say image is 'too much'. *Malaysia Kini*. www. malaysiakini.com/news/359435

⁹⁶ Searches on the subject of Sisters in Islam and alleged deviant practices would usually result in several blog posts condemning the NGO as deviants in line with the claims of state religious authorities. For example: https://al-faedah.blogspot.my/2014/11/ siapa-sis-sisters-in-islam.html; https://al-faedah.blogspot. my/2014/11/siapa-sis-sisters-in-islam.html

⁹⁷ Menara.my. (2017, 13 June). Iftar GAY terbesar Malaysia – Numan Afifi. *Menara.my*. www.menara.my/ iftar-gay-terbesar-malaysia-numan-afifi

⁹⁸ Joint Action Group for Gender Equality (JAG). (2017, 15 March). JAG condemns online attack on #WomensMarchKL. *Malaysia Kini*. https://m.malaysiakini.com/letters/375734

⁹⁹ A1485, 4 June 2015.

means and the person who is making or circulating the seditious publication cannot be identified, action can be taken under the CMA to prevent access to it. Fortunately, beyond the alterations discussed above, the amendment itself does not include any provisions or additional punishment for seditious comments made online.

The other legal amendment that deals with the criminalisation of freedom of expression is the potential amendment of the Communications and Multimedia Act 1998. Although it has been a matter of discussion since 2015, there has been no concrete draft law tabled or released publicly. As of August 2017, the amendment had yet to be tabled in Parliament or produced in any form.¹⁰⁰ Rumours derived from the comments of ministers with regard to the amendment include the possibility of registration of bloggers and increased penalties for offences as part of the proposed changes.¹⁰¹

To this end, one can say that the proposed and known amendments to laws that directly affect the criminalisation of freedom of expression would not necessarily alter the current status quo in terms of criminalisation. However, the proposed amendments may well increase the "costs" of being found guilty for an offence.

Furthermore, amendments to the Criminal Procedure Code could be equally damaging in this regard. Amendments to the Criminal Procedure Code made in December 2016 removed a degree of judicial discretion in terms of sentencing for first time offenders when they are charged for a serious offence. Serious offence denotes an offence punishable by imprisonment for a term of 14 years or more.¹⁰² While most offences discussed above would not usually fall under this criterion, there are possibilities that future amendments would restrict or limit existing protections that could mitigate prosecution against human rights defenders.

Summary and conclusion

Reflecting on the overall circumstances described above, one would reasonably conclude that freedom of expression in Malaysia both offline and online is subjected to various degrees of criminalisation. While criminalisation is not necessarily common in the greater scheme of things, cases documented by SUARAM suggest a trend in which an average person could be arrested, detained, harassed and prosecuted for a relatively innocuous comment made on Facebook or other online social media.

For better or for worse, the lack of distinction between the application online and offline of laws that criminalise freedom of expression means that all of the existing laws that penalise or restrict freedom of expression can cross over to application in the online sphere. As noted in some of the cases above, a comment made online could potentially be "double the trouble", as an individual can be charged for a traditionally offline crime under laws such as the Sedition Act 1948, and at the same time, charged for an offence under the Communications and Multimedia Act 1998.

With the rise of social media applications and the growing popularity of instant messaging applications on a global level, with almost nationwide adoption, state authorities would naturally feel more inclined to extend their existing powers to cover these platforms. On one hand, the government would reiterate the need for "holistic" solutions and prevention with regard to issues of security, online fraud and "fake news", and would utilise this as leverage for further control and punitive measures; on the other hand, the imposition of additional regulations with expanded regulatory powers afforded to a politically aligned entity would mean that legitimate interest in freedom of expression would likely be compromised to achieve the former.

With the rising prevalence of hate crimes and death threats against activists and other actors in the civil and political rights discourse, there is a growing need for laws that can restrict and criminalise such behaviours online and offline. Realistically, at this juncture, suggestions or implementation of any further regulations would likely be met with scepticism with regard to the sincerity of the laws and their implementation. This unfortunate dilemma leads to the question: How do we address the need for legitimate protection when the institution implementing it is not necessarily trustworthy?

¹⁰⁰ Malaysia Kini. (2016, 9 March). Salleh: Amendments to internet laws won't be tabled now. *Malaysia Kini*. www.malaysiakini.com/ news/333286

¹⁰¹ Astro Awani. (2016, 22 February). Amendment to Communications and Multimedia Act 1998 in March. Astro Awani. english. astroawani.com/malaysia-news/amendment-communicationsand-multimedia-act-1998-march-95481

^{102 52}B of the Penal Code.

Myanmar: A study on the criminalisation of online freedom of expression

Htaike Htaike Aung Myanmar ICT for Development Organisation www.myanmarido.org

Introduction

Today, Myanmar is going through a transition period from a quasi-military government to a civilian democratic government. During this period, freedom of expression has suffered a setback, and Myanmar has failed to meet internationally acceptable standards. PEN Myanmar, in its freedom of expression scorecard, gave the current government a score of 6 out of 80 in its half-year assessment, and 8 out of 60 for its full-year assessment on freedom of expression.¹ The abysmally low score was due to the spike in arrests of journalists and activists for their online expression, and the government's use of laws related to information and communications technologies (ICTs) to curb online free speech.

During the previous government's term, there were only four known cases of criminalisation of freedom of expression online. However, the Telecommunications Law Research Team reports that there have been 73 cases of such criminalisation of online free speech under the present government – from April 2016 to August 2017 alone.² Out of the 73 cases, 30 were filed by private individuals, 12 by the government, 11 by political parties, nine by supporters of political parties, six by the media and five by the military; more than half of the cases were motivated by political reasons. Although there have been some efforts³ made by the parliament to amend the primary law that has been overly used to oppress freedom of speech online, the proposed amendments failed to address the root cause of the law that allows it to be misused for various political reasons.

Methodology

This report looks at the existing laws and regulations that curtail and criminalise freedom of expression online. The laws are put into different categories: fundamental laws and freedoms, governance and regulations of online spaces, and sectoral laws. The research team is limited by the lack of an accessible system to collect data on court cases and by the non-existence of a freedom of information law. However, a number of high-profile cases are highlighted in this report, gathered from local and international news and media reports, human rights violation documentation groups and existing ICT policy research papers.

Although there are only a few laws that had been used to criminalise online speech, we also look at other possible laws and provisions that could be used to curtail online expression. These are laws and provisions that have the potential to be used to curtail freedom of expression online, and we anticipate that they will be used by digital rights advocacy groups in the country in their advocacy efforts.

Lay of the legal land

Fundamental laws and freedoms

Constitution

Myanmar's current constitution is very recent in comparison to those of neighbouring countries since it was drafted in 1994 and enacted in 2008. This is the third constitution adopted after the 1947 constitution, which was a parliamentary democratic constitution, and the 1974 constitution, which was adopted during the socialist democratic government system. The 1974 constitution ended in 1988 with the country's fall into military dictatorship. In 1993, during the military junta era, the military government (State Peace and Development Council –SPDC) started the drafting process for the new constitution, which took 15 years, until it was adopted in 2008.

PEN Myanmar is a chapter of PEN International, a worldwide association of writers that promotes literature and freedom of expression. See: PEN Myanmar. (2017, 3 May). Scorecard assessing freedom of expression in Myanmar. https://pen.org/ wp-content/uploads/2017/05/May-2017-Scorecard-English.pdf, accessed Aug 2017.

² https://www.facebook.com/ ResearchTeamForTelecommunicationsLaw66D

³ Freeman, J. (2017, 25 July). Myanmar moves to amend controversial online defamation law. VOA. https://www.voanews.com/a/ myanmar-moves-to-amend-controversial-online-defamationlaw/39582o6.html

TABLE 1.	TABLE 1.			
Exceptions with regard to defamation established by the Penal Code				
Exception 1	It is not defamation to impute anything which is true concerning any person, if it be for the public good that the imputation should be made or published. Whether or not it is for the public good is a question of fact.			
Exception 2	It is not defamation to express in good faith any opinion whatever respecting the conduct of a public servant in the discharge of his public functions, or respecting his character, so far as his character appears in that conduct and further. [sic]			
Exception 3	It is not defamation to express in good faith any opinion whatever respecting the conduct of any person touching any public question, and respecting his character, so far as his character appears in that conduct and no further.			
Exception 4	It is not defamation to publish a substantially true report of the proceedings of a Court of Justice, or of the result of any such proceedings.			
Exception 5	It is not defamation to express in good faith any opinion whatever respecting the merits of any case, civil or criminal, which has been decided by a Court of Justice, or respecting the conduct of any person as party witness or agent in any such case, or respecting the character of such person, as far as his character appears in that conduct and no further.			
Exception 6	It is not defamation to express in good faith any opinion respecting the merits of any performance which its author has submitted to the judgment of the public, or respecting the character of the author so far as his character appears in such performance and no further.			
Exception 7	It is not defamation in a person having over another any authority, either conferred by law or arising out of a lawful contract made with that other, to pass in good faith any censure on the conduct of that other in matters to which such lawful authority relates.			
Exception 8	It is not defamation to prefer in good faith an accusation against any person to any of those who have lawful authority over that person with respect to the subject-master of accusation.			
Exception 9	It is not defamation to make an imputation on the character of another, provided that the imputation be made in good faith for the protection of the interest of the person making it, or of any other person, or for the public good.			
Exception 10	It is not defamation to convey a caution in good faith to one person against another, provided that such caution be intended for the good of the person to whom it is conveyed, or of some person in whom that person is interested, or for the public good.			

The constitution consists of 15 chapters, and the fundamental freedoms of the citizen are described under Chapter 8, which is titled, "Citizen, Fundamental Rights and Duties of the Citizens". In Article 354 under Chapter 8, citizens' right to freedom of expression is guaranteed as:

Every citizen shall be at liberty in the exercise of the following rights, if not contrary to the laws, enacted for Union security, prevalence of law and order, community peace and tranquility or public order and morality:

(a) to express and publish freely their convictions and opinions.⁴

Although Article 354(a) of the constitution guarantees freedom of expression, justifications and limitations have been laid out. That is, freedom of expression is not absolute, and as the justifications and limitations are vague – "if not contrary to the laws, enacted for Union security, prevalence of law and order, community peace and tranquility or public order and morality" – they may lead to arbitrary limitations on the right to freedom of speech and expression. The constitution also guarantees the right to privacy, in Article 357:

The Union shall protect the privacy and security of home, property, correspondence and other communications of citizens under the law subject to the provisions of this Constitution.

The Penal Code

The Penal Code in Myanmar was adopted on 1 May 1861, and drew from the Indian Penal Code, 1860, drafted in the colonial era. Although there have been several amendments made to the Penal Code, Article 500, which criminalises defamatory speech, still exists in the Penal Code.

Article 500 of the Penal Code states: "Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both."⁵

However, Article 499 of the Penal Code establishes 10 exceptions with regard to defamation which are presented in Table 1.

⁴ English translation sourced from: www.burmalibrary.org/docs5/ Myanmar_Constitution-2008-en.pdf

⁵ English translation sourced from: www.burmalibrary.org/ docs17/1861-Penal_Code-ocr-en+bu.pdf

The Penal Code is not the only piece of legislation where defamation is mentioned. In Article 66(d) of the Telecommunications Law of 2013, defamation is again stated, but it is unclear whether the abovementioned exceptions are applicable as well. Although the exceptions to the crime of defamation define the scope of the offence in a narrower sense, this is still not in line with international standards, as the Myanmar Penal Code continues to criminalise defamation with harsh punishments such as jail terms, affecting both online and offline speech.

Law Protecting the Privacy and Security of the Citizen

While the right to privacy is guaranteed in the constitution, the government has also enacted a law solely dedicated to privacy, in March 2017. Enacted without meaningful public consultation, this law was passed with haste in the parliament. The result has been the lack of robust definitions in the law, which fall below international standards, and also the lack of protections for the right to privacy online and with regard to digital data.

In the Law Protecting the Privacy and Security of the Citizen, in the definition chapter, privacy is defined as follows:

Privacy means the right to freedom of movement, freedom of residence and freedom of speech of a citizen in accordance with law. Security means security of private affairs of a citizen. It shall also include the security of residence or residential compound and building in the compound, possessions, correspondence and other communication of a citizen.⁶

While the definition does, in principle, protect certain aspects of privacy of a citizen (but not of non-citizens), it is far from comprehensive, falling below the standards set out in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and its corresponding General Comment, which extends privacy to the digital sphere. The definition, though enacted in 2017, also falls short of the United Nations General Assembly's recognition that privacy is a crucial right in the digital age.

The Evidence Act

The Evidence Act in Myanmar was adopted on 1 September 1872 from the Indian Act 1 of 1872. Due to the outdated definitions of "documents", it was amended in 2015 to include electronic records and information. This is followed by more detailed examples, and among these, the one related to digital spaces is:

Any record generated, sent, received or stored by means of electronic, magnetic, optical or any other similar technologies in an information system or for transmission from one information system to another.⁷

Before the amendment of the Evidence Act, the courts had limitations on accepting digital evidence according to the respective laws that are used in cases. For example, previously, defamation online would be difficult to prosecute using the Penal Code since the evidence could not be submitted to the court due to the limitations of the Evidence Act. This lack of digital evidence provisions was also one of the arguments that lawmakers gave to justify their rejection of the repeal of Article 66(d) of the Telecommunications Law. A civil society coalition consisting of 21 groups called for the repeal of Article 66(d) of the Telecommunications Law given that defamation already exists in the Penal Code and the Evidence Act had been amended accordingly.

Governance and regulation of online spaces

Computer Science Development Law

This law was enacted in 1996 with objectives mainly targeting the development of computer science education and professionals. The law contains outdated requirements that demand prior permission in order to possess computer devices and also to develop computer networks. This is established in the law as follows:

Article 32. Whoever imports or keeps in possession or utilizes any type of computer prescribed under sub-section(a) of section 26, without the prior sanction of the Ministry of Communications, Posts and Telegraphs shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years and may also be liable to a fine.

Article 33. Whoever sets up a computer network or connects a link inside the computer network, without the prior sanction of the Ministry of Communications, Posts and Telegraphs shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years and may also be liable to a fine.⁸

⁶ English translation sourced from: www.myanmarresponsiblebusiness.org/pdf/Law-Protecting-Privacy-and-Security-of-Citizens_en_unofficial.pdf

⁷ English translation sourced from: www.burmalibrary.org/docs21/2015-12-24-Law_Amending_the_Myanmar_Evidence_Act-73-bu.pdf

⁸ English translation sourced from: www.burmalibrary.org/

TABLE 2.				
Electronic Transactions Law provisions that curtail freedom of expression				
Article	Description	Penalty		
Article 33	 (a) committing any act detrimental to the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture. (b) receiving or sending and distributing any information relating to secrets of the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture. 	Jail term from five years to at most seven years.		
Article 34	(d) creating, modifying or altering of information or distributing of information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organization or any person.	Fine from MMK 1,000,000 to 5,000,000. If unable to pay fine, he/she will be liable to be sentenced from six months to not more than one year of imprisonment.		

Although there are no longer cases filed in relation to this law, there are still potential risks as there is an article that targets freedom of speech online. In Article 35 of the Computer Science Development Law, seven to 15 years in prison and/or a fine are the punishment for committing any act (including transmitting and receiving information) that "undermines state security, prevalence of law and order and community peace and tranquillity, national unity, State economy or national culture."

Electronic Transactions Law

The Electronic Transactions Law was enacted in 2004 and later amended in 2014. The main objective of the law is to promote and support electronic transaction technologies for economic development and educational purposes. However, because of the severe penalties and vague definitions, it was infamous for putting many political activists behind bars during the era of the military government. According to the original Electronic Transactions Law. a person is liable for imprisonment from seven to 15 years for committing any act that undermines national security, community peace and tranquillity, national unity, the state economy or national culture.⁹ We must note that these are vague terms. Under the law, it is also possible to be imprisoned for three to five years for "dishonesty" and "defamation". The provisions in the Electronic Transactions Law that curtail freedom of expression are detailed in Table 2.

Due to the resultant controversy and threat for journalists and political activists, the Electronic Transactions Law was amended by a motion in parliament by MP U Thein Nyunt¹⁰ from the National Democratic Force party in 2014. The amendment reduced the jail terms and also replaced some of the jail terms with fines for defamatory speech online. Despite this effort, the law is still on the books and can be used to criminalise online speech.

Telecommunications Law

The Telecommunications Law was adopted in 2013 during Myanmar's telecom liberalisation process. The law is mainly targeted towards the telecom sector players, which are the regulatory body, the Ministry of Transport and Communication, telecoms operators and network companies. It also aims to address consumer protection, specifically for the telecommunications sector. Despite its main objectives, there is a clause in the law that has proved to be problematic. A number of cases have arisen from the usage of Article 66(d) of the Telecommunications Law, which states:

Whoever commits any of the following acts shall, on conviction, be liable to imprisonment for a term not exceeding three years or to a fine or to both.

[...]

(d) Extorting, coercing, restraining wrongfully, defaming, disturbing, causing undue influence or threatening to any person by using any Telecommunications Network.¹¹

A person convicted of an offence under Article 66(d) is liable for imprisonment of up to three years and/

docs15/1996-SLORC_Law1996-10-Computer_Science_ Development_Law-en.pdf

⁹ English translation sourced from: www.burmalibrary.org/docs15/2004-SPDC_Law2004-05-Electronic_Transactions_Law-en.pdf

¹⁰ Soe Than Lynn. (2013, 4 February). Government to redraft 'outdated' electronic transactions law. Myanmar Times. www. mmtimes.com/index.php/national-news/3977-govertment-toredraft-outdated-electronic-transactions-law.html

¹¹ English translation sourced from: www.burmalibrary.org/ docs23/2013-10-08-Telecommunications_Law-en.pdf

or a fine. According to the Telecommunications Law Research Team, as of August 2017, there have been over 90 known cases under Article 66(d), where the section has been used against online speech. At the time of writing this report, an amendment of the Telecommunications Law has been discussed and passed in the parliament from the primary draft presented by the Ministry of Transport and Communication and with inputs from the lower and upper house (Hluttaws) of parliament.12 The amendment of the Telecommunications Law was approved and passed in August 2017.13 Despite campaigns and calls from civil society and the media to abolish Article 66(d) or at the very least remove the term "defamation" from the stated article, the amendment decreased the jail terms from three to two years, but without removing the term defamation.

Further, Articles 68(a) and (b) of the Telecommunications Law state that:

68. Whoever commits any of the following acts shall, on conviction, be liable to imprisonment for a term not exceeding one year or to a fine or to both.

(a) communications, reception, transmission, distribution or conveyance of incorrect information with dishonesty or participation;

(b) prohibiting, obstructing or interfering the transmission, reception, communication, conveyance or distribution of information without permission.

The vague definition "incorrect information with dishonesty" gives rise to the potential for misuse and arbitrary criminalisation of online speech, and leads to a chilling effect online.

Sectoral laws

News Media Law

The News Media Law was enacted in 2014 with the main objectives of promoting independent journalism and protecting journalists. Due to the recent enactment, the News Media Law includes the digital medium as a source of media, and media workers are defined as those who are involved in the media business and are responsible for news and information. Chapter 4 of the News Media Law outlines extensive duties for media workers, titled "Responsibilities and code of conduct to be complied with by news media workers".¹⁴ Therefore, the law fails to explicitly recognise media freedom in relation to freedom of expression. However, the News Media Law refers back to the existing rights and restrictions of the relevant laws within the country.

Printing and Publishing Enterprise Law

The Printing and Publishing Enterprise Law was enacted in 2014 together with the News Media Law in order to regulate and promote the print and publishing sector. It was meant to replace Myanmar's 1962 "Printers and Publishers Registration Law" which required prior approval by the Press Scrutinv and Registration Board for publishing content. which enabled pre-publication censorship. In 2012, the government dissolved the censorship board and the 1962 law was lifted. Although this new law was adopted as a successor to the previous draconian law, it still lacks a clear explanation as to why the law is needed for a democratic country, since it gives the regulator (which consists of government officials) the power to "take actions" on "unethical" media content.¹⁵ This could lead to future restrictions of both offline and online content.

Broadcasting Law

The Broadcasting Law was enacted in 2015 with the primary objectives of deploying spectrum usage and promoting access to knowledge and information by means of supporting public and private broadcasting services. Similar to the News Media Law, the Broadcasting Law fails to acknowledge and promote freedom of expression, with respect to the international standards and definitions, as in Article 19 of the Universal Declaration of Human Rights and the ICCPR. This can be seen from the questionable independence of the authority (regulatory body) and the council to be formed according to the law. Moreover, there is still room for improvement for the regulatory body for the broadcasting service to be independent, and for the power and provisions.

Curtailment of online freedom of expression

Although there are numerous laws in Myanmar that have or may have restrictions to freedom of expression online, the law that has been used widely is Article 66(d) of the Telecommunications Law. Since its adoption, there have been 96 known cases filed

¹² Win Ko Ko Latt, & Kan Thar. (2017, 18 August). Myanmar lower house approves minor changes to telecom law. *RFA*. www.rfa.org/ english/news/myanmar/myanmars-lower-house-approves-minorchanges-to-telecom-law-08182017161716.html

¹³ San Yamin Aung. (2017, 24 August). Amendments to telecoms law passed. The Irrawaddy. https://www.irrawaddy.com/news/burma/ amendments-telecoms-law-passed.html

¹⁴ English translation sourced from: www.burmalibrary.org/ docs18/2014-Media_Law-en.pdf

¹⁵ English translation sourced from: www.article19.org/data/files/ medialibrary/3679/Printing-and-Publishing-Enterprise-Law-Bill. pdf

using this law. Out of the 96 cases, seven were filed under the previous government and 89 were filed under the current National League for Democracy (NLD) government. The ratio of cases according to the party that filed the complaints during the NLD government is illustrated in Figure 1.

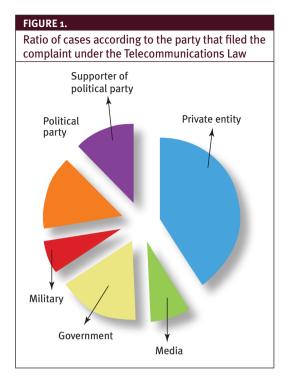
From the ratios, we can see that more than half of the cases are motivated by political reasons, which include cases filed by the government, military, political parties and supporters of a certain political party.

In Article 66(d) of the Telecommunications Law, there are seven actions for which a person could be charged: "Extorting, coercing, restraining wrongfully, defaming, disturbing, causing undue influence or threatening to any person by using any Telecommunications Network."

But in reality, almost all of the known cases have been filed under the category of defamation. All of the complaints have also been filed on the basis of content posted on Facebook and not on other online platforms such as websites or blogs. The following are some of the prominent cases under Article 66(d).

CASE STUDY 1: CHAW SANDI HTUN¹⁶

Chaw Sandi Htun, also known as Chit Thamee on Facebook, was arrested in October 2015 for her post on her Facebook profile that compared the colour of Military General Min Aung Hlaing's uniform to the colour of one of Aung San Suu Kvi's longavis (skirts). This was considered inappropriate according to the widely accepted culture in Myanmar, as comparing a man's shirt with a woman's underskirt is considered to lower the dignity of the man. The complaint against Chaw Sandi Htun was filed by an army official, for the reason that her Facebook post allegedly undermined the dignity of the Tatmadaw (army). Chaw Sandi Htun was held in custody for four days without proper judicial procedure. She was first charged under Section 34(d) of the Electronic Transactions Law, Article 66(d) of the Telecommunications Law and Section 500 of the Penal Code. In the final court judgment, which was available in December 2015, she was sentenced to six months imprisonment, under Article 66(d) of the Telecommunications Law.



CASE STUDY 2: HLA PHONE¹⁷

Kyat Pha Gyi (The Big Rooster) is the name of the Facebook account that mocks the government and military by posting "photoshopped" images. Hla Phone was accused of being the person behind Kyat Pha Gyi, and was arrested in February 2016 on the basis of a complaint filed by a military officer. He was sentenced to imprisonment for two years under Article 66(d) of the Telecommunications Law, the National Flag Act, and Section 505(b) of the Penal Code, which establishes penalties for:

Whoever makes, publishes or circulates any statement, rumour or report– [...]

(b) with intent to cause, or which is likely to cause, fear or alarm to the public or to any section of the public whereby any person may be induced to commit an offence against the State or against the public tranquillity...

¹⁶ The case of Chaw Sandi Htun, Global Freedom of Expression. https://globalfreedomofexpression.columbia.edu/cases/ case-chaw-sandi-htun-myanmar

¹⁷ Khine Khine. (2017, 27 May). Free, but not free. *The Voice*. thevoicemyanmar.com/perspective/8866-fre

CASE STUDY 3: MAUNG SAUNG KHA18

Maung Saung Kha is a poet and a member of the NLD youth committee. He is also a member of PEN Myanmar (the national branch of PEN International). Maung Saung Kha was arrested for the poem he posted on Facebook titled "Image", in which the controversial part read: "I have the president's portrait tattooed on my penis / How disgusted my wife is." The case was filed by a police chief in October 2015. Although the poem was published during President U Thein Sein's government, the case was concluded and the sentence was handed down under the NLD government. He was held in custody for six months and 19 days and later sentenced to six months in prison.

CASE STUDY 4: SWE WIN19

Swe Win is an award-winning journalist and the editor of Myanmar Now.²⁰ His criticism of U Wirathu, one of the leaders of the ultranationalist group Ma Ba Tha, in a Facebook post, led to a complaint being filed by a Ma Ba Tha supporter. The complaint was filed in March 2017 under Article 66(d) of the Telecommunications Law and Article 295 of the Penal Code, which states:

Section 295. Whoever destroys, damages or defiles any place of worship, or any object held sacred by any class or persons, with the intention of thereby insulting the religion of any person or with the knowledge that any class of persons is likely to consider such destruction, damage or defilement as an insult to their religion, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

Section 295A. Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of [persons resident in the Union], by words, either spoken or written, or by visible representations insults or attempts to insult the religion or the religious beliefs of that class, shall be punishes [sic] with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

Although the Ministry of Culture and Religious Affairs issued a statement saying that Swe Win's speech is legitimate and that he should not be charged under Section 295 of the Penal Code, the case is still ongoing on the basis of Article 66(d) of the Telecommunications Law.

International treaties

Although Myanmar is included in the first group of countries to sign the Universal Declaration of Human Rights, Myanmar has yet to ratify the key human rights treaties such as the ICCPR and the International Covenant on Economic, Social and Cultural Rights (ICESCR).

Myanmar is, however, a party to the Convention on the Rights of the Child (CRC) and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). Since Myanmar is a member of the Association of Southeast Asian Nations (ASEAN), it is also a party to the ASEAN Human Rights Declaration.²¹ In the ASEAN Human Rights Declaration, the right to freedom of speech and expression is enshrined in Article 23, which reads as follows:

Article 23 - Every person has the right to freedom of opinion and expression, including freedom to hold opinions without interference and to seek, receive and impart information, whether orally, in writing or through any other medium of that person's choice.

Future violations through draft laws

The Ministry of Culture and Religious Affairs of Myanmar is drafting an anti-hate speech law.²² While the law is still being drafted, the process itself is opaque, with civil society being kept out of the process. Concerned about the potential violations of freedom of expression through the draft anti-hate speech law, civil society organisations came up with a separate draft, named the "Interfaith Harmony Bill". The civil society initiative is supported by local and international human rights organisations and the document has been drafted in accordance with international standards. However, the chances of the government adopting the civil society bill are slim.

¹⁸ Freeman, J. (2016, 2 March). The bizarre trial of a poet in Myanmar. The New Yorker. https://www.newyorker.com/books/page-turner/ the-bizarre-trial-of-a-poet-in-myanmar

¹⁹ The Irrawaddy. (2017, 30 July). Myanmar Now editor arrested. *The Irrawaddy*. https://www.irrawaddy.com/news/burma/breakingmyanmar-now-editor-arrested.html

²⁰ www.myanmar-now.org

²¹ asean.org/asean-human-rights-declaration/ accessed September 2017

²² Ei Ei Toe Lwin. (2016, 20 May). NLD considers religious harmony law. Myanmar Times. https://www.mmtimes.com/national-news/ yangon/20397-nld-considers-religious-harmony-law.html

It is reported that a cybersecurity or cybercrime bill is being drafted by the Ministry of Home Affairs, but the process has been opaque until now and there are concerns among civil society groups about potential violations of online freedom of expression, and worries about broader digital rights issues in the country. Moreover, since 2013, the Ministry of Social Welfare, with technical support from the Gender Equality Network, has been working on a bill to prevent violence against women.²³

It must be noted that the government rarely conducts inclusive and meaningful public consultation sessions during the drafting process. This is particularly challenging since civil society is given a small role to play in the law-making process, which could lead to potential restrictions on freedom of expression and to problems with broader human rights issues in the country.

Summary and conclusions

Myanmar is a unique country in terms of internet usage and penetration. With the country being closed for many years, users had faced obstacles in access to the internet in terms of prices and infrastructure. But after 2012, when the government liberalised the telecoms market, these factors became less of an obstacle, and internet penetration has skyrocketed. Although usage has grown, the legal framework that enables the protection of civil rights and supports the use of the internet for civic engagement has proven to be lacking.

While freedom of expression is a constitutional right, it is still limited by vague and unspecific rationalisations such as union security, community peace and tranguillity, etc. In addition, Myanmar still criminalises defamatory speech. Moreover, defamation is contemplated not only in the Penal Code, but also in various other laws including the ones that govern the online space, such as the Electronic Transactions Law and the Telecommunications Law. The punishments are also inconsistent, with different penalties for defamation in different laws. With vague and problematic laws, particularly the Telecommunications Law, which leaves them open to the risk of misuse, there have been nearly a hundred cases of people being charged with criminal offences on account of their online speech within the short period of one vear. This negative trend could continue since the parliament did not tackle the root of the problem in the Telecommunications Law during the amendment period, but rather did window-dressing.

Although Myanmar has shown potential growth in terms of access to the internet, the space still remains restricted for exercising freedom of expression online. The government and lawmakers should conduct a meaningful public consultation process, inviting comments and participation from diverse stakeholders, so that this problem may be addressed.

²³ Ei Cherry Aung. (2016, 6 September). Bill to prevent violence against women "includes marital rape". Myanmar Now. www.myanmar-now.org/ news/i/?id=3f7caa52-e222-4f12-b55e-45dee00c56d1

Legal limitations on online expression in Pakistan

Sadaf Khan Media Matters for Democracy (MMfD) mediamatters.pk

Introduction

The internet and freedom of expression

On 19 March 2014, the Express Tribune, a local affiliate of the International Herald Tribune, was published with five columns of blank space. The space was originally given to an article titled "What Pakistan Knew about Bin Laden",¹ an opinion piece about Pakistan's possible knowledge of Bin Laden's presence in Abbotabad. In the times before the internet, the Pakistani readership would have remained unaware of what was supposed to appear in those ominously blank five columns. However, within hours of the distribution of the blank paper. Twitter was alive with links of the censored article. This incident demonstrates both the impact of the internet on freedom of expression and access to information and the mindset of states that still believe in controlling public access to information.

That freedom of expression online is a fundamental human right is now well established through multiple UN resolutions and recommendations. In 2012, the United Nations Human Rights Council (UNHRC) affirmed that "the same rights that people have offline must also be protected online."² This affirmation means that at state levels it is important to ensure that the practice of rights online is enabled and ensured. As technology grows and the penetration of the internet widens, the benefits of technology, particularly in connection with the practice of social and political rights, have become more and more obvious. We live in a world where the Arab Spring is globally recognised as a political revolution that was triggered and sustained through the use of social media and digital technology. As a consequence of the demonstrated potential of digital technologies to challenge political power structures, states have responded by enacting legislation that enables them to exercise increased control over the digital avenues of expression. It is thus important to document how laws and policies in different countries have come to interact with internet rights. One right that this paper is particularly concerned with is the right of freedom of expression.

Freedom of expression, a cornerstone right of any democratic society, has hugely benefited from digital technologies. Whether it is the possibility of anonymity, the connection and networking with like-minded audiences, the ease and cost of mass communication, the access to information at a global level or the potential to mobilise, the internet has enabled journalists, activists and citizens to enhance the potential impact of their expression. Consequently, states, particularly those where power status quos are existent, have responded negatively to this potential new threat to the power dynamics.

The Pakistan context

In May 2017, the Federal Ministry of Interior and then Federal Minister of Interior Ch. Nisar Ahmed issued multiple statements expressing their displeasure over the use of social media and expressing intent to initiate and strengthen a crackdown against those using social media platforms for expressing sentiment that was deemed dangerous by the ministry. On 23 May, the Interior Minister issued a statement saying that "our cultural and religious values are under attack from a section of social media."³ The statement also included a vow to ensure

¹ Gall, C. (2014, 23 March). What Pakistan Knew About Bin Laden. The New York Times. https://www.nytimes.com/2014/03/23/ magazine/what-pakistan-knew-about-bin-laden.html

² Human Rights Council. (2012). The promotion, protection and enjoyment of human rights on the Internet. A/HRC/20/L.13. ap.ohchr.org/documents/alldocs.aspx?doc_id=20280

³ The Express Tribune. (2017, 23 May). No restrictions either: No unbridled freedom on social media, says Nisar. The Express Tribune. https://tribune.com.pk/story/1417195/ anti-army-content-social-media-will-not-tolerated-chaudhry-nisar

that "efforts were accelerated to track internet users' activities online and hunt down undesirable elements."

It is not just political power hubs like the Ministry of Interior that have advocated an increase in restrictions and monitoring of social media. In March 2017, Justice Shaukat Aziz Sidiqui of the Islamabad High Court (IHC) commented that blasphemy through social media is "a greatest form of terrorism and people involved in this heinous act are biggest terrorists,"⁴ and ordered the Ministry of Interior to "eliminate access to blasphemous content on social media, even if it means blocking *all* access to social media platforms."⁵

The discussions on media, the statements from ministries and the comments from honorable judges of the judiciary appear to limit the narrative on social media to the issue of blasphemy. Yet the reality is much more complex. The statements from the Ministry of Interior followed a political disaster that unfolded on Twitter, after the official account of the Inter-Services Public Relations (ISPR) was used to send out a tweet that rejected a government statement regarding Dawn Leaks.6 The tweet was later withdrawn through a statement that the "Twitter post stands withdrawn and has become infructuous."7 However, the original use of Twitter to reject a government statement and the following public outcry created an extremely humiliating scenario for the government, and the Ministry of Interior was at its midst.

The comments from the IHC judge followed harrowing incidents of enforced disappearances of five bloggers and activists, who were accused of being involved in running blasphemous pages, but were also known to be political activists with critical and dissenting opinions.

- 5 Shehzad, R. (2017, 7 March). Blasphemy: IHC directs authorities to block all social media if necessary. *The Express Tribune*. https://tribune.com.pk/story/1348784/ ihc-directs-authorities-block-social-media-necessary
- 6 Dawn Leaks refers to a news story published in Pakistan's oldest and most widely circulated English-language newspaper, Dawn. The story was based on information leaked from a high-level meeting between the civil and military leadership. The publication of the story was seen as anti-national and led to a high-level inquiry and the dismissal of then Federal Minister of Information Pervez Rasheed. See Almeida, C. (2016, 6 October). Exclusive: Act against militants or face international isolation, civilians tell military. Dawn.com. https://www.dawn.com/news/1288350/ exclusive-act-against-militants-or-face-international-isolationcivilians-tell-military
- 7 Dawn. (2017, 10 May). Army withdraws tweet "rejecting" PM Office's directives on Dawn story probe. *Dawn.com*. https://www. dawn.com/news/1332244

Ch. Nisar's own warning about possible permanent blocking of all social media websites came right after "the refusal of the Facebook administration to share details of those persons who allegedly were running a malicious campaign against the superior judiciary through the social networking site."⁸ The bloggers were later "recovered," without much explanation from state authorities. However, despite any presented evidence or a court case, the bloggers were directly linked to blasphemy in the public imagination through a prolonged and structured campaign that was run online and through certain media channels.

The recounted incidents and statements occurred in the first half of 2017 alone. They remain reflective of the direction the state is taking with regard to the regulation and criminalisation of expression online. State actions connected to restriction of speech online have gone beyond mere statements, and over the last few years, Pakistan has witnessed a very structured attempt to legally restrict the space for political and other expression through the enactment of regressive laws and policies.

Methodology

This report is primarily based on a review of laws, legal cases and literature that outline legal limitations imposed upon freedom of expression online. Through a general analysis of available case law, the report also looks at how laws related to expression online have been implemented and interpreted by courts. The research framework is largely drawn from one developed by SMEX.⁹ Using this framework, the report explores sections related to online expression within the country, in the following areas:

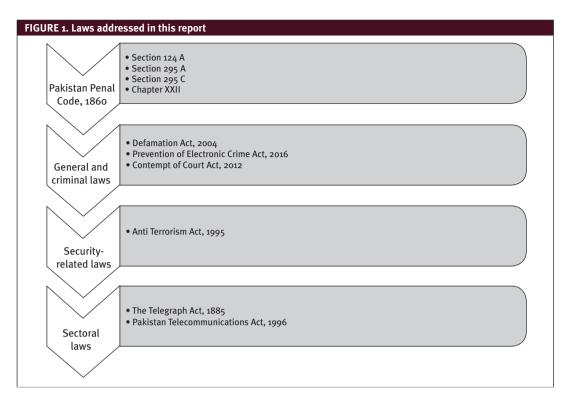
- Legal foundations including those codes that inform the legislative and legal groundwork in the country, including the constitution, the penal code and the code of procedure.
- Fundamental rights and freedoms as defined within the constitution and special laws.
- Governance of online and networked spaces

 as regulated by relevant criminal laws and within IT policies.
- Sectoral laws laws that are directly related to the operations of the information and communications technology (ICT) sector.

⁴ Asad, M. (2017, 8 March).). IHC wants blasphemous content on social media blocked. *Dawn.com*. https://www.dawn.com/ news/1319102

⁸ Rao, S., & Mukhtar, I. (2017, 10 March). Nisar threatens to block social media websites. *The Nation*. nation.com.pk/national/10-Mar-2017/ nisar-threatens-to-block-social-media-websites

⁹ https://smex.org



 Other laws – in particular security and terrorism-related laws

The main source of case law used for this research is the Pakistan Law Site that curates different decisions of higher courts across Pakistan. Media reports on known cases have also been referred to.

Lay of the legal land

Legislative system

Pakistan has had a turbulent legislative history. In 1948, after independence from the British and partition from the Indian sub-continent, a constituent assembly was formed. The idea was to create a constitution under the Objectives Resolution,¹⁰ which held Islamic conjunctions prime. Due to the assassination of the first prime minister, Liaguat Ali Khan, the death of Mohammad Ali Jinnah and the subsequent political turmoil, the first constitution, which declared Pakistan as an Islamic Republic. could not be passed till 1956. The constitution was suspended by the first military dictator, General Yahya Khan, and was replaced by another constitution in 1962, through which the presidential system was introduced in the country. After two other periods of martial law, the parliamentary system was eventually restored through a new constitution passed by the National Assembly in 1973. The 1973 constitution is the one in effect at the moment.

In terms of the larger legal systems and procedures, Pakistan is still operating under British Common Law. The Pakistan Penal Code (PPC) is an adapted version of the 1860 code introduced by the British in colonial India. The code therefore is colonial in nature and tends to treat citizens like subjects. An added complexity in the general legal system is the presence of a parallel system of Islamic jurisprudence. However, for the sake of this study the dual nature of the law is not relevant as the Islamic or Sharia courts have largely been used for matters related to family law.

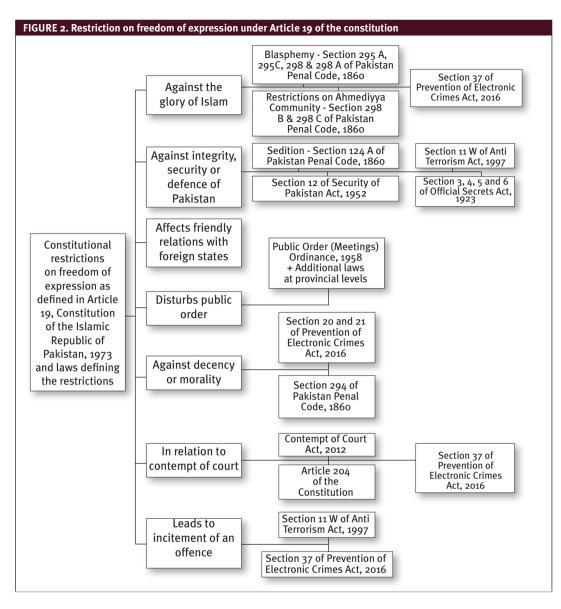
Legislation around freedom of expression

The right to freedom of expression is guaranteed through Article 19 of the constitution. The right is not absolute and the constitution allows for some restrictions that have to be prescribed by law.

In addition to laws related to restrictions there are also other laws that are used to regulate expression. For the sake of this study we will largely be looking at four kinds of laws: the penal code, criminal laws, general laws and sectoral laws (see Figure 1).

Another set of laws that are related to regulating expression are the media laws including the

¹⁰ https://en.wikipedia.org/wiki/Objectives_Resolution



Pakistan Electronic Media Regulatory Authority Act, the Press Council of Pakistan Act, and other laws defining censorship and content regulation in films and advertisements. However, none of these specifically extends to the online sphere and thus they are not a subject of study in this paper.

Curtailment of online freedom of expression

Constitutionally prescribed restrictions on freedom of expression

The discussion on online freedom of expression has to start with Article 19 of the Constitution of the Islamic Republic of Pakistan, which both grants and limits the right of freedom of expression in the country. Article 19 states that:

Every citizen shall have the right to freedom of speech and expression, and there shall be freedom of the press, subject to any reasonable restrictions imposed by law in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, [commission of] or incitement to an offence.

Most of the restrictions prescribed in Article 19 have been codified through a set of laws (see Figure 2).

Constitutional restrictions on right to freedom of expression and related laws

There are other laws that restrict expression and define criminalised forms of expression, like the Defamation Act 2004, that do not clearly fall within the prescribed restrictions structure. There has been debate over the subjective nature of some of the prescribed limitations. In particular the limitation on speech that is against "decency" and "morality" remains highly subjective and open to interpretation, as these terms have not been defined in any of the legal mechanisms.

In Benazir Bhutto vs Federation of Pakistan (1988), Chief Justice Muhammad Haleem states:

The difficulty of determining what would offend against morality is enhanced by the fact that not only does the concept of immorality differ between man and man, but the collective notion of society also differs amazingly in different ages. All that can be said is that the antonym of the word "morality" according to the existing notion depends upon acts which are regarded as acts of immorality by the consensus of general opinion.¹¹

In Yaqub Beg vs State, Justice A. S. Faruqi states:

Obscenity as understood in law consists of publishing or exhibiting such matter or object which has the tendency to corrupt the minds of those who are open to immoral influences by exciting in them sensuality and carnal desire.¹²

Thus, even the case law within which the concepts of morality, etc. have been deconstructed sets a subjective parameter for their definition.

Here is a look at other restrictions and legal tools used for defining those restrictions, particularly in the online sphere.

Blasphemy

The offence of blasphemy is defined in different sections of the Pakistan Penal Code. From the banning of platforms like YouTube, to initiation of arrest warrants for Facebook founder Mark Zuckerberg, enforced disappearances of bloggers accused of blasphemy, vigilante murders for alleged blasphemous expression online, awarding a death sentence to an accused, or a court order recommending

11 Reported Caselaw Trends on the Freedom of Speech and Expression in the Islamic Republic of Pakistan (2015). building a firewall to block Facebook completely in case of failure to rid it of all blasphemous content: this particular area of restriction has the most well-developed body of case law focused on the online space.

The offence is codified in the following three sections from the Pakistan Penal Code, 1890:

295 A – Deliberate and malicious acts intended to outrage religious feelings of any class by insulting its religion or religious beliefs. Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of [citizens of Pakistan], by words, either spoken or written, or by visible representations, insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to [ten years], or with fine, or with both.

295 C – Use of derogatory remarks, etc., in respect of the Holy Prophet. Whoever by words, either spoken or written, or by visible representation, or by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Muhammad (peace be upon him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

298 A – Use of derogatory remarks, etc., in respect of holy personages. Whoever by words, either spoken or written, or by visible representation, or by any imputation, innuendo or insinuation, directly or indirectly, defiles the sacred name of any wife (Ummul Mumineen), or members of the family (Ahlebait), of the Holy Prophet (peace be upon him), or any of the righteous Caliphs (Khulafa e Raashideen) or companions (Sahaaba) of the Holy Prophet (peace be upon him) shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Different court orders strictly affirm the restriction; in Zaheeruddin vs State (1993), Justice Abdul Qadeer Chaudhry states that "anything, in any fundamental right, which violates the Injunctions of Islam thus must be repugnant." In Masroor Ahsan vs Aredeshir Cowasjee (1998), Justice Munawar Ahmad Mirza states that "a citizen has to be mindful about paramount religious, cultural or social textures and basic features by avoiding [...] provoking towards contravention of existing laws or prejudicing glory of Islam in the

¹² Reported Caselaw Trends on the Freedom of Speech and Expression in the Islamic Republic of Pakistan (2015).

garb of freedom or liberty whether for speech or press."

In addition to Section 295 A and B of the PPC, Section 37 of the Prevention of Electronic Crimes Act, 2016 also instructs the Pakistan Telecommunication Authority (PTA) to block access to content that is "against the glory of Islam" – i.e. blasphemous content.

Some of the more prominent cases of blasphemy involving technology include a first information report (FIR) filed against Shan Taseer, son of a former governor who was killed by his own guard for criticising the blasphemy law.¹³ The FIR against Shan Taseer is also on criticism of the law, not conducting blasphemy itself. The criticism was expressed through social media. In 2017, Pakistan also witnessed the first sentence of capital punishment¹⁴ for someone convicted of expressing blasphemy online. On 17 September 2017, another death sentence was given to a Christian man for sending a blasphemous poem over WhatsApp.¹⁵ Cases filed have included incidents of sending SMS,¹⁶ sending text over WhatsApp,17 recording and sending blasphemous content via mobile phone,18 or "liking" blasphemous posts on Facebook¹⁹ or other social media.²⁰ Cases have also been registered against non-Pakistani citizens and residents.²¹

- 16 Islam, S. (2012, 3 March). Blasphemy prosecution: Cleric made complainant on court directive. *The Express Tribune*. tribune. com.pk/story/344660/blasphemy-prosecution-cleric-madecomplainant-on-court-directive
- 17 AFP. (2016, 11 July). Christian man in Lahore charged with blasphemy over WhatsApp poem. The Express Tribune. tribune.com.pk/story/1139513/ christian-man-lahore-charged-blasphemy-whatsapp-poem
- 18 Gabol, I. (2016, 28 June). Two Christians among three sentenced to death for blasphemy by Punjab court. *Dawn.com*. https://www. dawn.com/news/1267876/two-christians-among-three-sentencedto-death-for-blasphemy-by-punjab-court
- 19 Jami, A. (2017, 24 March). FIA arrests three in social media blasphemy case. *Dawn.com*. https://www.dawn.com/ news/1322531
- 20 Dhakku, N. (2014, 15 November). Man held over blasphemy allegation. Dawn.com. https://www.dawn.com/news/1144655/ man-held-over-blasphemy-allegation
- 21 Islam, S. (2012, 28 February). Blasphemy: Burning Quran is a form of international terrorism, says petitioner. The Express Tribune. tribune.com.pk/story/342763/blasphemy-burning-quran-is-aform-of-international-terrorism-says-petitioner

Another serious development was the decision of Salman Shahid vs Federation of Pakistan. Justice Shaukat Aziz Siddiqui of the Islamabad High Court commented in the decision²² that the government should try to initiate action to permanently shut down websites and pages that host blasphemous content. The court also asked the government to "agitate the matter before the United Nations through its permanent delegate for legislation at international level against such acts and convey the reservations of the Muslims of the world in general and that of Pakistan in particular regarding the publication of such objectionable material." The justice has also recommended more stringent legislation on the likes of other "Islamic countries" as well as China.

Restrictions on the basis of national security

The most prominent law that defines restrictions geared towards protection of national security is the Anti Terrorism Act. Section 11W of the Anti Terrorism Act has been used to register cases against speech online:

11W. Printing, publishing, or disseminating any material to incite hatred or giving projection to any person convicted for a terrorist act or any proscribed organization or an organization placed under observation or anyone concerned in terrorism.

(1) A person commits an offence if he prints, publishes or disseminates any material, whether by audio or videocassettes [or any form of data storage device, FM radio station or by any visible sign] or by written photographic, electronic, digital, wall chalking or any other method [or means of communication] which [glorifies terrorists or terrorist activities or] incites religious, sectarian or ethnic hatred or gives projection to any person convicted for a terrorist act, or any person or organization concerned in terrorism or proscribed organization or an organization placed under observation:

Provided that a factual news report made in good faith shall not be construed to mean "projection" for the purposes of this section.

(2) Any person guilty of an offence under subsection shall be punishable on conviction with imprisonment, which may extend to five years and with fine.

In June 2017, a man was handed the death sentence for committing blasphemy over Facebook. The

¹³ Tanvir, R. (2016, 31 December). Shaan Taseer booked for "hate speech" following Christmas message. The Express Tribune. https://tribune.com.pk/story/1280484/ shaan-taseer-booked-hate-speech-following-christmas-message

¹⁴ Rasmussen, S., & Gillani, W. (2017, 11 June). Pakistan: man sentenced to death for blasphemy on Facebook. *The Guardian*. https://www.theguardian.com/world/2017/jun/11/ pakistan-man-sentenced-to-death-for-blasphemy-on-facebook

¹⁵ Johnston, I. (2017, 16 September). Christian man sentenced to death in Pakistan over 'blasphemous' WhatsApp message sent to friend. *The Independent*. www.independent.co.uk/news/world/ asia/pakistan-blasphemy-death-sentence-nadeem-james-poemwhatsapp-message-gujrat-a7950561.html

²² Salman Shahid vs Federation of Pakistan via Ministry of Interior, Writ Petition739/2017 (Islamabad High Court 2017).

sentence was handed over by the Anti Terrorism Court and Section 11W was one of the sections used to bring about the charge. In this particular case, Section 11W was evoked as the speech could "whip up sectarian hatred".²³ Section 11W has also been used in a case of blackmail over Facebook.²⁴

Within Pakistan's security context, Section 11W is seen as a key instrument to curb speech that can threaten national security in any manner. A demonstrative case regarding application of 11W is High Court Bar Association vs Government of Balochistan.²⁵ The case was initiated through the Registrar of Balochistan High Court who drew notice to the reporting of a terrorist incident in which 26 persons were brutally murdered and a banned organisation Lashkar e Jhangvi (LeJ) claimed responsibility. The notice included reports mentioning LeJ from 10 newspapers. The judgment notes the fact that the court had received statements from media representatives regarding the threats they receive unless they air the claims of organisations like LeJ. However, the judgment holds that despite the threats and the fear of life, the compliance with 11W was mandatory. Upon reception of threats the media was directed to "report to the police" but if the electronic media and press "propagate the view of banned organizations they are not acting as good and responsible journalists but as mouthpieces for malicious and vile propaganda." In this context the government was instructed to initiate action under Section 11W against any publications/broadcasts that included claims from banned/terrorist organisations.

It is important to note that journalists in Balochistan are directly under threat from banned organisations and other actors. In the last 17 years more than 22 journalists have been killed in the region²⁶ and in 2012, the year before the judgment was issued, the wave of violence against journalists had extended to targeting their family members.²⁷ This case does not relate to online expression and has been cited only to demonstrate the approach

24 Hussnain, F. (2017, 2 August). Facebook blackmailer sentenced to 14 months in prison. *The Nation*. nation.com.pk/lahore/o2-Aug-2017/ facebook-blackmailer-sentenced-to-14-months-in-prison that is taken by the court when the law's application is concerned.

In the new cybercrime legislation, the Prevention of Electronic Crimes Act (PECA) 2016, section 12 criminalises preparation or dissemination of "information, through any information system or device that invites or motivates to fund, or recruits people for terrorism or plans for terrorism."

Another Section in PECA criminalises "glorification of an offence":

Section 9. – Glorification of an offence. (1) Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism, or activities of proscribed organizations or individuals or groups shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to ten million rupees or with both.

So far there are no judgments in any cases that have been registered on the basis of Section 9 or 12 of the law. PECA also empowers security and intelligence agencies to initiate action, including real-time surveillance for "national security" reasons.²⁸

Contempt of court

The Contempt of Court Act, 2012, defines the offence of contempt of court:

Whoever disobeys or disregards any order, direction or process of a court, which he is legally bound to obey or commits a willful breach of a valid undertaking given to a court or does anything which is intended to or tends to bring the authority of a court or the administration of law into disrespect or disrepute, or to interfere with or obstruct or interrupt the process of law or the due course of any judicial proceedings, or to lower the authority of a court or scandalize a judge in relation to his office, or to disturb the order or decorum of a court, is said to commit "contempt of court".

There is no documented case of the Act itself being used to initiate legal action against expression online. However, one prominent case of a political worker being arrested for "tweeting against the judiciary" has been documented. A political worker from Pakistan, Tehreek Insaaf, was arrested by

²³ Gabol, I. (2017, 10 June). First death sentence handed to man for blasphemy on social media. *Dawn.com*. https://www.dawn.com/ news/1338684

²⁵ PLD 2013 Balochistan 75.

²⁶ Baig, A. (2015, 3 June). Safe Nowhere – Plight of Journalists in Pakistan – Part 3: Case List of Journalists Killed in the Line of Duty. *Media Matters for Pakistan*. mediamatterspakistan.org/844

²⁷ The Express Tribune. (2012, 26 October). Second son of Khuzdar Press Club president passes away. The Express Tribune. https://tribune.com.pk/story/457243/ second-son-of-president-khuzdar-press-club-passes-away

²⁸ Gishkhori, Z. (2016, 20 October). ISI to take action against cyber crimes breaching national security. *Geo.tv.* https://www.geo.tv/ latest/118292-Govt-accepts-ISIs-role-in-taking-action-againstcyber-crimes

the Federal Investigation Agency (FIA) for tweeting against the judiciary following a tweet in which he had shared a wedding invitation card to demonstrate conflict of interest²⁹ in a judgment.

While the framing of the charge dealt with tweeting against the judiciary, the law used to initiate the charge was not the Contempt of Court Act, but the Electronic Transactions Ordinance (ETO).³⁰ Article 36 of the ETO, which was used to initiate the action states:

Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorised to gain access, as aforesaid, shall be guilty of an offence under this Ordinance punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both.

For what actually constitutes contempt with regard to speech, Justice Shabir Ahmed in the State vs Abdur Rehman³¹ held:

It is not everything said or written against a Judge that amounts to contempt of court and it is only such utterances or writings which are calculated to bring a Court or a Judge of Court into contempt or to lower his authority or such utterances or writings which are calculated to construct or interfere with the due course of justice or the lawful process that amount to it.

Sedition

Sedition has been defined in Section 124-A of the Pakistan Penal Code:

124-A – Sedition. Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Federal or Provincial Government established by law shall be punished with imprisonment for life, to which fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine. An interesting case evoking charges of sedition is Ali Raza vs Federation of Pakistan³² brought before Justice Mohsin Akhtar Kyani. The case was registered for the putting up of posters in the Federal Capital that seemingly called for the imposition of martial law. The posters displayed a glamorous picture of then Army Chief Gen. Raheel Sharif, along with the caption: "Education, health, peace, move on Pakistan." The initial case was brought forward after a police officer filed an FIR on grounds of sedition and conspiracy against the state, stating that the posters appear to call for one institution to take charge of other democratic institutions. In this case, the court held that "private persons cannot agitate the matter regarding sedition charges, rather it should be initiated, inquired and investigated by the Government or at least on their instruction." The court also held that there must be a clear call for rebellion or promotion of feeling of enmity, hatred or ill will between different religious groups, or racial or linguistic or regional groups or castes. The judgment also holds that in matters of sedition, the court "has to consider the speech in a free, fair and liberal spirit and not in a narrow minded or sectarian way."

The judgment also quotes a previous judgment of Sindh High Court, 2010 YLR 1647 Flt. Lt. (Dr) Shariq Saeed vs Mansoob Ali Khan and five others:

The right of free speech extends to all subjects which affect ways of life without limitation of any particular fact human interest and include in the main term "freedom of expression". Moreover the right to freedom of speech and expression carries with it the right to publish and circulate one's ideas through any available means of publication.

The inclusion of the reference to the right being applied to "any means of publication" is important in this regard as the offending posters on which the writ petition was initiated were also circulated widely through social media.

There are no prominent cases in which sedition charges have been applied to speech/expression that was exclusively online. However, if one sees seditious speech as largely being anti-state speech, there are examples in which such material has been blocked. A look at a Facebook transparency report demonstrates that the state regularly gets "anti-state" content that is critical of the state³³ removed from the social media platform. Some of the content has been removed for condemnation

²⁹ The judge who had granted bail to the accused in a corruption case was the mother-in-law of the accused.

³⁰ Akbar, A. (2015, 28 October). FIA arrests PTI activist for "tweeting against judiciary". Dawn.com. https://www.dawn.com/ news/1215966

^{31 1957} PLD (W. p.) Baghdad-ul-Jadid 6.

^{32 2017} PLD 64 Islamabad.

³³ https://govtrequests.facebook.com/country/Pakistan/2013-H2

of the country's independence.34 According to media reports the FIA holds that "anti-state and hate propaganda" is the second-most misused subject on social media. The FIA also claims to have received "7,500 complaints from the public as well as state institutions of as many as 64,000 Twitter accounts and Facebook pages being involved in blasphemy and supporting anti-state, criminal and terrorist activities." The same report states that three social media users were arrested in Lahore, Islamabad and Quetta for alleged involvement in anti-state activities.35 The sedition law has not been used in any of these cases; however, if sedition is largely seen as speech that is "anti-state", then there are various instances in which such speech has been blocked and criminalised.

Additionally, legislators including cabinet members have criticised the speech by bloggers at Bhensa, Mochi and Roshni as being anti-state. However, even in these cases, the state did not get involved in litigation and the bloggers allegedly involved in running these pages were abducted and later returned without any explanation from the government itself. This demonstrates that even in the cases where there was some public narration about possible anti-state activities online, the course selected to tackle such speech was extrajudicial.

Pornography

There is a general social consensus in Pakistan about blocking access to pornographic material. Pornographic content is generally seen as falling within the "decency and morality" related restrictions. The internet regulator, PTA, has been engaged in launching massive drives to block pornographic content, once landing in a controversy when allegedly a 15-year-old was engaged to make a list of pornographic websites to be blocked within the country. The teenager Ghazi Muhammad Abdullah found almost 780,000 adult pages in six months, calling this task his "religious and national"³⁶ duty. After driving criticism PTA issued a tender for creation of a system for filtering content. As per media reports, over 500,000 websites with pornographic content are currently blocked in the country. A media report also indicated that in the guise of blocking pornographic content, other content was also being blocked. The investigation by Dawn.com found that "the list of 429,343 websites, obtained by Dawn.com from an ISP source close to the ongoing process, has been found to be flawed as scores of sites with no pornographic content are included in the list."³⁷

The same list was also used to block Tumblr from Pakistan.

Within the law, the focus is on criminalisation of child pornography. Both the PPC and PECA include sections that criminalise and define penalties for those engaged in production, possession or distribution of content that depicts children/minors in sexually explicit conduct. The relevant sections of the law include:

Section 292 B, Pakistan Penal Code, 1860 -Child pornography. (1) Whoever takes, permits to be taken, with or without the consent of the child or with or without the consent of his parents or guardian, any photograph, film, video, picture or representation, portrait, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of obscene or sexually explicit conduct, where. - (a) the production of such visual depiction involves the use of a minor boy or girl engaging in obscene or sexually explicit conduct; (b) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in obscene or sexually explicit conduct; or (c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in obscene or sexually explicit conduct; is said to have committed an offence of child pornography.

(2)The preparation, possession or distribution of any data stored on a computer disk or any other modern gadget, shall also be an offence under this section.

Section 22, PECA 2016 – Child pornography. (1) Whoever intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in an information system, that visually depicts—

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; or

³⁴ https://govtrequests.facebook.com/country/Pakistan/2016-H2

³⁵ Haq, R. (2017, 20 August). Cyber crime: 64,000 social media users reported to FIA. The Express Tribune. https://tribune.com.pk/ story/1486291/cybercrime-64000-social-media-users-reported-fia

³⁶ Crilly, R. (2012, 14 March). Pakistan uses teenage boy to help with pornography crack down. *The Telegraph*. www.telegraph.co.uk/ news/worldnews/asia/pakistan/9143296/Pakistan-uses-teenageboy-to-help-with-pornography-crack-down.html

³⁷ Haque, J. (2016, 25 May). Pakistan's impossible attempt to block 400,000 porn sites continues. *Dawn.com*. https://epaper.dawn. com/DetailImage.php?StoryImage=25_05_2016_001_007

(c) realistic images representing a minor engaged in sexually explicit conduct; or

(d) discloses the identity of the minor, shall be punished with imprisonment for a term which may extend to seven years, or with fine which may extend to five million rupees or with both.

Defamation

The offence of defamation has been defined in the Pakistan Penal Code and within the Defamation Act, 2004. The relevant sections are as follows.

Section 499, Pakistan Penal Code, 1860 – Defamation. Whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.

Defamation Act 2004

2(b) "broadcasting" means the dissemination of writing, signs, signals, pictures and sounds of all kind, including any electronic device, intended to be received by the public either directly or through the medium of relay stations, by means of,

(i) a form of wireless radioelectric communication utilizing Hertzian waves, including radiotelegraph and radiotelephone; or

(ii) cables, computer, wires, fibreoptic linkages or laser beams, and "broadcast" has a corresponding meaning;

(e) "publication" means the communication of the words to at least one person other than the person defamed and includes a newspaper or broadcast through the internet or other media; and

(2) Defamation is of two forms, namely: (i) slander; and

(ii) libel.

(3) Any false oral statement or representation that amounts to defamation shall be actionable as slander.

(4) Any false written, documentary or visual statement or representation made either by ordinary form or expression or by electronic or other modern means or devices that amounts to defamation shall be actionable as libel.

8. Notice of action. No action lies unless the plaintiff has, within two months after the publication of the defamatory matter has come to his notice or knowledge, given to the defendant

fourteen days notice in writing of his intention to bring an action, specifying the defamatory matter complained of.

Case law on defamation demonstrates that accusations of defamation often result in acquittals or dismissal of cases without penalties. Both technical and other grounds are used for dismissal of cases. Case law on defamation also sets a high standard for accusation of defamation to be proved. In Mst. Shash Begum vs Bashir Ullah, Justice Seikh Ahmed Faroog (2013 PCrLJ 1737 Federal Shairait Court) holds that "the most essential ingredient for constituting an offence of defamation is mens rea or intention (Reliance PLD 2001 - Jarachi - 115)." The judgment also holds that any "accusation preferred in good faith against any person to any of those, who have lawful authority over that person or an imputation made in good faith by person for protection of his right or interest, as do not fall within the definition of Defamation as envisaged under section 499 PPP."

The Defamation Act and case law both have a strong tradition of defence. The judgment in Sved Mehmood Ali vs Network Television Marketing (pvt) limited and other defendants (2005 C LD 840) in connection with the interpretation of the law holds that "a class or particular section group of people cannot claim to be defamed as a class, section, group or community nor an individual can claim to be defamed by general reference to the class, section group or community to which he belonged." The judgment also holds that a "person accused of libel may defend the action on the plea of fair comment on a matter of public good or interest, absolute or qualified privilege or if it shown to be with the permission or consent of the injured and aggrieved person."

There are no prominent cases in which defamation suits have been initiated purely on the basis of speech/expression online.

However, the Prevention of Electronic Crimes Act, 2016 has also introduced certain provisions through which defamation charges might be brought forward. In particular, section 20 of PECA 2016, "Offences against dignity of a natural person", holds:

Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both. This section does not apply to content aired by broadcast media or distribution service licensed under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002).

Unlike Section 499 of the PPC and the Defamation Act 2004, both of which include a strong set of defences, section 20 of PECA 2016 does not offer any kind of defence to the accused. The PPC and the Defamation Act also set a limitation of liability defining the time within which defamation charges can be brought. This limitation is also missing in PECA. The lack of any limitation and defined defences in the law create the possibility of abuse of the law. However, since the law is fairly new, and courts have only recently been notified,³⁸ the case law showing how this section is interpreted and applied is not developed as yet.

Hate speech

Regulation of hate speech online has been a challenge worldwide. In Pakistan, hate speech has been an issue of serious concern. There is a large presence of terrorist and sectarian organisations online, including Lashkar-e-Jhangvi who have traditionally called out for murder and violence against the minority Shia sect. Hate speech against the Ahmadiya community is also abundant and often includes calls for violence. In addition, accusations of blasphemy online, followed by calls for murder of the accused, are increasingly common and have a very real potential of translating into physical violence. On the other hand, defining hate speech is a challenge. Given the state's track record of crackdowns against political and ideological dissidents, the likelihood of hate speech laws being misused remains high.

Hate speech was traditionally tackled through Section 11W of the ATA. However, PECA 2016 has introduced a specific section criminalising hate speech online. The section states:

11. Hate speech – Whoever prepares or disseminates information, through any information system or device that advances or is likely to advance interfaith, sectarian or racial hatred, shall be punished with imprisonment for a term, which may extend to seven years or with fine or with both.

No case law has been developed so far to demonstrate the application and interpretation of this section. During the public consultations with civil society, the Ministry of IT held that this section was being included to make sure that terrorist outfits and proscribed organisations³⁹ that openly engage in inciting sectarian violence by using hate speech online are brought under the ambit of the law. However, a year after the law was passed, in September 2017, an investigation by the country's oldest English-language newspaper Dawn⁴⁰ demonstrated the continued presence and operation of these organisations online. The investigation showed that these organisations "are present on Facebook in the form of hundreds of pages, groups and individual user profiles" and enjoy a collective following of 160,000 people. The investigation also found that the content of these pages largely includes "hate speech directed at religious minorities and other members of society."

One of the outfits that are present and operating on Facebook is the Lashkar-e-Jhangvi (LeJ), a militant organisation that has publicly accepted responsibility for killing members of the Shia community and that openly calls for violence against them. The outfit has been engaged in multiple high-profile incidents of terrorism including the killing of US journalist Daniel Pearl, the killing of Iranian diplomats and an attack on a Sri Lankan cricket team in Lahore, Pakistan. Dawn's investigation found that the group is operating eight pages and groups on Facebook.⁴¹ These pages and groups obviously promote the hate-filled ideology of Laskhar-e-Jhangvi and yet there are no cases registered that evoke the hate speech clause against LeJ. In addition to Facebook, the same organisation and its supporters continue to openly distribute fatwas or religious decrees against the Shia sect, calling the murder of Shias *jihad* or a part of the Holy War.⁴² The fatwa referred to here calls Shia Muslims "infidels" and says they are "liable to be murdered." It also pledges to rid the country of this *napaak* or unclean community by continuing to engage in their murder. The group continues to circulate such decrees online. These obviously come under the definition of hate speech as defined in PECA. However, so far we have not really seen its implementation and not a single case has been brought forth under the section.

This lends support to the fear that the sections that criminalise different forms of speech included in PECA are more actively used to clamp

³⁸ moit.gov.pk/policies/designatedcourts.pdf

³⁹ nacta.gov.pk/proscribed-organizations

⁴⁰ Haque, J., & Bashir, U. (2017, 14 September). Banned outfits in Pakistan operate openly on Facebook. *Dawn.com*. https://www. dawn.com/news/1335561

⁴¹ Ibid.

⁴² Jafria News. (2013, 10 April). Lashkar e Jhangvi Pamphelet Against Shia Community. Jafria News. https://jafrianews. com/2013/04/10/wahabi-clerics-issuing-fatwas-of-sexual-jihadfor-fsa-terrorist-allowing-them-raping-non-sunni-women-in-syria/ lashkar-e-jhangvi-pamphelet-against-shia-community

down against political dissidents rather than being evoked against those who are directly engaged in terrorist and militant activities.

Other restricting mechanisms

PECA includes another set of provisions that do not fall directly under the categories defined above. The most prominent of these is Section 21:

Offences against modesty of a natural person and minor. Whoever intentionally and publicly exhibits or displays or transmits any information which,-

(a) superimposes a photograph of the face of a natural person over any sexually explicit image or video; or

(b) includes a photograph or a video of a natural person in sexually explicit conduct; or

(c) intimidates a natural person with any sexual act, or any sexually explicit image or video of a natural person; or

(d) cultivates, entices or induces a natural person to engage in a sexually explicit act, through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to five million rupees or with both.

At first glance, the section appears clear in its intention: most cases initiated under this clause, including one currently being heard in the special court in Karachi, have been brought by women being blackmailed and intimidated by the use of morphed pictures. However, since May 2016, the FFIA, the key investigative body defined in PECA, has been engaged in a crackdown against journalists, bloggers and micro-bloggers who have been accused of penning *anti-Army* content.⁴³ In a number of cases, including one involving a journalist, Zafar Achakzai,⁴⁴ the FIA has used Section 21 of PECA. The journalist was arrested in Quetta and later granted bail.⁴⁵ How exactly a piece or tweet that is critical of the Army falls under the ambit of this section is something that is yet to be explored as there are no decisions in any of these cases yet.

What is alarming is the abuse and even disregard of the procedures described within the law. FIA officials have not only brought in people without registration of formal charges, they have also allegedly gone through their data and devices. A news story in The Guardian quotes an FIA official saying that "his agency had orders from the interior ministry to interrogate, and seize laptops and phones, without warrant."46 The story also claims that the agent was authorised to detain anyone on suspicion. Following a similar attempt by the FIA to intimidate another journalist into submission. Taha Siddiqui, the affected journalist, initiated a petition against the agency in the Islamabad High Court. The journalist, who is known to be critical of the security institutions, was initially contacted by the Counter Terrorism Department of the agency. During the course of the court hearing, his case was transferred to the Cyber Crime Wing47 and he was later asked to visit the FIA so that "log in and technical staff may scrutinise his account." This is against the procedure defined within the law, which requires the agency to acquire a warrant before any such logging or scrutinisation can take place. Since PECA 2016 has been enacted, there have been various cases of concern where bloggers have faced enforced disappearances, journalists have been picked up and tortured while being interrogated about their social media activity,48 and political workers have been harassed to leave digital spaces.

Another restricting mechanism is PECA Section 37, which does not criminalise content *per se*, but defines very broad categories of "unlawful content" that is supposed to be proactively blocked by the PTA. Section 37 states:

The Authority (PTA) shall have the power to remove or block or issue directions for removal or blocking of access to an information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act.

⁴³ The Nation. (2017, 16 May). FIA traces 12 websites with anti-Army content. *The Nation*. nation.com.pk/national/16-May-2017/ fia-traces-12-websites-with-anti-army-content

⁴⁴ Hashim, A. (2017, 30 June). Pakistan: Zafar Achakzai charged for anti-army post. *Al Jazeera*. www.aljazeera.com/ news/2017/06/pakistan-zafar-achakzai-charged-anti-armypost-170630074828317.html

⁴⁵ Shah, S. (2017, 5 July). Quetta court grants bail to journalist arrested by FIA over "anti-state" social media posts. *Dawn.com*. https://www.dawn.com/news/1343411/quetta-court-grants-bailto-journalist-arrested-by-fia-over-anti-state-social-media-posts

⁴⁶ Rasmussen, S., & Gillani, W. (2017, 11 June). Op. cit.

⁴⁷ The Express Tribune. (2017, 6 July). Journalist Harassed: Case transferred to cyber crime wing. *The Express Tribune*. https://tribune.com.pk/story/1451057/ journalist-harassed-case-transferred-cyber-crime-wing

⁴⁸ Dawn. (2017, 11 July). Journalist freed after "torture". *Dawn.com*. https://www.dawn.com/news/1344495

This section borrows language directly from Article 19 of the constitution, effectively giving the PTA, an executive authority operating under the federal government, the power to interpret the constitution. Interpretation of constitutional provisions has traditionally been done only through the higher judiciary. Article 19, as discussed in the previous sections, clearly says that the restrictions have to be defined by law; however, through this provision, the interpretation of already subjective limitations like integrity of Islam, decency and morality, etc. has been transferred to a body that has traditionally been tasked only with the licensing of the telecommunication sector and reports to the government. Since the enactment of PECA, the PTA has established a research cell of 25 persons⁴⁹ who scour the internet for objectionable material to be removed or blocked.

The law instructs the PTA to "prescribe rules providing for, among other matters, safeguards, transparent process and effective oversight mechanism for exercise of powers under subsection" and until that time, to "exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government." For the sake of transparency and accountability, the PTA was instructed to file a report about the implementation of this section in the parliament. However, despite a formal request from a legislator, Senator Farhatullah Babar,50 the PTA has yet to submit this report. The law also defines a redressal mechanism in cases where internet users might feel aggrieved by the censorship orders. The aggrieved person/s must "file an application with the Authority for review of the order within thirty days from the date of passing of the order" and "an appeal against the decision of the Authority in review shall lie before the High Court within thirty days of the order of the Authority."

However, there is a challenge with this redressal mechanism as well: the PTA has historically been secretive of the list of websites/pages/users it chooses to block. The local organisation Media Matters for Democracy (MMfD) has filed multiple requests under the Right to Information Act requesting a complete list of banned websites along with the reasons for blockage, and received no response from the Authority. This situation is likely

49 Yousufzai, A. (2017, 9 May). PTA Monitored and Blocked 1660 Blasphemous Links/Sites. *Propakistani*. https://propakistani.pk/2017/05/09/ pta-monitored-blocked-1660-blasphemous-linkssites

50 Ahmad, Z. (2017, 20 July). Senators call for cyber crimes legislation under Article 19. *Business Recorder*. fp.brecorder. com/2017/07/20170720199842 to continue. Thus, the redressal mechanism would technically enable only the creators of the content to initiate proceedings, because without an updated list of blocked material, general consumers of information, i.e. internet users, might not even be aware that it has been blocked.

Media reports also demonstrate that in addition to the PTA, other state departments have also been activated to keep an eye out on the internet. In July 2017, the Punjab Safe Cities Authority (PSCA) reported "684 objectionable pages and IDs of both Facebook and Twitter during its strike against anti-state, anti-social, blasphemous and sectarian warmongering elements on social media."⁵¹ In June 2017, the counter-terrorism department in Sindh had also identified and sought action against "25 such websites, which were involved in spreading religious and ethnic extremism and terrorism."⁵²

Finally, an old colonial law that can potentially be used to restrict speech online is the Telegraph Act 1885. This Act includes a section that can be used to criminalise "fabricated or obscene messages" sent online. Section 29 of the Telegraph Act states:

If any person transmits or causes to be transmitted by telegraph a message which he knows or has reason to believe to be false or fabricated, or a message which is indecent or obscene, he shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.

Potential for further violations

There are no draft laws currently available that have the potential for a direct impact on the practice of freedom of expression online. However, the potential for an increase in the abuse of existing laws is demonstrated through the political statements that have been given by cabinet members. The framing of social media tools like Twitter as a "threat to democracy" and the FIA's crackdown against people tweeting against the Army without obtaining proper warrants or following the prescribed legal procedure appear to be a grim indication of things to come. Legislators from opposition parties have also publicly expressed doubts about the intentions underlying the cybercrime legislation. Senator Farhatullah Babar from the opposition Pakistan

⁵¹ The News. (2017, 7 July). 684 social media IDs objectionable. The News. https://www.thenews.com.pk/ print/214986-684-social-media-IDs-objectionable

⁵² Ali, I. (2017, 22 June). CTD seeks ban on 25 websites spreading "terrorism, extremism". Dawn.com. https://www.dawn.com/ news/1341033

People's Party termed the law "an attempt to curb citizens' freedom of speech rather than protect them."⁵³

The government's efforts to coerce corporations into providing user data also continue. In July 2017, Facebook refused a request by Pakistani authorities to link all user accounts with mobile numbers. Concerning this request, the PTA said that "mobile numbers are verified through biometric verification system in the country. The issue of fake accounts could be overcome if all existing accounts are verified with phone numbers." Given the history of political victimisation, the mere idea of linking users' Facebook activity with their identity and biometric data poses serious concerns.

There is a draft of a potentially enabling law: a new right-to-information legislation at the federal level. The law, if enacted in the form that is being advocated by civil society, will enable access to government and state documents through digital formats. Since information is directly connected to expression, the enactment of a strong right-to-information law at the federal level may widen the space for online expression as well. Another possibility of positive intervention in this regard is the fact that Pakistan has signed on to the Open Government Partnership (OGP). As a part of the national action plan that is being created to move towards the goals of openness and transparency, the Ministry of IT has signed on to a commitment to table a consultative draft of data protection legislation in the parliament. The draft IT policy also includes a commitment to introduce data protection legislation for the "protection of personal data and online privacy for improved transparency and security of sensitive and confidential information." Data protection legislation, again, can have an enabling impact on online expression.

Finally, the implementation process of PECA gives rise to various concerns about the sincerity of the government. It has been more than a year since the law was passed and notified and yet there are questions about how exactly it is being implemented. Media reports point towards the creation of cells within the PTA and FIA to monitor and censor online content, but there is no transparency about the composition of these cells or the process followed to enact them. Multiple right-to-information requests to the PTA have gone unanswered. A set of interviews conducted by MMfD⁵⁴ also showed a

discrepancy in the perspectives being given by the Ministry of IT, which prepared and tabled the law, and the FIA, the key investigating agency implementing the law. For instance, when asked about the role of intelligence agencies in real-time surveillance, an invasive and extreme tactic allowed under the cybercrime bill that can have a direct impact on the environment for online expression, the representative from the Ministry continued to hold that the intelligence agencies have no role and the FIA would be leading the implementation. However, interviewees from the FIA itself minimised their own role in this operation and held that the intelligence agencies are largely taking the lead in surveillance-related aspects of the law. Previously, media reports also claimed that "Rules being formed under the newly-passed legislation called the Prevention of Electronic Crime Act (PECA), 2016 will empower many agencies to crack down on individuals misusing the internet, social media, in particular."55

These contradictions and the lack of transparency have not gone unnoticed. On 8 August 2017, the Sindh High Court, during the hearing of a constitutional petition against a crackdown on bloggers, "directed the interior ministry and the Federal Investigation Agency (FIA) to file a detailed report on cybercrime laws."56 In July 2017, Senator Farhatullah Babar, a member of the Senate's standing committee on human rights, raised the issue on the floor of the Senate and inquired about a report⁵⁷ on the implementation of the bill that was due to be submitted six months after the law was enacted. Six months after this question was raised, the Federal Minister of Interior finally responded, giving his assurance that the said report would be filed within the week. However, at the time of writing, no report had been filed by the Ministry. This continued secrecy over the procedures and processes through which this law is being implemented remains a threat to the practice of freedom of expression online.

Summary and conclusion

The cases discussed above demonstrate an increase in the government's tendency towards criminalisation of online expression. The cybercrime law, PECA 2016, is one of the key indicators of the government's approach towards online expression,

⁵³ Guramani, N. (2017, 19 July). Senators term Prevention of Electronic Crimes Act, 2016 a "black law". *Dawn.com*. https://www.dawn. com/news/1346310

⁵⁴ The interviews are yet to be published and will appear on MMfD's digital rights website: digitalrightsmonitor.pk

⁵⁵ Gishkori, Z. (2016, 20 October). Op. cit.

⁵⁶ Siddiqui, T. (2017, 8 August). SHC asks Interior Ministry, FIA to file report on cyber crime laws. *Dawn.com*. https://www.dawn.com/ news/1350224

⁵⁷ Ahmad, Z. (2017, 20 July). Op. cit.

particularly expression that has political and ideological messages.

There is largely a lack of distinction within the laws about expression online and offline – for instance, the national security and terrorism-related laws, which have been applied in multiple cases on online speech, do not include a chalked-out distinction between the medium used to express. However, while the traditional laws have been applied online, the cybercrime law does include criminal penalties for expression that is exclusively shared online – in some instances these penalties do not apply or differ from penalties defined for similar expression in the offline sphere.

In addition to the laws that criminalise expression, there are three major points of concern with regard to the way these laws are being implemented and framed for the general public.

First, there is a complete lack of transparency and clarity when it comes to application of online censorship clauses included within the cybercrime law, which also makes it difficult for general internet users to ascertain how the PTA and FIA are interpreting the provisions of PECA. PECA includes certain clauses that do not directly criminalise expression but define the general environment within which freedom of expression online is to be exercised - for example, real-time surveillance and data collection clauses. With regard to these sections, which can potentially be invasive and restrictive of the practice of freedom of expression, there is a contradiction between the Ministry of IT and the investigative agency FIA: while the Ministry continues to hold that the country's security and intelligence agencies have no role in the implementation of these sections, the civil investigative agency representatives openly admit that the role of agencies in real-time surveillance is much higher than their own. The section itself is framed in reference to another law - the Investigation for Fair Trial Act that legitimises the role of intelligence agencies in real-time digital surveillance in addition to the designated FIA.

Second, there is a structured campaign on the part of the government to link online expression to blasphemy and anti-state activities. More alarming than the actual legislation perhaps is the narrative being built by different state institutions to justify an increase in the crackdown against activists and journalists who frequently turn to the online sphere. As demonstrated in this report, both civil and military authorities have increasingly referred to the "dangers" that "anti-national and anti-state" elements online pose to the country. This narrative, supported by strong propaganda tools, has been internalised by a significant populace and it is common to see violent reactions towards freedom of expression advocates. Social media, whenever mentioned by cabinet members and government parliamentarians during their media talks and briefs, is referred to as a tool for creating instability, a means of spreading anti-Islam and anti-state messages. In the same vein, the people who are vocal online, particularly those who openly protest and demonstrate against crackdowns on online freedom of expression, are framed as anti-state elements who do not have religious and moral grounding.

Finally, the prevalence of "mob justice" by rightwing elements who feel offended and threatened by religiously provocative speech is increasing. The government has failed to offer protection and justice and remains complicit even in cases where it was proven that the violence done in the name of blasphemy was deliberately provoked by the authorities. The case of Mashal Khan's murder is reflective of this brewing trend. At this stage it is very clear that the administration of Mardan University was involved in provoking the violence against their own student.⁵⁸ some of the screenshots used by the members of the mob to call him a blasphemer were fake, and the murder and subsequent mutilation of his body itself is obviously a heinous crime. And yet, political parties within the government were not only reluctant to take action against this brutality, but some right-wing parties actively tried to rile up the public sentiment further by connecting murder investigations with possible amendments in the blasphemy law.⁵⁹ Before the murder, a structured campaign against the bloggers who faced enforced disappearances and the activists who demonstrated for their recovery showed very clearly that state functionaries and their cronies with the media are willing and able to use the "blasphemy card" to taint even political speech in the eyes of the general public, thus creating an environment where people fear mob justice and retreat from their online spaces – and when this happens, the most regressive ways of evoking the criminalisation laws are not even necessary.

⁵⁸ Akbar, A. (2017, 17 April). Lynching suspect gives statement: "University administration asked me to testify against Mashal". Dawn.com. https://www.dawn.com/news/1327576

⁵⁹ The Nation. (2017, 1 May). "Will cut tongue of anyone wanting to change blasphemy law," says Jamaat-e-Islami KP chief. The Nation. nation.com.pk/national/o1-May-2017/will-cut-tongue-of-anyonewanting-to-change-blasphemy-law-says-jamaat-e-islami-kp-chief

The criminalisation of freedom of expression online in Thailand

Freedom of Expression Documentation Centre, iLaw https://freedom.ilaw.or.th/en

Introduction: Background on the political situation in Thailand

Thailand is a sovereign country ruled by democracy with the King as the head of state. However, after a revolution against the absolute monarchy in 1932, Thailand has had at least 13 military coups with 11 unsuccessful rebellions and 20 constitutions. The time period under military governments is longer than that of elected governments.

The 1997 constitution created a new form of democratic government that led to the rise of a successful political party led by Thaksin Shinawatra, a millionaire businessman. The Thaksin administration and policies became popular among poor people in the countryside along with many corruption allegations. This phenomenon did not satisfy the traditional institutions such as the military, judiciary, bureaucrats and middle class society who cooperated to fight against the new emerging power, that of business politicians. The anti-Thaksin movement gathered with yellow as a campaign colour, as it is the colour of King Rama IX, while the pro-Thaksin movement adopted the colour red, as it is a symbol of the common people. The political conflict arose around 2005 with the "yellow shirt" demonstrations against Thaksin which led to a military coup on 19 September 2006. The "red shirt" movement fighting against the invisible power outside the constitution emerged in response.

Thaksin's younger sister, Yingluck Shinawatra, was elected as prime minister after the junta-drafted 2007 constitution was enacted. But there are many movements and accusations against her. The big movement, which consisted of conservative groups, professional elites and some NGOs that opposed the political influence of the Shinawatra clan, and is called the People's Democratic Reform Committee (PDRC), shut down the country for months in late 2013. The PDRC rose after Yingluck's government tried to pass a general amnesty (for her exiled brother), and after high-level corruption in a failed rice-subsidy scheme was revealed. Yingluck ordered the dissolution of the parliament and called for a new election, contradictory to the demand from protestors who were opposed to the election and called for the creation of a new ruling system by people's assembly. This led to a deadlock and a military coup on 22 May 2014 led by General Prayuth Chan-o-cha in the name of the National Council for Peace and Order (NCPO).

With the justification of resolving the political conflict in society, the NCPO proceeded to impose martial law on 20 May 2014 and repressed individual liberties and freedoms using political and legal claims. In part, they achieved this through the speedy and forced promulgation of an interim constitution on 22 July 2014.

The absolute power of the NCPO is enshrined and entrenched in Sections 44, 47 and 48 of the interim constitution. Section 44 confers absolute power to the head of the NCPO to issue any executive orders and announcements deemed necessary for "the benefit of reform in any field and to strengthen public unity and harmony, or for the prevention, disruption or suppression of any act which undermines public peace and order or national security, the monarchy, national economics or administration of state affairs." This enables General Prayuth, as the head of the NCPO, to override any checks and balances from the parliament and judiciary. Section 47 states that all executive orders and announcements issued by the junta are "lawful, constitutional, and final." Section 48 grants immunity from prosecution to the members of the NCPO and all other individuals acting under the orders of the NCPO with regard to the coup, thus giving full discretion to the NCPO to govern without judicial oversight.

A considerable part of the NCPO's strategy to maintain its hold on power is the use of the existing laws (Section 112 and 116 of the Penal Code) and enacting new laws to enhance military power in judicial process (Head of NCPO Announcement No. 7/2014 and Order No. 3/2015), and also other laws to repress opponents to the establishment (the Public Assembly Act of 2015, the Computer Crimes Act, and the Referendum Act). The NCPO has summoned more than 1,300 people to report and forced them to be under an "attitude adjustment" programme. It has arrested at least 500 people on political grounds, and has also established jurisdiction of the military court over civilian cases under "national security" offences or charges against people who do not kneel before the NCPO.

As this report will show, the prosecution and conviction rates under existing criminal and civil procedure laws have increased dramatically. Arbitrary arrests and *incommunicado* detentions under the NCPO have become commonplace.

Indeed, the NCPO uses repression as a central strategy to enact and enforce its policies. This was clearly seen in the use of the Referendum Act in the August 2016 constitutional referendum. The Act, in effect, criminalised any form of campaigning against the junta-written constitution. Within this repressive environment, the new constitution entrenches the role of the military in the future politics of Thailand, with the Senate being fully appointed by the NCPO, a new electoral system that disadvantages large, established parties being instituted, and non-party members eligible to become the prime minister. In addition, Section 44 has also been used at least 160 times by General Prayuth to push through a raft of administrative and economic reforms. The NCPO-appointed National Reform Committee is also in the process of drafting a 20year National Strategy Plan, which is a series of long-term policies that future elected governments will be legally forced to adhere to.

This report will focus on the legal means that the NCPO uses to entrench itself politically and repress dissent. Specifically, it will examine the use of provisions in the criminal code and civil procedure, executive orders and announcements, and laws approved by the rubber-stamp National Legislative Assembly.

Lèse majesté: Section 112 of the Penal Code

The lèse majesté law in Thailand is located in Section 112 of the Thai Penal Code, and is classed under offences against the monarchy. Section 112 states: "Whoever defames, insults, or threatens the King, the Queen, the Heir-apparent, or the Regent, shall be punished with imprisonment of three to fifteen years."

Due to the fact that Thailand has a long-lasting history of absolute monarchy, the people's beliefs

and national culture are very much based on the monarchy institution. This law became problematic during the reign of King Bhumibol Adulyadej, King Rama IX of the Chakri dynasty, who was in the Guinness Book of World Records as the longest reigning monarch. Before he passed away on 13 October 2016, King Rama IX had carried out a lot of royal projects for social benefit. During the military regimes in the 1950s to 1970s, the new ideology was promoted, the monarchy was established as the heart of the nation, and the penalty for lèse majesté offences was increased. The mainstream ideology among the Thai people considered the King as god and as a symbol of goodness. Thai constitutions usually state that the King shall be enthroned in a position of revered worship and shall not be violated. No person shall expose the King to any sort of accusation or action.

The lèse majesté law and its enforcement have become the most sensitive and controversial issue in Thai political conflict for the past 10 years. Political opponents have accused the other side of being disloyal to the monarchy and thus guilty of lèse majesté. This accusation is the most severe in Thai society. People who are accused of lèse majesté can be perceived by the society as wicked people and also a threat to national harmony.

During the crackdown on red shirt protests in 2010 that led to nearly a hundred deaths, the government accused protesters of being anti-monarchy. Soon after the crackdown a number of people were arrested under the charge of lèse majesté for expressing their views on the political conflict. The demand for reforming the lèse majesté law was also rising during that time. However, even the elected government led by Yingluck Shinawatra did not consider the proposal from the pro-democracy wing to amend the law.

From 23 May 2014 to 17 May 2017, under the NCPO regime, at least 90 people were charged with lèse majesté for peacefully expressing views on the King and other royal family members.¹ Since the political movement was restricted in other media, most of the cases concerned online expression, especially on Facebook.

The problems of the enforcement of Section 112 The problematic aspects of the lèse majesté law have been discussed for years. Legal experts and other academics including those from many

¹ iLaw. (2016, 10 May). Interesting statistics concerning bail in 112 cases in NCPO era. Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/blog/ interesting-statistics-concerning-bail-112-cases-ncpo-era

different political standpoints are agreed on many issues.

Problems with the legal provision itself

High penalties: The penalty of three to 15 years' imprisonment is too high and comparable to the penalty for the offence of preparation to commit insurrection, manslaughter, or kidnapping of a minor under 15 years of age. Even the minimum penalty of three years is too high. Although the case could be trivial, the Court is left with no discretion but to impose at least this penalty.

Vague terms: Besides "defamation", which has quite a clear definition in the Penal Code, there are some vague elements of the crime, particularly the terms "insult" and "threaten", which have been interpreted widely, covering a variety of acts or expressions. In practice, when the court has needed to explain how expressions were an alleged offence under Section 112, it has often failed to specify whether the allegedly infringing messages were defamation, insults or threatening, but has written a verdict to cover all three words.

Same level of protection: Section 112 protects persons holding different positions, including the King, the Queen, the Heir-apparent or the Regent, equally and indiscriminately, even though the penalty for damage done to the King should be more severe than for damage done to other personalities.

Offence against security: Section 112 is included under the Title on "Offences relating to the Security of the Kingdom". Therefore, its interpretation and enforcement can be cited for the sake of maintaining national security, and that would do a disservice to the defendants.

Problems related to its enforcement

Broad interpretation: Though an offence against Section 112 must be confined to defamation, insult and threatening of the persons protected by the legal provision, including the King, the Queen, the Heir-apparent or the Regent, in reality it has been subjected to extensive interpretation and use in order to criminalise a variety of actions without clear boundaries. It is difficult for ordinary persons to understand which kind of act constitutes the offence. The broad interpretation includes charges against persons who criticise King Rama IX's dog, King Rama V, and King Naraesuan, who was the monarch over 400 years ago.

From its legal provision, Section 112 protects the persons holding four positions only and does not cover the "monarchy". Therefore, a criticism about the monarchy as an institution should be permissible without criticising the persons or making other criticisms about other personalities relating to the monarchy. The other royal family members, the Privy Council, close aides, the Crown Property Bureau and the Royal Project are not protected by the legal provision, and any criticism of them should be permissible. But the general climate in Thai society and politics has made the boundaries of possible expression very dubious and risky to touch upon.

Anyone can initiate a case: Any ordinary person can bring a charge against another person invoking Section 112. The law does not oblige the injured party to make the complaint. As a result, Section 112 has been used to accuse many people, especially political opponents or business competitors.

In addition, given that Section 112 has been used for serious criminalisation, it has been abused to take revenge upon another person, even among people who are related to each other. Some examples are the case of an older brother who took his own younger brother to court on this charge by alleging that he had made lèse majesté remarks in their house,² or the cases in which fake Facebook pages have been created to retaliate against another person, accusing them of committing a lèse majesté offence as a result of personal conflict.³

Climate of fear: Law enforcement officials involved with prosecution under Section 112 have often found themselves subject to great pressure from society and as a result, it would be hard for them to make any discretion in favour of the defendants, i.e., by refusing to indict the case, allowing the alleged offenders to be released on bail, or dismissing the case. Less than half of the lèse majesté accused can access the right to bail due to the high amount of security, around 400,000 baht (USD 12,000), and the lack of court approval. The police usually pass the cases on to public prosecutors and the prosecutors issue prosecution orders in almost all cases. When the cases are in the hand of courts, which also theoretically exercise their judicial power on behalf of the King, the judges also exercise their legal knowledge under the traditional culture and the climate of fear.

Military court procedure: On 25 May 2014, three days after the military seized power, the NCPO issued Announcement No. 37/2014 to establish a new practice, under which civilians would be tried in military court for charges of an offence against the King and royal family, charges of an offence against national security, charges of defying any of the NCPO's

^{2 &}quot;Yutthapoom: 112- Brother vs Brother". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/439

^{3 &}quot;Sasivimol: Posted messages on Facebook". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/681

orders and announcements, and charges of usage or possession of firearms used in wartime.

A lot of lèse majesté cases with civilians as defendants went to military courts where some of the judges are military personnel without legal backgrounds. Under the military court's procedure, the court usually does not schedule the dates of trial continuously, so there is a large lapse of time between each witness examination; thus the trials take a long time. So far there has not been any lèse majesté case under military court where the defendant denied the charge. In many cases, the military courts also try the cases in secret. No observers, including the defendant's relatives, can be present in the courtroom.

Prosecutions of false claims using the lèse majesté law

A new phenomenon in the use of Section 112, which has appeared since the 2014 coup, is the arrest and prosecution of those who have close connections with the institution of the monarchy on charges of making false claims about the monarchy to seek personal benefit.

In November 2014, the prosecution of people charged with making false claims, fraud and lèse majesté which attracted much public attention involved a network of high-ranking police officers, led by Pol. Lt. Gen. Pongpat Chayapan, Commander of the Central Investigation Bureau, and Pol. Maj. Gen. Kowit Wongrungroj, Deputy Commander of the Central Investigation Bureau. At least 26 people have been accused of associating with this monarchy-citing network of high-ranking police, 19 of whom have already been charged with lèse majesté. Out of this number, 16 suspects have been brought to trial.

In October 2015, there was another similar prosecution of false claims under the lèse majesté law. Three people were accused of making false claims about the monarchy to seek personal benefit. They were Suriyan Sutjritpolwongse, aka Mo Yong, a well-known fortune teller who was involved in organising the "Bike for Dad" event; Jirawong Wattanathewasilp, his close associate; and Pol. Maj. Prakrom Warunprapa, an inspector in the Technology Crime Suppression Division. Suriyan died in custody and Pol. Maj. Prakrom reportedly committed suicide in his cell.⁴

There is no clear record of the number of people arrested for "false claims" since most of the accused are related to the royal institution and are not known to the public. It is believed that there are more than 50 persons involved. Some of the suspects in the news report are relatives of the former Princess Srirasmi, Royal Consort to the Crown Prince.⁵ The "false claim" lèse majesté cases are far more mysterious and scary than the cases against free expression.

The impact of lèse majesté charges on society

The massive number of people prosecuted under Section 112 and the harsh penalties applied, coupled with the trial procedure whereby most of the accused have been denied bail and the court has ordered a secret trial, have engendered a burgeoning climate of fear. It has engulfed the whole society with the notion that the monarchy is untouchable and people are supposed to practise self-censorship. They have to be cautious when discussing any issues about the monarchy during both personal and public communication. This has gravely compromised Thai people's knowledge and understanding about the monarchy.

CASE STUDY 1: JATUPAT⁶

Jatupat or Pai, 25, was a student at the faculty of law at Khon Kaen University. He became a social activist and was a member of the Daodin group. He also participated in many activities in northeast Thailand together with people who were affected by economic development projects. Jatupat and the Daodin group organised many anti-NCPO activities.

On 2 December 2016 around 5:07 a.m., the Facebook account under the name "Pai Jatupat" shared a BBC Thailand article with a biography of the new King of Thailand. In the same Facebook post, Pai also copied part of the article. Lt. Col. Phitakpol Chusri, the acting head of the Civilian Affairs Division of Military Circle 23, saw Pai's post and filed a complaint with the police. On 3 December 2016, the police arrested Jatupat under a lèse majesté charge. Jatupat was detained at a police station for one night before he was released on bail on 4 December 2016.

⁴ AFP. (2015, 9 November). Thai fortune teller held under royal defamation law found dead. *The Guardian*. https://www. theguardian.com/world/2015/nov/09/thai-fortune-teller-moryong-held-under-royal-defamation-law-found-dead

⁵ Reuters. (2015, 11 March). Parents of former Thai princess jailed for insulting monarchy. *The Telegraph*. www.telegraph.co.uk/news/ worldnews/asia/thailand/11464642/Parents-of-former-Thaiprincess-jailed-for-insulting-monarchy.html

^{6 &}quot;Jatupat: shared BBC's article". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/756

On 22 December 2016, the Khonkean Provincial Court was ordered to revoke Jatupat's bail after the police sought revocation of his bail on the grounds that he was still active on Facebook and showed disrespectful behaviour by mocking state authorities. Jatupat has been detained in prison since 22 December 2016, requesting bail at least 10 times; however, all requests were denied.

Jatupat first denied the charges and started to fight his case in the witness examination. Later, Jatupat changed his plea to guilty and the court sentenced him to five years in prison, which was reduced to two years and six months. He told the public that in such cases, there is no other option for the defendant.

CASE STUDY 2: PATNAREE7

Patnaree or Nueng is the mother of Sirawith, or "Ja New", a well-known democracy activist. Patnaree is a freelancer, working mostly as a housemaid. Patnaree was charged with lèse majesté. The alleged offence consisted of messages in Facebook Messenger where she had a conversation with Burin, a man who had been convicted in another lèse majesté case. The Military Prosecutor filed charges against her before the military court on 1 August 2016. The statement of accusation described that after Burin said something about the monarchy, Patnaree replied without attempting to stop Burin from saying such a thing. Patnaree was released on bail and is fighting her case in military court.

CASE STUDY 3: PONGSAK8

Pongsak or Sam is a tour agent from Kanchanaburi province. He participated in red shirt political rallies several times. Pongsak's name appeared on NCPO's summons order no. 58/2014 issued on 9 June 2014. However, he did not report to the NCPO.

Pongsak was arrested on 30 December 2014 at Phitsanulok Transport Station and accused of posting six photos and messages deemed to be lèse majesté on his own Facebook account named "Sam Parr". He was charged with six counts under Section 112 of the Criminal Code (lèse majesté) and Section 14 of the Computer Crimes Act. Pongsak stated that during the interrogation the military did not hurt him, but threatened him to make him confess. The military also told him that this case was not a political case but was a matter of national security. The Bangkok Military Court ordered that his case would be tried as a closed-door trial and sentenced Pongsak to 60 years in jail. Since the defendant pleaded guilty, the court halved the sentence to 30 years in jail.

CASE STUDY 4: YUTTHASAK9

On 28 January 2014, Yutthasak, who is a taxi driver, provided service to an unknown passenger. During the ride, they discussed politics. It turned out that both had a different opinion. The passenger then used her mobile phone to record their conversation and used it as evidence to press a lèse majesté charge against Yutthasak the next day.

Yutthasak was arrested in June 2014, after the coup. He requested bail but the court denied his plea. In the deposition examination, Yutthasak pleaded guilty as he had no lawyer. The Criminal Court sentenced him to five years in prison which was reduced to two years and six months. He was released on 20 May 2016.

CASE STUDY 5: WICHAI10

Wichai, 33 years old, was accused under lèse majesté for creating a fake Facebook account with someone else's name and picture and posting messages deemed to be a defamation to the King. He was arrested in December 2016 after the owner of the Facebook account accused him.

In the statement of accusation, Wichai was charged for 10 counts by the military prosecutor. Wichai first denied all charges and wanted to defend his case but later changed his mind and confessed because the trial took too long. On 9 June 2017, Wichai was taken to military court

^{7 &}quot;Patnaree: Facebook chat". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/768

^{8 &}quot;Pongsak: Posting lèse-majesté messages on Facebook". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/ en/case/650

^{9 &}quot;Yutthasak: The taxi driver". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/575

^{10 &}quot;Wichai: faked facebook". *Freedom of Expression Documentation Centre*. https://freedom.ilaw.or.th/en/case/722

to hear the verdict. For posting 10 lèse majesté messages on Facebook, the military court punished him separately for 10 counts, with seven years in prison for each count, totalling 70 years in prison for the whole case. The defendant confessed so that the penalty would be reduced by half, to three years and six months for each count. Thus, the defendant was sentenced to 30 years and 60 months, or 35 years.

The case of Wichai was marked as the case with the highest punishment that has ever been recorded.

CASE STUDY 6: "TANET"11

"Tanet" is an alias of a man who has paranoid schizophrenia. "Tanet" was accused of sending an email to an English man with a link to some content that was deemed to be defamation of the King and the Heir. After being arrested, he was sent to have a mental examination and the doctor agreed that he has mental illness. "Tanet" told the doctor that he has heard whispers in his ears for years, telling him to do or not to do something, including sending the email which lead to the prosecution.

The defence lawyer argued that "Tanet" had sent the email under the influence of mental illness, with a doctor's certification and testimony. The court sentenced him to five years imprisonment, reduced to three years and four months. The court was not convinced that while committing the offence, the defendant was oblivious to morality or was unable to control himself due to his mental disorder. Thus, the defendant could not cite it as a reason to exonerate himself.

Sedition: Section 116 of the Penal Code

The sedition law in Thailand is located in Section 116 of the Thai Penal Code,¹² and is classed under offences against internal security in Sections 113 to 118 of the Thai Criminal Code.¹³ Section 116 states:

Whoever makes an appearance to the public by words, writings or any other means which is not an act within the purpose of the Constitution or for expressing an honest opinion or criticism in order:

- To bring about a change in the Laws of the Country or the Government by the use of force or violence;
- To raise unrest and disaffection amongst the people in a manner likely to cause disturbance in the country; or
- To cause the people to transgress the laws of the Country, shall be punished with imprisonment not exceeding seven years.

While Section 116 is aimed at preventing expression which affects national security, Section 116 itself allows people to exercise their constitutionally protected right to freely criticise the government mandate, legislation and policy issued by the government as long as it is a good faith statement. Therefore, whether the expression of the people is a request to revoke or amend the laws or a request to change the government, as long as it is a peaceful expression without harm, those expressions shall not be considered as an offence under Section 116.

Before the NCPO regime, Section 116 was also used by many governments to charge leaders of big movements or demonstrations that demanded a change in government. In many of those cases, Section 116 was used to charge people with other less severe offences and many times the court dismissed sedition charges.

Under the military rule, sedition charges have frequently been used to target peaceful criticism of the military, its leaders, its policies and the May 2014 coup. From 22 May 2014 to 18 August 2017, at least 66 individuals (in 26 cases) have been charged with sedition under Section 116.¹⁴ In most cases, the accused had just expressed their opinion peacefully.

The problems of the enforcement of Section 116

The main problems with the NCPO's use of the sedition law are outlined below.

Ambiguity of the legal provisions

Some of the essential elements of the offence under Section 116 are clear themselves; however,

^{11 &}quot;Tanet": Sending an email with mental disorder. Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/614

¹² English translation sourced from: http://library.siam-legal.com/ thai-law/criminal-code-offense-internal-security-sections-113-118

¹³ English translation sourced from: https:// www.thailandlawonline.com/laws-in-thailand/ thailand-criminal-law-text-translation#chapter-2

¹⁴ iLaw. (2017, 13 September). Section 116: When 'Sedition' is used as the obstruction of freedom of expression. *Freedom of Expression Documentation Centre*. https://freedom.ilaw.or.th/en/blog/ section-116-when-%E2%80%98sedition%E2%80%99-usedobstruction-freedom-expression

there are some gaps for the other parts which can be interpreted in many aspects, such as the words: "To raise unrest and disaffection amongst the people." It is not certain what action is considered as the expression against Section 116. The lack of any guiding, objective speech test or standard to measure the seditious elements of speech is problematic due to the ambiguous nature of the terms "raise unrest and disaffection" or "likely to cause disturbance." This ambiguity has clearly opened the floodgates for criminalising a broad pool of public and private speech.

The majority of sedition prosecutions centre around criticism that does not constitute direct or implicit advocacy of violence

Most of the recent cases do not genuinely constitute sedition. They are merely statements or conduct expressing one's own opinion about the political situation, and generally lacking any exhortations or urging of lawlessness or violence. This originates from a distorted view of how speech can translate into action, and thus, fails to distinguish between legitimate criticism of the government and actual seditious speech. A central element to this distortion is that the limits on protected speech before it can be classed as seditious are extremely low, to the point where a simple expression of dissent is taken to mean exhorting disorder. This has the effect of censoring legitimate and good-faith criticisms of the NCPO.

Sedition prosecutions have been systematically directed at critics of the NCPO

The charges have been used as a repressive political tool to deter dissent by prominent anti-government critics such as ministers under the former Yingluck Shinawatra government (Chaturon Chaisang, Pichai Naripthapan), renowned journalists (Pravit Rojanaphruk), human rights defenders (Sirikan June Chaorensri) and activists with a popular following (Sombat Boongam-anong). This is also evidenced by the increase in the frequency of sedition charges and prosecutions during periods of perceived political turbulence, such as immediately after the May 2014 coup; when there were rumours of corruption in military projects in late 2015; and during the trials of Yingluck Shinawatra and ministers in her former cabinet over a corruption allegation. When the military arrested and charged people for sedition, press conferences were usually held in order to spread fear among the public that charges for a severe offence had been granted as a result of dissent against the NCPO.

Burdens placed on the accused to fight national security charges

Section 116 falls under the Penal Code chapter of offences against national security and carries a severe punishment of up to seven years in prison. This penalty rate can lead to pre-trial detention for up to 48 days. During this period the accused has to find an amount of security to request bail. The courts usually require around 70,000 to 150,000 baht (USD 2,100 to 4,500) as a security for a sedition charge. However, in one case, the court called for 400,000 baht (USD 12,000) as a security; the accused did not have enough money, so he was detained in prison for the pre-trial duration.

The NCPO also issued Announcement No. 37/2014 through which civilian cases involving offences against national security are to be tried under the jurisdiction of military courts. The sedition charge therefore was used to charge NCPO opponents who the NCPO saw as untamed persons and wanted to put under control. Even though sometimes military courts dismissed sedition charges, the accused have never felt safe to be provided the rights to a fair trial.

CASE STUDY 1: CHATURON CHAISANG¹⁵

On 27 May 2014, Chaturon Chaisang, the education minister under the former Yingluck Shinawatra administration, was arrested and charged with sedition for publicly stating his opposition to the 22 May 2014 military coup at a press conference at the Foreign Correspondents Club of Thailand (FCCT).

The statements in his speech included the following:

For dozens of years over these last years, I have indicated that in my opinion, no matter how difficult a problem the country was faced with, a coup was not the way out. If one did occur, then it would always exacerbate the problem. When the coup this time occurred, I had the same opinion and have indicated my opinion in opposition to the coup.

Coups are not the way out or solution to problems of divisiveness in society. If they come along they create even more divisiveness. What's worrisome is that if those in power don't manage things well it might create violence and increased loss.

^{15 &}quot;Chaturon: Defying NCPO order, Section 116, CCA". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/600

A coup is a process that is not democratic and that worldwide, as well as through most of Thai society, will not accept. It is bound to damage the country's image, damage cooperation with other countries, and increase economic problems of the country.

The conduct of General Prayuth and group who declared seizure of power thus conflicts with Article 68 of the Constitution. Orders of the NCPO during the time when there was still no Royal Proclamation appointing any NCPO head, are thus illegal orders.

I continue to confirm that I will use what rights and freedom I have to appeal for our land to be a democracy, beginning with an appeal to the NCPO to quickly return democracy to the people and allow elections according to democratic rule. In this, anything that I do will be peaceful and in compliance with Article 2 and in compliance with just laws.¹⁶

Chaturon's speech was clearly not seditious, but was only a criticism of the coup. Chaturon's speech does not pose a reasonably clear and imminent risk of violence, as the speech did not use inflammatory or provocative language, but was rather an opinion – and a fact-based reading of the political situation at the time. On the contrary, Chaturon explicitly stated that he would only act through peaceful and legal means.

The case is currently ongoing at Bangkok Military Court, with a slow process of witness hearings.

CASE STUDY 2: SOMBAT BOONNGAM-ANONG¹⁷

Sombat Boonngam-Anong, a social service worker and a former leader of anti-coup social movements, was arrested by the Technology Crime Suppression Division (TCSD) and charged with sedition and under the Computer Crimes Act on 5 June 2014 for posting messages on Facebook urging people to protest against the coup in a peaceful manner and to flash the three-finger salute (as popularised in the film series *Hunger Games*) as a symbol of defiance against the military junta. Currently, the case

16 Prachatai. (2014, 28 May). Chaturon Chaisang's speech before the arrest. Prachatai English. https://prachatai.com/english/ node/4048

17 "Sombat Boonngam-Anong: 116". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/604 has already conducted 10 witness hearings, and is still ongoing in Bangkok Military Court.

The urging of peaceful protest and the flashing of a symbolic salute directly shows that there was no counsel to violence nor was it an advocacy of violence. The three-finger salute, while viewed as controversial by the NCPO, is merely an expression of opinion. Under the bail agreement with military courts, Sombat was prohibited from participating in any political movements and travelling abroad without permission. The court procedure and the verdict may not mean to the society as much as the NCPO can keep Sombat under silence.

CASE STUDY 3: PONLAWAT¹⁸

Ponlawat was arrested on 27 March 2015 for distributing leaflets with the message "Wake up and rise now, all democracy lovers! Down with dictatorship! Long live democracy" and a picture of the three-finger salute. The leaflets were distributed at public places, including a kindergarten, a park, a school, a bus stop and a technical college in Rayong Province. The inquiry officer stated that the messages in the leaflets could cause conflict and confusion in society and could lead to violence. The case is currently being tried in a military court and the first witness examinations are being conducted.

The messages in the leaflets can be construed as advocating to pro-democratic sections of the public to overthrow the dictatorial NCPO regime and institute a democratic government in its place. However, Ponlawat's messages do not specifically contain any advocacy of violence, force, or the threat of violence to overthrow the government. Moreover, Ponlawat was not advocating for concrete action (as he did not provide specific plans to overthrow the government); his leaflets could be better described as advocating his belief or his principle of overthrowing governments.

^{18 &}quot;Ponlawat : Dropped leaflets in Rayong". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/659

CASE STUDY 4: PRAVIT ROJANAPHRUK¹⁹

Pravit Rojanaphruk, a renowned and awardwinning journalist from the online newspaper *Khaosod English*, was charged with two counts of sedition for authoring and publishing a series of messages on Facebook (each message was posted on a separate date):

Junta representatives called me twice yesterday to express their displeasure over a photo of me showing the middle finger to the junta-sponsored draft charter. I told them in fact the photo was uploaded on Facebook and Twitter as a set of three pictures and it includes a photo of my giving a thumbs up to the same document. I am ready to defend freedom of expression and will neither run nor delete the photo. It's ironic that the very people who teardown the previous 2007 constitution in an act of military coup now want people to treat their own juntasponsored draft charter [...].

With the junta now wanting to limit questions to junta leader General Prayuth to 4 per session, here's my four questions. 1) When will there really be free & fair elections? 2) When will you stop being a dictator while depending on taxpayers' money without their consent for your salary & perks? 3) When will you apologize to the people for having illegitimately seized power in a coup? 4) When will you stop fooling yourself & others by telling us through the song you claim to have written that you are only asking for a little time in power?

Yingluck's trial, with verdict coming soon will be a test of will of both those in power and pro-Yingkuck Redshirts. She may become Thailand's most visited prisoner and Buddha knows what may happen from there.

Yingluck insists that the junta has already confiscated her money in the bank accounts prior to Aug 25 verdict while Prayuth flatly denied. If this is the case, what kind of justice is it?

A Voice TV reporter tweeted saying a soldier shouted expletive at her and other reporters and threatened to confiscate their cameras while reporting about government's rice allegedly selling at a much lower rate than market price. Hail Prayuth's men in uniform and Juntaland!

Severe flood hitting Sakon Nakorn and Sukhothai provinces. Wait until Prayuth is done with his weekly monologue first.

A local news source from TV station told me he heard no warning about incoming flash flood in Sakon Nakorn province. Looking at the pictures of row of cars being inundated and local hotel not moving their beds from now flooded ground floor and we could have guessed that. Military rule is top down. You wait for the order.

The case is still being investigated by police. In addition, Pravit was also charged under the Computer Crimes Act.

It should also be noted that during the legal proceedings against deposed Prime Minister Yingluck Shinawatra, there was a renewed spate of sedition charges by the NCPO to quell political dissent surrounding the trial. Pravit is also very active in criticising the NCPO on his personal Facebook and Twitter accounts. Pravit was, at least twice, summoned to report and detained in a military camp in order to stop him from expressing his opinions. But the military summons did not stop him. This case therefore can be considered as another step from the NCPO to suppress Pravit.

CASE STUDY 5: PREECHA20

Preecha, a 77-year-old former schoolteacher, was arrested on sedition charges for giving food and flowers to a pro-democracy demonstrator who was leading a peaceful march and rally. The rally was protesting military trials of civilians. He was also convicted of a separate charge for violating the junta's ban on political gatherings; his sedition charges were dropped by a military prosecutor.

This is one of the most repressive uses of the sedition charge under the regime of the NCPO, as it was used in a way that is clearly distorted from its original conception, due to the political motivations of the government to repress any form of dissent. There could be no reasonable

^{19 &}quot;Pravit Rojanaphruk: Sedition charges after Facebook posts". Freedom of Expression Documentation Centre. https://freedom. ilaw.or.th/en/case/798

^{20 &}quot;Preecha: gave flowers to the protester". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/692

expectation that giving food and flowers to a demonstrator who was part of a peaceful protest would result in violence or lawlessness. The sedition charge was dropped, which indicates that the courts do understand the definition of advocacy.

CASE STUDY 6: RINDA PARUECHABUTR²¹

Rinda Paruechabutr, a single mother of two children, was charged with sedition for posting a rumour on social media that General Prayuth, the head of the NCPO, had transferred 10 billion baht to an offshore bank account in Singapore. She was imprisoned for three days after the military court in Bangkok ordered her pre-trial detention. She was then given bail, with the bail bond set at 100,000 baht (USD 2,800). However, the accusation of sedition was withdrawn. She is currently facing a charge under the Computer Crimes Act in civilian court.

Similar to the case of Preecha, this is also one of the clearly repressive uses of the sedition charge. A rumour about the prime minister does not constitute advocacy of violence or lawlessness. The idea that posting a negative rumour about the Prime Minister might lead to chaos and public disorder is an unsubstantiated link.

CASE STUDY 7: THEERAWAN22

Theerawan, 57, was arrested on sedition charges for posting a photo of herself holding a red plastic bowl that was inscribed with Thai New Year greetings from former Prime Ministers Thaksin Shinawatra and Yingluck Shinawatra. The inscription read: "Although the situation is heated, it's hoped that brothers and sisters will be soothed by the water in the bowl." What Theerawan actually did was to take her own photo with the red bowl and send it via the LINE mobile messenger application. But the photo was forwarded and a reporter at *Thairath*, a leading newspaper, put the photo on the front page during the time that the public was discussing the gift from the former prime ministers. She faced a pending trial at a military court and was looking at seven years in prison. Her bail bond was set at 100,000 baht (USD 2,800). To confirm that her charge was not a gross mistake by the judicial system, both the prime minister and deputy prime minister publicly justified the charge. Deputy Prime Minister Pravit Wongsuwon stated that her charge was "not groundless" and that she had clearly "violated the law", while Prime Minister Prayuth declared that her crime was a "national security" offence. Her charges have since been dropped.

The Computer Crimes Act 2007

The Computer Crimes Act or CCA was first issued in 2007. The law was widely used to criminalise online expression along with the Penal Code. On 16 December 2016, the rubber-stamp National Legislative Assembly unanimously revised the 2007 Computer Crimes Act, and criminalised broad forms of conduct and expression online. While the redrafting of the 2007 version of the law was expressly intended to combat phishing and online theft, it has been widely observed²³ that the rewriting of the new law will be used to silence critics of the NCPO and the monarchy.

The distinct change of the new amendments from the 2007 law is Section 18, which stipulates that law enforcement authorities can access "traffic data", encrypted data and computer systems. In addition, in Section 20, the new amendments stipulate that a "Computer Data Screening Committee" will be formed. It will consist of nine members of a government-appointed panel. The committee has the power to recommend an authority to apply for a court order to block or remove "offensive" content which sometimes does not have to violate any law.

The new amendments that will importantly restrict freedom of expression are in Section 14, 15 and 20.²⁴ Section 14 states:

Any person who commits any of the following crimes shall be liable to imprisonment for not more than five years, or a fine of not exceeding one hundred thousand baht, or both:

(1) dishonestly or deceitfully bringing into a computer system computer data which is distorted or forged, either in whole or

^{21 &}quot;Rinda: posted a rumor that Gen. Prayuth transferred money to Singapore". *Freedom of Expression Documentation Centre*. https://freedom.ilaw.or.th/en/case/682

²² Human Rights Watch. (2016, 30 March). Thailand: Sedition Charge for Red Bowl Photo. Human Rights Watch. https://www.hrw.org/ news/2016/03/30/thailand-sedition-charge-red-bowl-photo

²³ Bangkok Post. (2016, 15 December). Computer bill deeply flawed. Bangkok Post. https://www.bangkokpost.com/archive/ computer-bill-deeply-flawed/1160845

²⁴ English translation sourced from: https://thainetizen.org/docs/ cybercrime-act-2017

in part, or computer data which is false, in such a manner likely to cause injury to the public but not constituting a crime of defamation under the Penal Code: (2) bringing into a computer system computer data which is false, in such a manner likely to cause damage to the maintenance of national security, public safety, national economic security, or infrastructure for the common good of the Nation, or to cause panic amongst the public; (3) bringing into a computer system whatever computer data which constitutes a crime concerning security of the Kingdom or crime concerning terrorism under the Penal Code; (4) bringing into a computer system whatever computer data with vulgar characteristics, when such computer data is capable of being accessed by the general public;

(5) publishing or forwarding computer data, with the knowledge that it is the computer data under (1), (2), (3), or (4).

If the crime under paragraph 1 (1) is not committed against the public but it is committed against any particular person, the criminal or the person who publishes or forwards the computer data as said shall be liable to imprisonment for not more than three years, or a fine of not exceeding sixty thousand baht, or both, and the crime shall be compoundable."

Section 14(1): "False information"

The statistics for the period July 2007 to December 2011²⁵ demonstrate that lawsuits under the CCA for which the Court of First Instance has already passed verdicts were mainly filed under Section 14(1). The offences most frequently found are defamation, fraud and offence against computer systems, respectively. Before the amendment in 2016, Section 14(1) was written as follows:

Section 14. If any person commits any offence of the following acts shall be subject to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both:

(1) that involves import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to that third party or the public. The essential element of the offence under Section 14(1), in both the previous and the revised version, centres on "forged computer data or false computer data," making it different from the common defamation laws. The initial objective of this section is to prevent and to suppress any fraudulent computer data practice such as creating a forged website to mislead internet users and induce them to reveal personal information, known as "phishing". Section 14(1) is also aimed at filling a gaping hole in the offence of forgery of documents in the Penal Code.

However, during the 10 years of its enforcement, it turns out that Section 14(1) has been the section of the CCA that is the most used and is commonly used together with defamation lawsuits to criminalise content online, leading to the question of whether this is legislatively in accordance with its aim or not. It can be estimated that more than 10,000 cases have been filed with the police or courts every year under Section 14(1). Most of them are cases of individuals who posted something online that the individual accusers did not agree with or did not like. Some of these are cases between parties with unequal status, in which the legal procedure was used in order to silence critics or public participation on social interest topics.

Impacts of implementing Section 14(1) for defamation cases

Duplicate legislation: Since the Penal Code has already covered the offence of defamation, and even if an imputation is made through the internet, it shall be regarded as a defamation offence by means of publication. The duplication could also lead to confusion in the interpretation and enforcement of laws, causing too many cases in the court procedure.

Overly severe penalties: According to the CCA, offences under Section 14(1) are subject to imprisonment for up to five years and a fine of up to 100,000 baht (USD 2,800) or both. Meanwhile, in the Criminal Code, defamation offences are subject to imprisonment for up to one year and a fine of up to 20,000 baht (USD 560) or both, and for defamation by means of publication, the offender shall be punished with imprisonment for up to two years and a fine of up to 200,000 baht (USD 5,600). Therefore, when implementing Section 14(1) on the issue of defamation, the penalty will become intensely increased.

Cannot be settled through compromise: Defamation cases often concern personal matters; hence, many cases are dismissed during the court process by reaching a compromise. A compromise reached by all parties can be compensation or making an apology. However, offences under Section 14(1) of the CCA

²⁵ iLaw. (n/d) The Research on the Impacts of the Computer-related Crimes Act B.E. 2550 (CCA) and State Policies on the Right to Freedom of Expression. https://ilaw.or.th/node/1798

cannot be settled through compromise. Even if a settlement is made by a complainant and a defendant, the offence under Section 14(1) still remains. This creates an impact on the defendant and also unnecessarily makes cases pile up in the court process.

No regard for good faith or public interest: According to the Penal Code, Section 329-330, any alleged defamation deemed to be an opinion or statement expressed in good faith or any imputation proved to be of benefit to the public shall be considered of having a reasonable cause for exemption from guilt or penalty. However, under Section 14(1) of the CCA, neither the exercise of an individual's right to freedom to express his or her opinion in good faith, nor a criticism made in the public interest, can be claimed as a reason.

Threat to freedom of the media: Online media have been hugely increasing nowadays and even the mainstream media have adopted online channels as another medium of communication; thus, when a defamation charge occurs, Section 14(1) is likely to be integrated in the charge. This causes a greater burden to the media as well as to the accused. Also, the tendency for the media to be prosecuted under Section 14(1) is continually increasing, affecting the atmosphere of freedom in the society.

After the amendments, in the new version of the CCA enforced since May 2017, the phrases "dishonestly or deceitfully" and "but not constituting a crime of defamation under the Penal Code" were added to show the intention of the National Legislative Assembly drafting sub-committee to stop the enforcement of Section 14(1) against online criticism and comments. The compoundable and less harsh punishment conditions in paragraph two also show a good sign for online expression. However, the word "distorted" was added at the last minute by the drafting sub-committee to maintain the possibility of charging online opinion with Section 14(1). The new Section 14(1) has created confusion for interpretation. We have not yet seen any court's decision on the new Section 14(1) that benefits the future interpretation. On the other hand, cases under Section 14(1) in the court process are still going on and the number of cases is not decreasing.

CASE STUDY 1: ROYAL NAVY VS. PHUKET WAN26

A journalist and an editor of *Phuket Wan*, a small local English news website in Phuket Province, were charged with criminal defamation and with Section 14(1) of the Computer Crimes Act for publishing an article that accused the Thai Naval Force of being involved in and benefitting from trafficking of the Rohingya people. The Thai Royal Navy authorised a naval officer to report the case to the police.

The defendants argued that the news story published on the website actually referred to a Pulitzer Prize-winning report by Reuters. They had no intention to ruin the reputation of the Thai Royal Navy but were simply carrying out their journalism work. Moreover, when the Navy published its clarification on the report, *Phuket Wan* also publicised the Navy's statement. Later, the court dismissed the case, reasoning that Reuters is a reliable agency and therefore the information can be seen as truth.

CASE STUDY 2: CANNED FRUIT FACTORY VS. ANDY HALL²⁷

Andy Hall is a British researcher and a human rights defender. His studies focus on human rights violations against migrant workers. He was sued after publishing research on the violation of labour rights of migrant workers in the international private label products industry in Thailand. This case started in 2013, the court accepted the case in 2015 and the witness examinations began in 2016.

Hall fought the case on the grounds of academic rights and freedom of expression. The information published in his research was from interviews with 12 migrant workers who had already left the country because of fear of intimidation by the company. The plaintiff argued that the information provided by Hall was false and he had failed to verify the information with the company before publishing it. The Court of First Instance sentenced Hall to a fine of 150,000 baht (USD 4,200) and three years in prison with a suspension. The company also filed another three cases against Hall based on different grounds but on the same topic. Hall is now not in Thailand.

CASE STUDY 3: THAI INDUSTRIAL EMPLOYER VS. LABOUR UNION MEMBER²⁸

In mid-2010, Songkram Chimcherd, an employee of Thai Industrial Gases Plc and a member of the Thai Industrial Gases Labour Union, was accused

^{26 &}quot;Thai Royal Navy vs Phuketwan news agency". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/554

^{27 &}quot;Andy Hall: Computer Crime case". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/469

^{28 &}quot;Songkram Chimcherd: member of the Thai Industrial Gases Labor Union (TIGLU)". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/177

of sending a defamatory email stating that a senior executive ordered him to stop participating in the Union's activities. Later, a settlement between the parties was made, but although the accuser withdrew the defamation charge, the lawsuit under the CCA could not be withdrawn, which meant that Songkram had to deal with the remaining case. However, the case was dismissed by the court since it could not be proved whether the defendant was indeed the email sender.

CASE STUDY 4: DOCTOR VS. PATIENTS' RIGHTS ACTIVIST²⁹

Preeyanan, a patients' rights activist who was the mother of a son with a disability caused by medical error during his birth, posted a message on her Facebook account about the unjustness of the Medical Council of Thailand and demanding a reformation. The Medical Council of Thailand saw the message as a false statement which damaged its reputation and filed the charges directly to the court under Computer Crimes Act Section 14(1) and defamation.

The court has already conducted preliminary hearings and decided to accept the case for consideration. This case is still going on at Nontaburi Provincial Court.

CASE STUDY 5. PTT OIL COMPANY VS. CRITIC³⁰

In 2014, PTT Public Company Limited, the biggest state-owned petroleum production company in Thailand, filed a criminal defamation charge and a charge under section 14(1) of the CCA against Saran, an administrator of the Facebook page "Take Back Thai Energy". The case is based on 21 Facebook posts accusing PTT of fraudulent practices, causing the rise of energy prices, hiring a third party to use violence against protesters, and interfering with the media.

The Court of First Instance ruled that the information that the defendant posted on the Facebook page was false because the evidence brought by the plaintiff was more admissible than the defendant's. The Court therefore sentenced him to 40 months in prison without suspension. Later the Court of Appeal suspended the prison penalty but ordered him to pay fine of 800,000 baht (around USD 24,000). The case is still under consideration by the Supreme Court.

iLaw's database has documented at least 52 cases under Section 14(1) of the CCA that are lawsuits against faithful criticisms, media agencies, social activists, human rights advocates or environmentalists. These cases can also be seen as strategic litigation against public participation (SLAPP).

Sections 14(2) and 14(3): Information against national security

Sections 14(2) and 14(3) of the Computer Crimes Act are usually not used alone to charge people. In the national security-related cases, the main offence is usually lèse majesté or sedition. People who express opinions online and are charged under offences against national security would be charged together with CCA Section 14(2) or 14(3) or sometimes both subsections. But when a case continues until the process of reaching a verdict, the court will punish the accused under lèse majesté or sedition as they are the same act and violate several provisions of the law under Section 90 of the Penal Code.

However, the new Section 14(2) of the CCA has provided many broader elements of the offence, for example, "public safety", "national economic security" and "infrastructure for the common good of the Nation". These terms are open to broad interpretation and new ways of prosecution under this law.

CASE STUDY 1: EIGHT FACEBOOK ADMINISTRATORS³¹

On 27 April 2016, police arrested Natthika Worathaiyawich, Harit Mahaton, Noppakao Kongsuwan, Worakit Sakamutnan, Yothin Mangkhangsangsa, Thanawat Buranasiri, Supachai Saibut and Kannasit Tangboonthina for authoring and disseminating satirical commentary on the Facebook page "We Love General Prayuth". These eight suspects are also the creators and administrators of the page. They have been charged with violating Section 14(1), (2) and (3) of the Computer Crimes Act, in conjunction with Section 116 of the Thai Penal Code. The case is currently on trial at Bangkok Military Court.

^{29 &}quot;Preeyanan: CCA case for criticizing Medical Council of Thailand". Freedom of Expression Documentation Centre. https://freedom. ilaw.or.th/en/case/804

^{30 &}quot;PTT company vs Admin of 'take back Thai energy' FB page". Freedom of Expression Documentation Centre. https://freedom. ilaw.or.th/en/case/777

^{31 &}quot;Eight Administrators of the Facebook page 'We love General Prayuth'". Freedom of Expression Documentation Centre. https:// freedom.ilaw.or.th/en/case/716

CASE STUDY 2: THANAKORN³²

In December 2015, Thanakorn was arrested and charged with violating Section 14 (2) and (3) of the CCA for copying and disseminating an infographic explaining the Rajabhakti Park military corruption scandal and for satirising the King's dog. He was also charged with sedition and lèse majesté for this conduct. He was detained in prison for months since the court denied his request for bail. Later the military court changed its order and gave him a provisional release. The case is still in the process of witness examination in military court.

CASE STUDY 3: KATHA33

Katha was an employee in a stock trading firm. After posting a message about a sell-off on the stock exchange, he was arrested and was accused of using "Wet Dream" as his alias to post messages on the Fah Deaw Kan webboard. His was charged for two counts including posting false statements that caused panic among the public and compromised national security, a breach as per the Computer Crimes Act, Section 14(2).

He denied all charges, claiming that the stock market had failed due to a rumour circulating before the post was published. However, the court did not agree with him. The Court of Appeal sentenced him to two years imprisonment for each count, or four years all together. The penalties were subsequently reduced by one third, and so the defendant was sentenced to two years and eight months in prison.

Section 15: Intermediary liability

Section 15 of the revised CCA states:

Any service provider who provides cooperation to, consents to, or connives at the commission of any crime under section 14 within a computer system under his control shall be liable to the same punishment as the criminal under section 14.

The Minister shall issue an announcement determining processes for the giving of warnings, the termination of the circulation of computer data, and the removal of such computer data from computer systems.

If the service provider successfully proves that he has observed the announcement issued by the Minister by virtue of paragraph 2, he needs not to undergo the punishment.³⁴

This is the only provision which criminalises internet service providers (ISPs). Before the amendment, the definition of ISPs under Thai law was very broad and included all kinds of service providers: internet service providers, content providers, platform providers and server hosting had the same liabilities under Section 15. The uncertainty of the time period for ISPs in the previous version of Section 15 also led to a culture of following law enforcement officials' recommendations and self-censorship among ISPs. The amendment of the CCA brought a new hope with the "notice and takedown" process for ISPs to avoid legal charges.

However, to implement the new provisions of the CCA, the Ministry of Digital Economy and Society has created a new notice and takedown system³⁵ with unreasonably short and restrictive time limits for ISPs to remove "infringing" online material. The time limits are as follows:

- Online material violating Section 14(1) must be removed within seven days after the complaint has been received.
- Online material violating Section 14(2) and 14(3) must be removed within 24 hours after the complaint has been received.
- Online material violating Section 14(4) must be removed within three days of the complaint being received.

The system allows anyone, including police officers, security officers, individuals, business competitors or any internet users, to send a notice to ISPs to take down any content. The system has also created a big burden for ISPs to consider whether the alleged infringing content is a violation of laws or not. In practice, it is foreseen that ISPs tend to remove almost all content they have received notifications for. On the other hand, law enforcement officials will use

^{32 &}quot;Thanakorn : Clicked like on lèse majesté facebook page and satirized royal dog". *Freedom of Expression Documentation Centre*. https://freedom.ilaw.or.th/en/case/702

^{33 &}quot;Katha: Wet dream (Stock falling case)". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/83

³⁴ English translation sourced from: https://thainetizen.org/docs/ cybercrime-act-2017

³⁵ iLaw. (n/d). DE Ministry giving clear warning for notice and takedown of data breaching national security within 24 hours. *iLaw.* https://ilaw.or.th/node/4607

the procedure under Section 15 and the Ministry's regulation to send notifications to ISPs to take down content that the government perceives as a threat.

The process of disputing a takedown under the new regulation is also quite onerous for an "infringing" internet user. First, there is no boilerplate counter-notice that is available to the internet user, and second, ISPs have full discretion to decide whether to re-upload the existing content. In addition, internet users are considerably disadvantaged as there is no legal avenue for them to dispute the takedown of their material.

CASE STUDY: CHIRANUCH PREMCHAIPORN³⁶

Chiranuch Premchaiporn, the director of the Prachatai website, an independent online news network, and web administrator of the Prachatai webboard, was charged as an intermediary for her failure to comply with the timely removal of allegedly illegal messages from the webboard. The messages were deemed an insult to the King, the Queen or the Heir Apparent. Chiranuch was accused of being complicit or consenting to have the opinions posted on the Prachatai webboard under Section 15 of the CCA.

Chiranuch was arrested on 6 March 2009. She fought the case and got bail. She argued that she had done her duty to remove any illegal content but the posted messages were too numerous and she could not remove them fast enough.

The Criminal Court dismissed the charges for nine messages, given that Chiranuch did try to remove them. For the only one message that stayed for 20 days before she received a warrant and removed it, the Court deemed her as complicit or consenting. Therefore, Chiranuch was sentenced to one year in prison and a fine of 30,000 baht (roughly USD 900). The penalty was reduced by one third.

The plaintiff and the defendant submitted an appeal. The Court of Appeal later reaffirmed the first verdict and the defendant submitted the case to the Supreme Court. On 23 December 2015, the Supreme Court again reaffirmed the verdict. The case has now ended and leaves the only interpretation precedent of the online intermediary liability in Section 15 of the CCA before the Ministry's regulation has set a new practical standard.

Laws against peaceful assembly

Under the NCPO regime, the right to peaceful assembly has been severely curtailed through unilateral executive orders and legislation passed by the rubber-stamp National Legislative Assembly:

- NCPO Announcement No. 7/2014 (issued on 22 May 2014)³⁷ – Public gatherings of five people or more are banned, with violators facing a punishment of one year in prison or a fine of 20,000 baht (USD 560) or both.
- NCPO Announcement No. 57/2014 (issued on 7 June 2014)³⁸ – Political parties are banned from organising meetings or carrying out any political activity.
- Head of NCPO Order No. 3/2015 (issued on 1 April 2015)³⁹ – Article 12 of this executive order bans political gatherings of five people or more. Violators face a prison term of up to six months or a fine of 10,000 baht, or both.
- The Public Assembly Act (issued on 9 July 2015, and in effect from 13 August 2015).⁴⁰

The Public Assembly Act contains a series of restrictions on public assemblies:

- It requires protesters to "notify" the local police 24 hours in advance about the objective, date, place and time of the assembly. The authorities, however, have the power to allow or not allow the protest. This notification system seems to be a permission procedure.
- It bans demonstrations within 150 metres of royal places, or within the compounds of the Government House, Parliament and courthouses, unless a specific area has been authorised and designated by the authorities.
- It bans rallies from 6 p.m. to 6 a.m.
- It bans the use of amplifiers from midnight to 6 a.m.
- It prohibits protesters from blocking entrances.
- It prohibits any disturbance at government offices, seaports, train or bus stations, hospitals, schools and embassies.

^{36 &}quot;Chiranuch Premchaiporn: Director of Prachatai". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/112

³⁷ English translation sourced from: http://library2.parliament. go.th/giventake/content_ncpo/ncpo-annouce7-2557.pdf

³⁸ English translation sourced from: http://www.mea.or.th/moi/ pomc/doc/ncpo57.pdf

³⁹ English translation sourced from: http://library2.parliament.go.th/ giventake/content_ncpo/ncpo-head-order3-2558.pdf

⁴⁰ English translation sourced from: https://tlhr2014.wordpress. com/2015/11/06/thailands-public-assembly-act-2015-procedureson-notification-of-public-assembly-authorised-equipments-forcrowd-control-and-limitation-of-utilizing-the-sound-amplificationequipments

In the event that local police consider any assembly as a violation of the stated conditions, the police must first ask the protesters to disperse. If the protesters do not comply, the police need to seek a civil court's permission to force the protesters to disperse.

Violators of these provisions face a prison term of up to six months and a fine of up to 10,000 baht, or both. To date, at least 20 people have been charged for violating these conditions. Mostly they were charged for not informing the police in advance, using amplifiers without permission, or organising an assembly in a restricted area. These are offences with low penalties.

The problems of the enforcement of NCPO orders

NCPO Announcement No. 7/2014 was issued almost immediately after the military staged a coup on 22 May 2014. Its aim was to disperse all the political demonstrations that lasted for months before the coup and caused chaos within the country. And the NCPO also needed the power to control dissent and prohibit people from opposing the unlawful coup. However, the announcement has never been abolished or amended until today.

After martial law was lifted on 1 April 2015, Head of NCPO Order No. 3/2015 was issued to give special power to military officers instead of the martial law. The provision to prohibit political gatherings was also prescribed in Article 12 with half the penalty rate. Therefore, it was confusing since the NCPO had two provisions that ban political gatherings at the same time. In practice, after 1 April 2015, Head of NCPO Order No.3/2015 was used by security officers to prohibit all kinds of gatherings including academic seminars or discussions on other social issues.

People who defy these orders and gather under the NCPO regime can also be arrested and taken to an "attitude adjustment" programme, and if they comply, the NCPO can release them without charges. However, there are at least 278 people who were charged for defying NCPO Announcement No. 7/2014 and Head of NCPO Order No.3/2015. The cases of defying any NCPO orders or announcements are all taken to military courts.

CASE STUDY 1: APICHAT⁴¹

Apichat was arrested and charged with violating Announcement No. 7/2014 for participating in a protest against the May 2014 coup in front of the Bangkok Arts and Cultural Centre on 23 May 2014. The protest consisted of 500 members of the public but the officers claimed that Apichat stood out because he was holding a paper sign and shouting loudly. Apichat was also charged with violating Section 216 of the Criminal Code for failing to disperse after authorities had ordered the assembly to do so. The case is still ongoing in the Court of Appeal.

CASE STUDY 2: CHAINARIN42

Chainarin was charged under Announcement No. 7/2014 for a public assembly at the Siam Paragon shopping mall, displaying a sign stating "The coup makers fear A4 paper, [the] A4 paper is coming to you now", and reading a poem critical of the May 2014 coup. He was also charged under Section 215 of the Criminal Code. Chainarin was then taken to military court in Bangkok where he confessed. The court sentenced him to three months in prison with suspension and a 5,000 baht fine.

CASE STUDY 3: SEVEN DAO DIN ACTIVISTS43

On 22 May 2015, seven student activists from Khon Kaen University, members of the community rights activist group Dao Din, were arrested and charged under Order No. 3/2015 for gathering at the Khon Kaen Democracy Monument and displaying a banner protesting the May 2014 coup, on the anniversary of the coup. They were all charged on the day of arrest. All of them declared civil disobedience by not reporting or participating in the process under the NCPO orders. One of them was already arrested and prosecuted. The case is still ongoing in the Khon Kaen military court.

CASE STUDY 4: NATCHACHA AND THATCHAPONG44

A total of 38 activists were arrested for participating in a symbolic assembly in front of the Bangkok Arts and Cultural Centre on the

^{41 &}quot;Apichat: Protest Against the Coup". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/679#detail

^{42 &}quot;Chainarin : Defying the NCPO order and Ciminal Code Article 215". *Freedom of Expression Documentation Centre*. https://freedom. ilaw.or.th/en/case/610#detail

^{43 &}quot;7 Dao Din: Hold Banner against the Coup". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/683

^{44 &}quot;Natchacha and Tatchapong: Took action in front of the BACC". *Freedom of Expression Documentation Centre*. https://freedom. ilaw.or.th/en/case/688#detail

one-year anniversary of the May 2014 coup. All of them were released the next morning but later nine of them were summoned to be charged under Announcement No. 7/2014. Seven of them declared civil disobedience by not reporting or participating in the process under the NCPO orders. But two persons decided to cooperate and fight the case. The case is still ongoing in the military court.

CASE STUDY 5: RESISTANT CITIZEN GROUP⁴⁵

Anon Nampa, Pansak Srithep, Wannakiat Choosuwan and Sirawith Sereethivat were charged under Announcement No. 7/2014 for participating in a symbolic activity called "My Dear Election" in front of the Bangkok Arts and Cultural Centre on 14 February 2015. The assembly was considered as a political activity since it talked about an election. The case is still ongoing in the military court.

CASE STUDY 6: EIGHT ACADEMICS⁴⁶

Eight academics were accused of defying Head of NCPO Order No. 3/2015 after they delivered a statement titled "Universities Are Not Military Camps" at a hotel in Chiang Mai to protest against Gen. Prayuth's speech accusing university lecturers of teaching students the subject of democracy. Later, six academics reported to the commander of the military unit in Chiang Mai and signed a memorandum of understanding in which they agreed to not participate in any political movement. The charges against those six academics, therefore, were withdrawn.

CASE STUDY 7: RATCHABURI REFERENDUM MONITORING CENTER

On 19 June 2016, the United Front for Democracy against Dictatorship (red shirt movement) prepared for the opening of the Center for Referendum Watch nationwide to monitor possible fraud in the 7 August 2016 military-run constitutional referendum. One of the centres was set up in Banpong district of Ratchaburi province. Around 20 persons came to take a picture with a banner of the centre. Even though the activity at Banpong ran smoothly without intervention from the authorities, such as in other provinces, later on someone went to report the case to the police. As a result, 18 individuals were summoned to acknowledge the charges under Head of NCPO Order No. 3/2015. All the persons accused denied the charges, and they were released on the same day without depositing bail bonds.

The problems of the enforcement of the Public Assembly Act

There were many discussions on a public assembly law for almost 10 years before the Public Assembly Act 2015 was passed by the junta-appointed parliament, the National Legislative Assembly. At the early stage of its enforcement, many groups and movements did not know that it existed, as there was no public participation during the drafting and consideration process. Some of them were prohibited from gathering, some were arrested and charged. After news reports on the charges, the wider public acknowledged the existence of the new law.

However, since the act is quite new, there is no legal precedent from the court to interpret the provisions and low-level officers do not understand the law thoroughly. There are some provisions that are still debatable with regard to their interpretation such as the definition of "public spaces" or the "royal county".

In practice, assemblies on political and non-political issues are treated differently. In one instance, even though the organisers informed the local police 24 hours in advance and complied with all conditions under this Act, political activities were still banned claiming the power of Head of NCPO Order No. 3/2015. The non-political activities were allowed to proceed except for an assembly near the parliament or government house, on the grounds that it was the "royal county" area.

CASE STUDY 1: "JUST STANDING" ACTIVITY47

On 27 April 2016, the police arrested 16 individuals, including human rights lawyer Anon Nampa, for participating in a peaceful symbolic

^{45 &}quot;My Dear Election". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/658

^{46 &}quot;Academics delivered a statement titled 'Universities Are Not Military Camps'". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/700

^{47 &}quot;Anon: Just standing (second case)". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/759#uploads

protest at the Victory Monument. The protest, "Just Standing", demanded the release of nine individuals who were abducted and held in military custody on the same day. Anon Nampa, the leader of the Resistant Citizen movement⁴⁸ and organiser of the assembly, was charged with violating the Public Assembly Act for failing to notify the authorities about the assembly in advance, and was convicted of the charges by a municipal court. He was fined 1,000 baht.

CASE STUDY 2: SATHANONT49

A participant at an organised charity activity called "A March to Inform of Merit" in Sakon Nakhorn province was charged under the Public Assembly Act. The activity aimed to invite local villagers to participate in a cultural activity to protect the community's river. In addition to the accusation of failing to notify the authorities, Sathanont was also charged under the Traffic Act for obstruction of the public highway. The case is still ongoing.

CASE STUDY 3: SAMA-AE⁵⁰

Sama-ae, a fisherman from an association of fisherfolk, was charged for publicly gathering and delivering a letter to the Minister of Agriculture and Cooperatives to call for an amendment to the Fishing Act. He was charged for failing to notify the local police. He fought the case on the grounds that he and his friends gathered to submit the letter only, without an intention of public gathering. The case has since been dismissed.

CASE STUDY 4: ANTI-MINING PROTESTERS IN PHICHIT⁵¹

A total of 27 villagers in Phichit province were charged for gathering on a road that vehicles of the Akara Mining Company were using to transport the ore from the gold mine. In addition, the villagers were also charged under Section 309 of the Criminal Code⁵² for extorting the company. The protesters were fighting against the operation of the gold mine which they felt had an impact on the environment in their homeland. The court gave them suspended sentences.

Overall analysis on freedom of assembly

NCPO Announcement No. 7/2014 and Order No. 3/2015 completely remove the freedom of peaceful assembly. This blanket removal is a violation of Thailand's obligation under the International Covenant on Civil and Political Rights (ICCPR) and is designed as a content-based restriction by the NCPO as a large majority of protests in this time were against the legitimacy of military rule and the military coup. As observed in the cases in this report, most of the charges under these two executive orders are activities directly against the NCPO.

The many restrictions imposed by the Public Assembly Act show that these laws violate the principle of proportionality. The principle of proportionality dictates that the least intrusive restrictions should be prioritised by the authorities to ensure that the nature and character of the assembly are not fundamentally altered. However, the restrictions imposed by the Public Assembly Act on the locations, time and manner of assembly are not the least intrusive restrictions, and would fundamentally alter the nature and character of the assembly. For example, should a certain assembly intend on protesting an act of a ministry or the National Legislative Assembly, their rationally selected location of assembly outside the Government House or the Parliament would only be permissible if the protest is not within the compounds of those buildings or takes places at a distance further than 150 metres away from the buildings. This restriction has the effect of changing the character of the assembly should it be essential for the assembly's message and methods that their location should be within the compounds of the buildings or at a proximate distance outside of them. The alteration of the character and nature of the assembly is also enabled by the other restrictions, if the group intends on using an amplifier to convey its message, or if it chooses to operate between 6 p.m. to 6 a.m. These restrictions also could potentially interfere with the message communicated by the assembly.

⁴⁸ https://www.facebook.com/Resistantcitizen

^{49 &}quot;Satanont: Public assembly case from merit activity". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/796

^{50 &}quot;Sama-ae: Fish Flok's Public Assembly Act case". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/708

^{51 &}quot;Villagers in Phichit Protest against Mining". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/782

^{52 &}quot;Illegal Detention (Sections 309-311)". Siam Legal. http://library.siam-legal.com/thai-law/ criminal-code-illegal-detention-sections-309-311

The requirement to notify authorities should also take the form of a notice of intent, and not a request for permission. This is essential to recognise that spontaneous assemblies, due to their nature and character of organisation, would make it impossible for the organisers to notify within the set time limits. However, the notification restriction in the Public Assembly Act does not recognise this, and thus, discriminates against spontaneous public assemblies.

NCPO Announcement No. 7/2014, Order No. 3/2015 and the Public Assembly Act do not respect the right of individuals to use public spaces. As stated, most of these highlighted cases involve public assemblies at shopping malls or national-historical landmark or commemoration sites. However, these laws have been used to disrupt the use of public spaces for assemblies. The use of these spaces is integral to the success of the assembly in conveying its message, as typically, these public spaces are chosen based on the specific target audience of the assembly.

Local ordinances and low-level criminal law are also used to repress public assemblies. For example, the Cleanliness and Good Order Act has been used against activities such as scattering post-it notes and distributing leaflets, and the Amplifier Act 1950 has been used against many organisers of street activities.

Contempt of court

Contempt of court laws in Thailand are broadly distinguished between "insult of the court" (conventionally, indirect contempt) and "contempt of court" (direct contempt). Provisions governing "insult of the court" are found in Section 198 of the Penal Code, which states:

Whoever insults the Court or the judge in a trial or adjudication of the case, or obstructs the trial of adjudication of the Court, shall be punished with imprisonment of one to seven years or fined of 2,000 to 14,000 Baht, or both.

The provision governing "contempt of court" (direct contempt) is found in Section 30 of the Civil Procedure Code, which states:

The Court shall have the power to give to any party or any third person present in the Court such directions as it may think necessary for the maintenance of order within the precincts of the Court and for the fair and speedy carrying out of the trial. Such power includes the power to prohibit the parties from taking any vexatious, dilatory or superfluous proceeding. Section 31 of the Civil Procedure Code⁵³ lists types of behaviour that qualify as contempt of court offences. These are:

- Refusal to comply with any directions given by the court.
- Improper behaviour within the court's precincts.
- Presenting false evidence or statement(s) to the court during an inquiry to have the court's fee waived.
- Intentionally evading court orders if said party knows that they will be served with a Court order or document(s).
- Inspecting the file(s) of a case or obtaining a copy of the file(s).
- Disobeying a court order to appear in court.

These actions fall into the direct contempt category. Section 33 of the Civil Procedure Code states:

Where in any court, any party or person commits contempt of court, the court shall have the power to punish the offender whether to order him or her to leave the court room or sentence up to 6 months in prison or fine up to 500 Baht or both.

These provisions in the Civil Procedure Code grant the court special and arbitrary powers to punish an "offender" immediately without having to conduct an inquiry or witness examination or allowing the defendant to face trial.

In addition, contempt proceedings are conducted in a different manner to a normal criminal proceeding in these ways:

- Judges in contempt cases have the power to deliver a verdict and sentence (if convicted) to defendants immediately, if the offence happened before the judges. This is intended for the proceedings to run smoothly. Supreme Court Decision No. 4617/2004 states that this immediate-sentencing power does not depend on whether the offence was conducted in visible sight of the court or if the court knows about the offence from other evidence. In addition, the offence does not have to be reported to the police. It is clear that the rights of the defendants to trial proceedings are violated.
- Supreme Court Decision No. 635/2016 established that the trial proceedings for a contempt case are not a general criminal trial proceeding. The rights of the defendant set out in the Criminal

⁵³ English translation sourced from: https://www.imolin.org/doc/ amlid/Thailand_The%20Civil%20Procedure%20Code.pdf

Procedure Code do not exist in the Civil Procedure Code. Trials can proceed with defendants not being legally represented. As the inquiry process is a fact an inquiry, not a witness examination, the accused is not required to swear under oath.

• Even though the inquiry process needs to be conducted, it can be conducted without the presence of the accused. The court can conduct the process by itself where the court acts as an injured person, an accuser, a prosecutor, an inquirer and the decision maker by itself.

In the midst of long-lasting political conflict, the judiciary institution continues to exercise its power to interpret the laws, to adjudicate and to rule decisions on cases. However, there have been many cases where those holding power enact laws and implement them to suppress opposition. The court therefore has been pulled to play a part as the law enforcement institution and oftentimes the political actors claimed for their own legitimacy from the court orders. Many times in recent memory. courts' decisions have created a big impact on Thai politics and society - For example, the decision that the election was invalid in 2014, and the decision to revoke political parties and ban more than 100 politicians from electoral rights for 10 years in 2006. Both decisions led to political dead ends and opened a walkway for military coups.

During political conflict, where those with antiestablishment political views are prosecuted in court, discontent arises and the society begins to question the performance of the court. Offences of insult of court and contempt of court, therefore, are used against them to obstruct anti-establishment movements and restrict criticism and verbal attack against the court by people who are politically suppressed.

CASE STUDY 1: SUDSA-NGUAN SUTHEESORN⁵⁴

Sudsa-nguan Sutheesorn, Picha Wijitsilp and Darunee Kritboonyalai were sentenced to a month of imprisonment after being found guilty by the Supreme Court under "contempt of court" on 8 November 2016. The three individuals led a protest in front of the Civil Court on 21 February 2014 to protest the decision of the Civil Court in invoking the Emergency Law declaration. The protesters laid a wreath of flowers in front of the Civil Court with a message reading "for the injustice of the Civil Court." The Supreme Court's reasoning for the judgement was that the act of the three defendants in assembling a group of protesters outside the Civil Court was an attempt to pressure the Court and sabotage the judiciary. The Supreme Court opined that this act could deprive the court of its impartiality as it could be pressured to make a judgement that the protesters view favourably.

CASE STUDY 2: SEVEN ACTIVISTS⁵⁵

Benjamas (a pseudonym), Narongrith, Panupong, Akhom, Payu and Sirawith were charged with contempt for participating in an organised symbolic activity outside the fence of Khon Kaen Provincial Court to show their support toward a defendant (Jatupat "Pai Dao Din") in a lèse majesté case. The protestors used pieces of wood to imitate a tilted scale, with a military boot hanging on one side and an empty bucket on the other. There was also the reading of a statement, song singing, and encouragement to lay down a white rose on the base of the scale. Sirawith was given a suspended sentence of six months in prison and a 500 baht fine, while the other six activists were given one year of probation and 24 hours of community service.

CASE STUDY 3: WATTANA MUANGSOOK⁵⁶

Wattana Muangsuk, a former MP from the Pheu Thai Party, was given a suspended sentence of two years and fined 500 baht for conducting a Facebook Live transmission while he was detained in the detention room of the Criminal Court. Wattana was brought to obtain pre-trial detention for his sedition case, which was due to a Facebook post calling for support on the Yingluck Shinawatra rice-pledging scheme case. The cause of his contempt of court was not the content of what he said in the live feed but because he defied the court's regulation that photos or videos are prohibited in the court building without permission.

^{55 &}quot;Case: Contempt of Court case against activists (Khon kaen Provincial Court)". *Freedom of Expression Documentation Centre*. https://freedom.ilaw.or.th/en/case/772

^{54 &}quot;Case: Sudsanguan: Protested in front of Civil Court". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/754

^{56 &}quot;Case:Wattana: Contempt of Court by Facebook Live", Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ case/802

Overall analysis on contempt of court

With regard to the Thai offence of "insult of the court", similar to other countries, there is an inherent clash between maintaining the authority of the judiciary, the right to a fair trial and freedom of expression. However, the Thai treatment of "insult of the court" differs from other countries in that there is no strict legal test to determine if an "offence" has been committed. These strict legal tests that exist in other countries ensure that freedom of expression is not infringed unjustly. In addition, a defence to be established on truth and fair comment and the social need for public interest is not supported in Thai "insult of the court" cases. As demonstrated by the Supreme Court's legal reasoning in the case of Sudsa-nguan, there is no clear and sound legal test applied to show how the "offence" has a high likelihood of undermining and prejudicing the administration of justice and that the legal process was seriously prejudiced.

Another problem arises from the lack of a clear and consistent interpretation of the word "court vicinity". A Facebook post conducted at the offender's house was once interpreted as a punishable act with intention to cause damage in the court vicinity. The case against seven activists was for an activity clearly conducted outside the court's fence but near the court sign, while there was a court decision to punish a person who wrote and submitted a complaint letter against judges to official bodies outside the court building.

The legal proceedings for contempt cases are conducted in a special procedure that violates the rights of the accused. That legal representation for defendants is not a requirement for the trial is a violation of Article 14 of the ICCPR. Decisions by judges are often made in a short space of time, demonstrating that judges do not give sufficient consideration to determine if the trial proceedings in question have been impeded or prejudiced or if the reputation of the judiciary has been impaired.

Section 61 of the Referendum Act of 2016

In April 2016, the junta-appointed parliament passed the Referendum Act 2016 for the constitutional referendum on 7 August 2016. The draft constitution was written by a committee appointed by the NCPO without any public participation in the drafting process. The draft also installed many new mechanisms to ensure the military roles in politics; for example, it appointed 250 senators, set up the ethical standards for politicians, and established that the national strategy would be drafted by the junta. The NCPO therefore needed this draft to pass the referendum with as little resistance as possible. The Referendum Act of 2016 was enacted for a constitutional referendum and to control the political atmosphere before the referendum date. Section 61 was the main problem of this law, as it limited freedom of expression on criticism of the draft constitution. Section 61 of the Referendum Act states:

Any person who commits following acts; (1) to cause confusion to affect orderliness of voting,

Anyone who publicizes text, images or sound, through either newspaper, radio, television, electronic media or other channels, that is either untruthful, harsh, offensive, rude, inciting or threatening, with the intention that voters will either not exercise their right to vote, or vote in a certain way, or not vote, shall be considered as a person causing confusion to affect orderliness of voting.

Any person commits the act to cause confusion to affect orderliness of voting shall be punished with imprisonment of not exceeding 10 years and a fine of up to 200,000 Baht. The Court may order to revoke his/her right to vote of not exceeding five years.

If the offences are committed by a group of five persons or more, each person shall be punished with imprisonment of one to ten years, a fine from 20,000 to 200,000 Baht and a 10-year revocation of voting right by court.⁵⁷

The Referendum Act of 2016 caused a lot of problems in the society because the legislators did not limit the officials' authority and did not try to protect people's freedom of expression. Therefore, there were a lot of innocent people who were affected by this act.

Under the military rule, from 25 April 2017 to 7 August 2017, at least 64 individuals have been arrested or charged under Section 61 of the Referendum Act and from 19 June 2017 to 30 July 2017, at least 131 individuals have been charged under Head of the NCPO Order No. 3/2015 and other laws for participating in activities related to the referendum.⁵⁸

⁵⁷ Thai Lawyers for Human Rights. (2016, 12 July). Vote-No Activists and Reporter Prosecuted under Constitution Referendum Act. *Thai Lawyers for Human Rights*. http://www.tlhr2014.com/th/?p=1107

^{58 &}quot;Table of charges against Referendum Act of 2016". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/ node/363

The problems arising from the legal provision itself

Ambiguity of the law

There are several ambiguities in the legal provision, for example, the terms "harsh", "offensive" or "inciting". It is difficult to know which expression constitutes an offence against this section. Moreover, there are no definitions for these words in the Penal Code. This is against the principle of the Criminal Code that there should be clear definitions, so people can know their rights and freedoms.

Criminalising rude words

Expressing oneself with "rude" words may not be proper, but under normal circumstances it is not illegal. Moreover, there are no clear definitions explaining which words constitute rudeness. The interpretation of which words are rude is subjective and depends on the situation.

Limiting point of view

The use of the term "untruthful" in this act causes problems because when people read the draft constitution, they use their own experiences, ideas and beliefs to interpret the draft constitution. This means that people could have opinions on the draft constitution that might be different from those of the individuals who wrote it.

The problems arising from its enforcement

Use of the Referendum Act to threaten dissent

The military government kept advertising the good aspects of the draft constitution through millions of leaflets, all television channels and all kinds of media. Even Gen. Prayuth, the head of the NCPO, gave an interview to say that he would vote in favour of the draft. The drafting committee refused to join any debate, given that it was not its duty as a neutral body. But campaigns against the draft were strictly repressed. All of the people who were arrested and charged were "Vote No" supporters. The Election Commission also played an active role to threaten and prohibit people from campaigning.

For example, Somchai Srisutthiyakorn, a member of the Election Commission, said that he was told that there was a Facebook page of one political movement which sold t-shirts. Those t-shirts had messages that might affect the voters, so this might qualify as an offence under Section 61 of the Referendum Act. The political movement that Somchai mentioned was the New Democracy Movement and the message on the t-shirts was: "Vote No for the future we didn't choose".

Use of the Act to lay charges for unclear offences

An example of this was the case of "Vote No" stickers in Banpong District, in which the five defendants were allegedly carrying anti-constitution materials. However, they were charged with only the "Vote No" stickers with a message "Do not accept an unchosen future". Even in the complaint that was filed with the court, there is no clear explanation of how such messages violate the law.

CASE STUDY 1: CHUWONG⁵⁹

Chuwong, a lawyer and leader of the Krabi Landless Peasantries Group, posted a message on Facebook stating that he would vote no to the draft constitution on 7 July 2016. Someone saw his message on Facebook and went on to report the case to the police. On 15 July 2016, the police requested the court to issue an arrest warrant against Chuwong under the Referendum Act. Chuwong went to report to the police on 16 July and denied the charge. The police released him on bail on the same date with a cash deposit of 150,000 baht.

CASE STUDY 2: "VOTE NO" STICKERS⁶⁰

On 10 July 2016, Pakorn, Anan and Anucha, three New Democracy Movement activists, and Taweesak, a Prachatai journalist, were taken to Ban Pong police station for allegedly carrying anti-constitution material in their car. Later on, Phanuwat, a student from Maejo University, was taken from his residence in Ratchaburi to the police station. They were charged with violating Section 61, paragraph 2 of the Referendum Act for distributing the stickers, and were detained at the Ban Pong police station. On 11 July 2016, Ratchaburi Provincial Court granted bail to the five for 140,000 baht each. The trial of this case has finished. The court will render a verdict on 29 January 2018.

CASE STUDY 3: PIYARAT⁶¹

Piyarat, a 25-year-old activist, went to cast his vote at a polling station in the Bangna District Office on 7 August 2016, which was

^{59 &}quot;Chuwong: Posted Status Vote No to Draft Constitution". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/ en/case/724

^{60 &}quot;Vote No Sticker at Banpong District". Freedom of Expression Documentation Centre. https://freedom.ilaw.or.th/en/case/730

^{61 &}quot;Piyarat:Tearing Referendum Ballot". *Freedom of Expression* Documentation Centre. https://freedom.ilaw.or.th/en/case/732

the referendum date. After receiving a ballot, Piyarat tore it into pieces and shouted, "Down with dictatorship, long live democracy." The authorities immediately arrested Piyarat along with Thongtham and Jirawat, who filmed and uploaded the incident on social media, under the Referendum Act for disrupting the peace in a polling station.

On 26 September 2017, the Phra Khanong Provincial Court acquitted the three defendants of the charge of conspiring to create disorder in a polling station under the Referendum Act. As for Piyarat, who tore up his ballot, the court sentenced him to two months in prison and fined him the sum of 2,000 baht for destroying another's property. Piyarat's prison sentence was, however, suspended for a year.

Spread news, create fear: A more effective tool than legal measures

Apart from exercising legal powers to arrest and prosecute individuals for political dissent, the NCPO government has also used social or psychological measures to create a climate of fear in the public. Whether or not the NCPO planned to create a climate of fear, freedom of expression in Thailand has been affected. When people began to feel uncertain of how much they could express their opinion, they started to censor themselves and politics became a taboo topic in the society.

Normally, when the NCPO government uses legal actions to arrest political dissidents and charges them with sedition or lèse majesté, the NCPO holds a press conference. The NCPO has never prohibited any media reports about charges against political dissidents, so stories of their arrest and punishment could spread out.

Moreover, for the last three years under the NCPO government, officials have taken turns to provide news about new measures to control online media, most of which were just threats. For example:

On the afternoon of 28 May 2014, six days after the coup, there was some anti-coup protest which had been organised via Facebook. Then Facebook went offline for one hour, but the NCPO denied that they had any part in it. This demonstrated the NCPO's power to the people, and that the NCPO could do it if they wanted to.⁶²

- On 6 January 2015, the Cabinet accepted the principles of 10 drafts of digital security laws. One of them was the draft of the National Cyber Security Act, which contained Section 35 that allowed officials to spy on internet communication, email and phone calls without any court warrant. This caused a widely known public disagreement. In the end, these 10 drafts of digital security laws had to be put on hold, but eight of them were enacted one after another. However, most of those acts were about arrangement of the organisation's structure.⁶³ The draft National Cyber Security Act and the draft Online Privacy Protection Act had not been enacted vet and there was not any sign if they were going to be enacted soon.
- In September 2015, there was news reported that the government was developing a policy to create a single gateway system to take control over internet communication, even though this was not practical in Thailand. A single gateway was beyond the capabilities of Thailand's current technology and capital expenditure. Moreover, the government would have had to pass laws to take back the gateway's business which was now in the hands of the private business sector. Thus, this was hardly possible in reality. After news about this controversial policy was widespread, the society was against it. People were afraid that they might be under surveillance and blocked from information that the government did not want them to know.
- On 8 March 2017, the National Reform Steering Assembly (NRSA), a junta-appointed assembly for national reform purposes, introduced the draft "Media Registration Act". This draft law enforced all the media including online media such as Facebook fan pages to register with the National Press Council of Thailand and be under the regulation of a code of ethics. After this draft came out to the public, it was opposed by Thailand's professional media organisations. The NRSA subsequently amended the draft many times. It should be noted that the NRSA did not have legislative power and it could only give suggestions. Thus, in order for the draft to become a law, the cabinet would have to approve it and then the National Legislative Assembly would have to pass it. However, there is no longer any consideration of this draft.

⁶² Becker, O. (2014, 28 May). Thailand's Military Denies Briefly Banning Facebook. Vice News. https://news.vice.com/article/ thailands-military-denies-briefly-banning-facebook

⁶³ Thai Netizen Network. (2015, 15 January). Thailand's Digital Economy-Cyber Security Bills [English translation]. https:// thainetizen.org/2015/01/digital-economy-cyber-security-bills-en

- On 12 April 2017, the Ministry of Digital Economy and Society released a prohibition order preventing people from contacting three persons, Somsak Jeamteerasakul, Pavin Chachavalpongpun and Andrew MacGregor Marshall. The order was announced on online media so people would not dare to go and see these three's Facebook posts. This raised the question as to whether being a "friend" on Facebook with these three persons was legal or not. Hours later, Captain Somsak Kaosuwan, Deputy Permanent Secretary, Ministry of Digital Economy and Society, explained that this order had no legal effect.
- In May 2017, Provincial Police Region 1 announced that even though it could not arrest persons who posted content against the monarchy on Facebook who were in exile abroad, it had eyes on those Facebook pages. What we should bear in mind is that visiting and reading content on social media were not illegal under any existing laws.
- On 8 June 2017, the National Broadcasting and Telecommunication Commission (NBTC) announced an "over the top" system to regulate online content. The NBTC ordered all online media that had an online platform, for example, YouTube and Facebook, to register. The NBTC reasoned that YouTube and Facebook, which provide platforms for live streaming, are also broadcasters. This was all self-interpretation. Since then, the NBTC has not issued any rule or regulation on how to register with it and there is no one really registered with the "over the top" system. Under the NBTC Act, there is not any section that grants the NBTC such power.
- On 3 July 2017, the NRSA, through its steering committee on mass communication reform, released a "suggestion report" which

recommended a system through which all mobile phones, especially prepaid phones, would need to be registered with the NBTC, using fingerprints and facial scan identification cards all across the country. This became big news online and offline, even though this was only a suggestion report which would not be brought to practice and in fact, such a system was beyond the capabilities of Thailand's current technology and beyond its legal authority.

Most people who were interested in freedom of expression or followed the news would not have enough time to do in-depth research on these matters. What they could do was just follow the hot news. They could not have known if these policies or proposed laws would be enacted in reality and affect their freedom or not.

Thus, most people would just remember that the government tried to legislate to regulate online media, to suppress freedom of expression and to access people's online personal data. However, most of them do not know that those regulations and measures cannot be carried out in reality.

The public's confusion and misunderstanding regarding those measures and the government's legal authority brought fear to the society, since people do not truly know what the government could and could not do. Self-censorship was the first thing people would do to guarantee their own safety. This climate of fear affects freedom of expression online and we have to say that this has had more effect than enforcing the laws.

If the military government really intended to use these social and psychological measures to threaten the people, it was a successful plan. It suppressed freedom of expression without enforcing any laws or arresting any political dissidents, and the NCPO did not have to waste any time on legal processes.

UNSHACKLING EXPRESSION: A study on laws criminalising expression online in Asia

Freedom of expression and opinion online is increasingly criminalised with the aid of penal and internet-specific legislation. With this report, we hope to bring to light the problematic trends in the use of laws against freedom of expression in online spaces in Asia.

In this special edition of GISWatch, APC brings together analysis on the criminalisation of online expression from six Asian states: Cambodia, India, Malaysia, Myanmar, Pakistan and Thailand.

The report also includes an overview of the methodology adapted for the purposes of the country research, as well as an identification of the international standards on online freedom of expression and the regional trends to be found across the six states that are part of the study. This is followed by the country reports, which expound on the state of online freedom of expression in their respective states.

With this report, we hope to expand this research to other states in Asia and to make available a resource that civil society, internet policy experts and lawyers can use to understand the legal framework domestically and to reference other jurisdictions.

GISWatch 2017 SPECIAL EDITION https://www.GISWatch.org