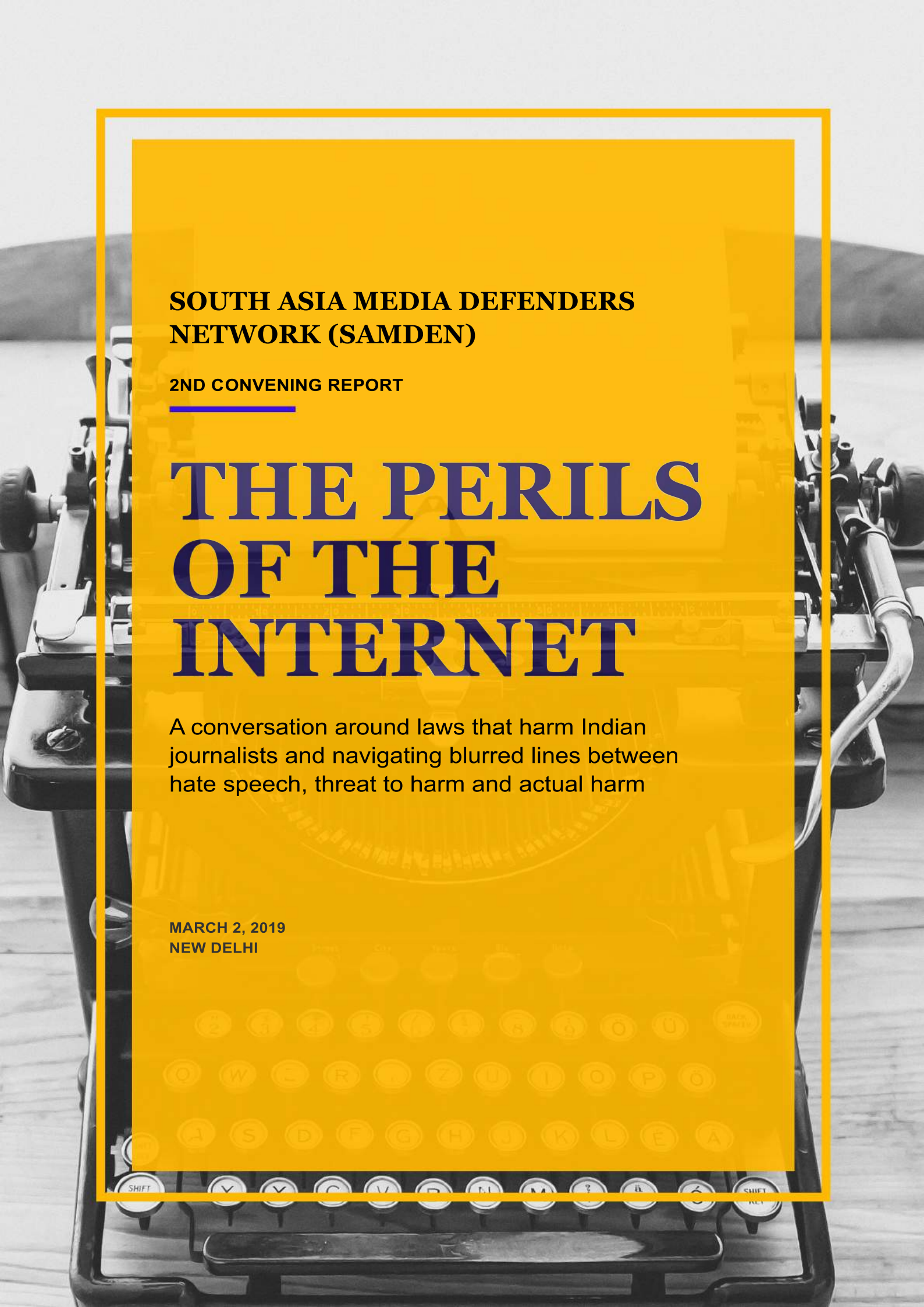

SOUTH ASIA MEDIA DEFENDERS NETWORK (SAMDEN)

2ND CONVENING REPORT

THE PERILS OF THE INTERNET

A conversation around laws that harm Indian journalists and navigating blurred lines between hate speech, threat to harm and actual harm

MARCH 2, 2019
NEW DELHI

ACKNOWLEDGMENTS

The South Asia Media Defenders Network (SAMDEN) is grateful to all who participated in its second convening and add to this report with their knowledge and experience.

We value the continuing support of all SAMDEN members for the network.

Convening participants generously gave their time towards this much-needed discussion: Kishore Bhargava, Technology Mentor, LinkAxis Technologies, Commodore Lokesh Batra, RTI activist, Akshit Sangomla, journalist with Down to Earth, Venkatesh Nayak, Head of CHRI's Access to Information programme, Smriti Singh Media and Advocacy manager at Amnesty International India, Patricia Mukhim, editor of The Shillong Times, Apar Gupta, Executive Director of the Internet Freedom Foundation, Joanne D'Cunha, associate counsel with the Internet Freedom Foundation, and Paranjoy Guha Thakurta, independent journalist, author and film-maker.

We are also very grateful to Mahfuz Anam, editor and publisher of Bangladesh's The Daily Star newspaper, Kumar Lopez, Director of the Sri Lanka Press Institute (SLPI), and Rana Ayyub, independent journalist and author, who took the time to join us over Skype and phone, and contribute to the discussion.

Richa Udayana, Media and Communications Officer, CHRI, helped organise the convening. Richa developed, wrote and designed this report which was edited by Sanjoy Hazarika, International Director, CHRI, and founder and co-convener of SAMDEN.

Sarthak Roy, Research Officer, CHRI, and Anju Anna John, Project Officer, CHRI, provided valuable inputs. We thank D Mohan Sundaram, Manager, Administration, and Kakoli Roy, coordinator, Acess to Justice programme, CHRI, for their logistical support, and appreciate the contribution of our intern Bhavayta Mahajan.

TABLE OF CONTENTS

INTRODUCTION

The South Asia Media Defenders Network (SAMDEN) was established in 2018 as part of CHRI's efforts to address the issue of increasing attacks on media workers and pressures on the freedom of speech and expression in the Commonwealth.

South Asia has a poor record in the areas of freedom of speech and expression where the space for voicing dissenting opinions has shrunk, gradually but alarmingly. Since August 2017, three Indian journalists were attacked in separate incidents, two fatally. The gunning down of eminent journalist, Gauri Lankesh, highlighted by the former UN High Commissioner in his speech at the Human Rights Council[1], sheds light on the impunity with which such assaults and murders take place.

SAMDEN was created by media professionals from across South Asia who have themselves faced discrimination and intimidation. During its first international convening in Goa in March 2018, its core and associate members decided on an initial plan of action to make the network sustainable and active in defending freedom of expression in the subcontinent. Key areas that this meeting focused on included working and building capacity of like-minded individuals and organisations across borders.

The group agreed to proceed with a clear goal of acting against attacks or threats to the life and reputation of journalists. Over the past year, SAMDEN has worked earnestly to consolidate its network and initiate these functions. In 2018, along with others, we advocated for the release of celebrated Bangladeshi photojournalist Shahidul Alam who was arrested and eventually freed. SAMDEN also drew attention to the arrest and detention of press workers elsewhere, such as that of Mimi Mefo from Cameroon and Maria Ressa in The Philippines.

This year, we aim to expand our network further and take up more research and advocacy responsibilities around chosen issues that bar honest reportage and deter press freedom in South Asia.

The meeting and this report come out of concerns about the safety of journalists and their work in the digital space. The problems here are unique, when

[1] Hindustan Times: "UN rights commissioner criticises India over Gauri Lankesh murder, handling of Rohingya refugees"

contrasted to those that they face offscreen (or 'offline'): harassment and abuse, trolling, doxing, illegal surveillance and 'tracking'. Even though these problems are common to journalists across the region (and indeed, across the world), this particular convening focused on journalists in India.

"We are meeting at a very challenging time when problems such as fake news abound. What can be done to address these? How do we deal with this continuous assault of the freedom of the press and journalists?" asked Mr. Sanjoy Hazarika, International Director, CHRI while introducing the first session of the convening. He also stressed on the fact that these problems cannot be solved in isolation. "We need to have each other's backs. We need to work together to support each other," he added, because in such times, it is more important than ever that defenders of truth and rights do not have to work in isolation.

To whom can a rural stringer, a regional reporter, or a suburban news outlet turn if they are attacked by, say, the sand mafia (as happened, for instance, in cases such as 1, 2 and 3), for uncovering corruption, or if they are dragged into frivolous, yet expensive lawsuits by powerful politicians or corporations (as happened in these cases)? What protects Indian journalists today? Very little.

On the other hand, there are several laws on the books that have been – and continue to be – used to target them for their work. Several of these laws are part of India's colonial heritage – a heritage it shares with other Commonwealth countries. To this day, media workers in these countries can be punished by arrest under various sections such as criminal defamation, sedition, morality, obscenity and expressions of sexuality, among others.

Yet other laws, such as certain section of the Information Technology (IT) Act give the State an astonishingly wide scope for surveillance. Section 69, for instance, can let any government official or policeman to listen in to personal calls, read SMSs and emails, and monitor websites visited, without a magistrate's warrant. The government can also block websites under Section 69(A). More recently, through the proposed IT [Intermediary Guidelines (Amendment) Rules] 2018, the government attempted to give service providers and platforms greater powers to monitor, censor and block user content – a move that drew criticism from rights groups across India as well as the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

Apart from legal attacks, journalists also face intimidation in other forms, including violence, both online and offline. According to the Committee to Protect

Journalists (CPJ), at least 47 journalists have been killed in India over the past 20 years -- 11 since 2014. Several, if not all, of these journalists received threats beforehand for the (often sensitive or controversial) work they had been doing.

While all threats do not end in acute violence, they often force editors and organisations to withdraw critical stories, quit their jobs, or suffer a heavy psychological toll. Some end in physical attacks meant to serve as warnings. A study by Trollbusters and the International Women's Media Foundation found that “around 40% of the female journalists they interviewed across the world had stopped writing about stories they knew would be lightning rods for attacks”.

These dangers can no longer be ignored.

Freedom of the press is not merely the freedom of the media to report, but also the freedom of the people to receive their news freely, Mr. Venkatesh Nayak, Head of CHRI’s Access to Information programme said at the convening. No discussion about free access to information can, therefore, be complete without addressing the ways in which governments can withhold information from their citizens. There have, historically, been several ways this has been done: by directly shutting down radio/TV shows, by directly attacking news outlets, banning them or financially pressuring them into refraining from reporting, or more recently, by shutting the medium of popular communication, the internet.

In this convening, therefore, we chose to focus on three major issues that plague journalists in India: the (mis)use of laws to attack journalists; trolling and online attacks against journalists; and the need for protection against surveillance and misinformation.

THE (MIS)USE OF LAWS TO ATTACK JOURNALISTS

> **"Legislation designed by British colonial rulers as a tool to aid in the oppression of indigenous populations is now used routinely by their own new leaders"**
>
> - "The Independence of the Commonwealth Media and Those Working Within It", Commonwealth Press Union[2]

In India, the press derives its rights from Article 19(1a) of the Constitution which guarantees its citizens the right to freedom of expression. Article 19(2) allows the state to impose "reasonable restrictions" on the practice of this right – but with the increasing number of state-supported or sponsored variety of attacks against the free press, the need for amending some particularly problematic provisions of laws becomes clear.

The Indian state has, on several occasions, (mis)used the law to silence journalists as threats or retribution for their work. In March 2016, Prabhat Singh, a journalist from Chhattisgarh, was arrested[3] under Section 67 (publishing or transmitting obscene material in electronic form) and 67(A) of the Information Technology Act, 2000 (henceforth referred to as the 'IT Act'), for allegedly posting an "obscene message" about a senior police officer on WhatsApp groups[4]. Indian journalists have also routinely been arrested under other laws, such as the National Security Act, the Unlawful Activities (Prevention) Act (UAPA), the Official Secrets Act (OSA), and sedition and censorship, among others.

Further, Section 69(a) of the IT Act authorises the government to block access to websites on grounds that mirror provisions of Article 19(2). Under this section, there have been a spate of internet shutdowns India -- in fact, in 2018, India had

[2] Commonwealth Press Union, 1999: The Independence of the Commonwealth Media and Those Working Within It. London: CPU

[3] The Indian Express: "Chhattisgarh: Journalist arrested for allegedly taking a dig at a cop on WhatsApp", as on March 23, 2019

[4] He was also charged under section 292, publication of obscene or scurrilous matter, of the Indian Penal Code.

the highest number of shutdowns in the world! This provision can be particularly detrimental to the free press[5] not just because it disables news outlets from reaching their readers online, but also because all proceedings under this Section are secret (with only the government and the intermediary being aware of the blocking order), and journalists are effectively stifled until the ban is eventually lifted after an often extremely slow pace appeal process.

While there are several other legal threats to journalism in India, apart from the ones named above – such as Parliamentary privilege, criminal defamation, the use of the Cable Television Network (Regulation) Act, contempt of court, and disclosure of sources -- this convening focused mainly on provisions of the IT Act and two other specific pieces of legislation, criminal defamation and contempt of court, that have been used muzzle journalism.

Ms. Patricia Mukhim, editor of the Shillong Times – one of the oldest newspapers in India's north-east -- discussed at the convening her recent legal ordeal where the Meghalaya High Court filed a contempt of court case[6] against her and the publisher of the newspaper, a move that was criticised by journalist groups and lawyers across the country for its harshness. The court's order had come in response to a story published in the paper in December, which discussed a judgement providing perks and facilities for retired judges and their families. The Court imposed a fine of ₹2 lakh each on both journalists.

"Such penalties… [have] succeeded in hurting me. Some of us have reached a point where we wonder whether it is still worth doing journalism. How many attacks can we bear?" said Ms. Mukhim at the convening

A week after the court's order (and the date of this convening), the Supreme Court of India stayed the Meghalaya court's order.[7] At the time of writing, the case is *sub-judice*.

Mr. Mahfuz Anam, editor and publisher of The Daily Star, who joined the convening from Dhaka via Skype, discussed the negative effect that the recently passed Digital Security Act (DSA) has had on Bangladeshi media. "The

[5] The Indian Express: "Yes, snooping's allowed"
[6] The Hindu: "Heavy-handed order: on contempt law"
[7] Because the case is still *sub-judice*, we would like to emphasise that with deepest respect to the wisdom of courts, SAMDEN believes that while they are entitled to initiate contempt proceedings in cases where "*the statement [is] not only false, but [also in] such a character that can proximately lead to impeding the course of justice*", this particular judgement was deeply disturbing as it impacted one of the oldest newspapers in the North-East. Mr. Sanjoy Hazarika, has said, "During times of shrinking spaces for freedom of expression – as this certainly is -- a country should be able to look up to its judiciary for guidance and security. The court should have taken this as an opportunity to engage with journalists if it felt that it had been misrepresented. Patricia Mukhim is a respected member of the SAMDEN team and we support her legal rights as a citizen and journalist."

government pretends that the law is only meant to combat communal hatred on digital platforms, but its vagueness gives much power to the state to attack journalists that it creates an environment of intimidation everywhere."

Under the DSA, which was enacted last year, the police have been given unlimited powers to make arrests without warrants, raid newsrooms and even take away computer servers on the mere suspicion of wrongdoing. Non-cooperation by a suspect can lead to arrest for obstruction of justice and the Act itself provides for 20 provisions for punishment, out of which 14 are non-bailable, five are bailable (on the discretion of the judge), and one is relatively relaxed. The period of punishments range from a year to a lifetime.

"Since every news outlet now has a strong online presence and given that the future of journalism lies online, this law strongly affects and suffocates all journalists. The environment [in Bangladesh right now] is absolutely non-conducive to any form of dissent," he added.

"Law enforcement agencies might be given similar power in India soon too," remarked Mr. Kishore Bhargava, Technology Mentor at LinkAxis Technologies – referring to recent attempts by the Ministry of Electronics and Information Technology[8] to amend the Intermediary Guidelines of the IT Act that would give unspecified government agencies the power to order social media companies to monitor and block user content in India.

Mr. Apar Gupta, Executive Director of the Internet Freedom Foundation (IFF) added that these very social media companies are often heavily funded by political parties in power (who are also often the largest advertisers on these platforms). This created the risk of turning these platforms into political propaganda machines.

Another deterrent to the freedom of expression, participants pointed out, has been the criminal defamation law, especially "strategic lawsuits against public participation" (SLAPPs), which can be used against anyone "alleged of having uttered, written or published content that is malicious, baseless and harmful to the reputation and social standing of another party, under provisions relating to both civil and criminal defamation laws under IPC Sections 499 and 500 and Sections 199(1) to 199(4)".

Reference was made to an article which emphasised how "defamation and SLAPP lawsuits have become an all-too-common tool for intimidating and

[8] IT Amendment Rules 2018: Special Procedures, Human Rights Council writes to the govt of India expressing concerns over provisions

silencing critics of governments, corporations, businesses, actually anyone who is at a lower rung on the clout ladder" [9].

Indeed, SLAPPs can have a "chilling effect" on free press when large corporations or governments take on journalists and tie them up in protracted and expensive cases. For instance, between 2011 and 2016, the Tamil Nadu government under the political party AIADMK, filed 55 defamation cases against journalists (from a total of 213 defamation cases filed overall)[10]. In June 2017, the Adani group filed criminal and civil defamation cases against the news website The Wire and the Economic and Public Weekly (EPW)[11] for publishing an article titled "Modi Government's ₹500 Crore Bonanza to Adani Group Company". The Adani group eventually lost the case[12].

Mr. Paranjoy Guha Thakurta, who had in 2017 resigned from his position as EPW editor a result of this SLAPP[13], said that it was time "to come together as journalists and work on decriminalising defamation, and possibly even take this cause forward legally."

Mr. Apar Gupta agreed, saying that "there is no major democracy in the world where defamation continues to be a criminal offence… Laws such as sedition and criminal defamation are colonial remnants that need to be done away with." The IFF has been working on speechbill.in, alongside a former MP[14] to draft and advocate for legislation to solidify India's defamation laws, he said.

Indeed, Mr. Kumar Lopez, Director of the Sri Lanka Press Institute (SLPI), a SAMDEN partner organisation, told the convening through Skype that Sri Lanka too had successfully repealed criminal defamation in the late 1990s.

---

[9] The Wire: "We Need an Anti-SLAPP Law To Encourage and Protect Free Press": As journalists, academics, legislators and bloggers across the country have recognised, such lawsuits are an increasingly-used weapon against speech that some people and businesses would rather have silenced," says The Wire. The author notes that "the goal of complainants (the allegedly defamed) in these cases is not necessarily to actually win the lawsuit, but to drag their critics to court and bury them under the tyranny of a judicial process…"

[10] The NewsMinute: "Jaya Govt filed 213 defamation cases in 5 years: Here are some of the strangest cases"

[11] The Quint: "Adani Slaps Defamation Case on EPW for 'Crony Capitalism' Story"

[12] The Logical Indian: "Adani Loses Defamation Case Against The Wire & Economic And Political Weekly"

[13] The Wire: "Adani Group 'SLAPP' Pushes EPW Editor Out of His Job"

[14] The MP, Tathagat Satpathy, had noted on the Speechbill website, "If we look around the world, there is an emerging global trend to abolish criminal defamation … United Kingdom, the country that gave us the IPC in its original form, has repealed criminality in its defamation law in 1996 and… passed a reasonable law in 2013, properly defining what constitutes as defamation … Our legislature needs to step in and deliberate on the nature of the Criminal Defamation law and its effects."

The presence -- and the subsequent and inevitable -- misuse of such laws leads to self-censorship among news outlets, completely thwarting the purpose of a free and healthy press in a democracy. The group arrived at a plan of action to work on these issues, which have been noted below.

RECOMMENDATIONS

1. Seek details from the Bangladesh Editors Council regarding their position and reactions on how the DSA will stifle free press. It will then work with the group to identify specific problematic provisions of the law and advocate for their repeal.
2. Collaborate with the Indian Freedom Foundation (IFF) and offer networking support for its campaign on decriminalising criminal defamation
3. Draft a national legislation to protect journalists in India, which will be then shared for public consultations through stakeholders.

TROLLING AND ONLINE ATTACKS

> **"… Self-censorship is growing in the mainstream media and journalists are increasingly the targets of online smear campaigns by the most radical nationalists, who vilify them and even threaten physical reprisals. At least three of the journalists murdered in 2017 were targeted in connection with their work."**

- Reporters Without Borders[15]

One of SAMDEN's goals is to provide a network of support to suburban and rural journalists who may not have the contacts or tech support to protect themselves from threats, as journalists working with larger media outlets do.

Faced with such threats, journalists and media outlets can begin to self-censor their work, or continue working under unreasonable and unconscionable levels of stress.

Ms. Smriti Singh, Media and Advocacy manager at Amnesty International India spoke of a 2017 survey by the organization of 4,000 women in eight countries to see how they behaved on social media in response to online harassment and abuse[16]. They found that "76% of women who said that they had experienced abuse or harassment on a social media platform made changes to the way they use the platforms, and 32% said they'd stopped posting content that expressed their opinion on certain issues."

"This shows us that there is a subconscious fear in almost all women who use these online platforms," said Ms. Singh.

She then discussed another Amnesty project called "Troll Patrol"[17], which identified more than 700 female journalists and politicians in the US and the UK, and analysed their tweets across 2017, checking for abusive responses. The

[15] Reporters Without Borders: India Report
[16] Amnesty: "Amnesty reveals alarming impact of online abuse against women"
[17] Amnesty: Troll Patrol Findings

study found that around 1.1 million tweets in response to the women were abusive and problematic.

Mr. Kumar Lopez added that journalists in Sri Lanka too frequently faced (often verbal) abuse from government officials, which appeared to be an attempt by the government to control the press. “The media is fearful, and as a result, journalists themselves are sometimes guilty of spreading disinformation or misinformation,” he added.

Closer home, in India, journalist Rana Ayyub joined the convening over a phone call and discussed her experiences with online abuse. In April 2018, an online hate campaign against her in response to her work that was critical of the ruling party became so violent that she had to file a police complaint. The spate of abuse and violent threats also drew the attention of the Office of the United Nations Human Rights Commissioner, whose Special Rapporteurs called on Indian authorities to protect her[18].

However, “absolutely nothing has happened in response to the police complaint,” she told the convening, adding that the delay in due process has been on the police’s part. “There is a general lack of capacity at all levels coupled with a lack in civil awareness and training in the police force [when it comes to online attacks],” she said.

On the contrary, said Ms. Ayyub, Twitter – the platform where the hate campaign against her was most vicious – has been cooperative and even provided links to the offending tweets based on her screenshots to the police.

However, “community guidelines” on platforms such as Twitter and Facebook exclude content that might covertly imply a threat to a journalist. This loophole makes their claims of trying to create safe online spaces ring hollow, and may be the reason why several requests for help are turned down. It is also difficult to quantify the effectiveness of the efforts by these platforms, given lack of transparency around their processes.

For instance, Twitter recently “refused to make public meaningful data on how the company responds to reports of violence and abuse, on the grounds that such data ‘is not informative’ because ‘reporting tools are often used inappropriately’[19].”

[18] UNOCHR website: “UN experts call on India to protect journalist Rana Ayyub from online hate campaign”
[19] Amnesty: “Online Abuse Of Women Thrives As Twitter Fails To Respect Women’s Rights”

Despite some steps having been taken by these companies, trolling, doxing (leaking someone's personal details, such as addresses and phone numbers online), abuse and hate speech continues unabated online. In its 2018 report, Reporters Without Borders noted that, "Hate speech… [is an issue] in India (which in 2018 fell two places to 138th in the World Press Freedom Index)." It spoke of the "torrent of online insults" that investigative reporting draws: "As elsewhere in the world in 2017, this verbal violence has tragically led to physical violence".[20]

Threats and harassment against journalists is not limited to the online space. Ms. Patricia Mukhim recounted her own experiences of facing attacks in response to her work. "In April 2010, someone hurled a petrol bomb at my house. It hit a wall very close to my head. After this, the police assigned to me two personal security officers who still accompany me everywhere. I feel uncomfortable with this. I don't think this is any way to do journalism, with cops around you," she said.

"I have received a lot of trolling on communal grounds. Sometimes, it becomes very personal. In some parts of Shillong, they burn our newspapers or ban it. I feel such trolling is a way to demonise a person and create a narrative around them, like 'this is why they deserve to die' — so it becomes easier to eventually attack them," she added.

In the absence of any nation-wide legislation to ensure the protection of journalists from (both online and offline) attacks, neither the police nor social media platforms act urgently on complaints -- sometimes, not even until it is too late. Most Indian journalists who faced reprisals in the form of attacks (or even murder) in the past few years had received online threats first.

According to the Committee to Protect Journalists (CPJ), at least 64 journalists and press workers have been killed in India since 1999[21]. Several, if not all, of these journalists received threats beforehand for the sensitive or controversial work they had been doing. In March 2018, Sandeep Sharma, a journalist from Madhya Pradesh who was investigating sand mafia was killed in an alleged road accident. He had earlier sought police protection after having received threats. He got no help. Before her murder, Gauri Lankesh too had been the target of an active online hate campaign.

[20] Reporters Without Borders: "RSF Index 2018: Asia-Pacific democracies threatened by China's media control model"
[21] CPJ.org: "64 Journalists and Media Workers Killed in India"

“Most journalists in big cities are secure physically even after being trolled, but those living in smaller towns are more vulnerable to such threats turning into physical attacks,” said Ms. Smriti Singh.

“The main problem that journalists facing online abuse in India is the general lack of infrastructure for seeking legal help and support,” added Ms Ayyub.

RECOMMENDATIONS

1. Create a website where it will share details of all attacks against journalists in India, Pakistan, Bangladesh and Sri Lanka (to begin with). It will also share with users details of lawyers and cyber-crime cells in cities across India to facilitate easier reporting of threats and attacks.
2. Create a handbook for best digital practices that journalists can use to guard themselves against online attacks.
3. Work with partner groups to advocate for social media platforms to improve their community guidelines to make platforms safer for journalists.

STAYING SAFE ONLINE: ON THE NEED FOR PROTECTION AGAINST SURVEILLANCE AND MISINFORMATION

> **"Your password should be like a toothbrush: Choose a good one, don't share it with anyone and change it frequently."**
>
> - Kishore Bhargava, Technology Mentor

Education around personal digital privacy continues to be limited. Mr. Bhargava said, "[When it comes to protecting ourselves against surveillance] People say 'I have nothing to hide', but personal privacy is underrated by most. Anyone using technology needs to be aware of the ways in which it can be misused."

He went on to say, "The amount of data that is being generated on a daily basis – a quintillion bytes of data daily – can be analysed and parsed in seconds. And this can easily be used against you."

Indeed, in addition to the lack of legislation protecting user privacy in India -- which leaves the millions of smartphone users in the country susceptible to privacy and data loss -- there is also woefully little awareness about how personal data can be misused, and how to best protect privacy. Internet users, including journalists, thus end up adopting lazy digital practices, such as re-using passwords (or not choosing a strong one to begin with), logging into unverified services with their Google or Facebook accounts, giving apps access to their files, location, and contacts – all of which can and has been misused to mine user data around the world.

"Today, tou can go to Nehru Place [a New Delhi marketplace], and for less than ₹5,000, buy 4 or 5 lakh email addresses," said Mr Bhargava.

Commodore Lokesh Batra, an RTI activist, offered personal examples of how he suspected user data was being mined by the government. "I get phone calls and emails about [Indian Prime Minister Narendra] Modi's *Mann ki Baat* [a programme in which he addresses citizens on All India Radio, DD National and

DD News] despite never having signed up for it or given consent to receive these!"

"We need to examine why it is important for the state to constantly monitor every individual. Often, the tools for such analysis are developed by private companies who initially begin to do this for their own perception studies. We must also remember that the capability for such monitoring is being paid for by taxpayer funding," said Mr. Venkatesh Nayak.

"How can there be accountability when intelligence agencies are not answerable to audits, and don't are not obligated to make their reports public? This system needs to be opened up, so we can know exactly how much snooping is happening in a minute-to-minute basis," he added.

Mr. Paranjoy Guha Thakurta, journalist, author and political commentator, said, "Earlier, there used to be targeted surveillance of people of interest but now, the state has moved to mass surveillance. And it is made easier by technological advancements. Today there is enough server space to record the digital history of every person on the planet till they are 100 years old. This is the reality of the world we live in."

"A decade ago, very few of us imagined that a conglomerate of six corporations would dominate the digital landscape today: Facebook, Google, Amazon, Netflix, Apple, Twitter. Between them, they own most of user data in the world today," he added. The possibility of surveillance in India also becomes high "since (according to Trai, the Telecom Regulatory Authority of India), there are almost a billion SIM cards[22] in India, and over half of the phones in India are smart phones".

Ms. Anju Anna John, project officer with CHRI, said that online monitoring of internet users under Section 66A of the IT Act continued in parts of the country, despite it being struck down by the Supreme Court in 2015[23]. Before it was struck down, the Act (often described as "draconian") made it an offense to "send any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages."

[22] India Today: "Having more than 9 SIMs may land you in trouble"
[23] Huffington Post: "The Supreme Court Struck Down Section 66A of the IT Act in 2015, Why Are Cops Still Using It to Make Arrests?"

This disregard of the Court's directions aided the mining of user data, she added, asking whether it was a good idea to get the Act repealed by the legislature to bring an end to its use.

Speakers said that as consumers in the digital age we need be cognisant of the fact that all our browsing data is monitored and stored – then used to send targeted ads to us. Several mobile applications seek access to our devices' cameras and microphones (that unsuspecting users almost always grant), giving these companies access to even more information on citizens.

"This is how private vendors and corporations get our data -- and they can store them for as long as they want," said Commodore Batra. It is disturbing that there is currently nothing to stop corporations from retaining this data for as long as they want – and indeed, from passing it on to other groups or political parties for anything ranging from voter targeting to active surveillance. The participants agreed that citizens cannot be reduced to data subjects – either by the government or corporations.

Another point of concern raised was the lack of regulation around where such data on users will be stored. Are localised storage servers safer? Or are those located in "neutral" countries with sturdier data protection laws better for user privacy? Several "secure" online services and email clients such as Protonmail claim enhanced protection because of the physical location of their servers in countries such as Switzerland which have strong data protection laws[24] [25]. The convening agreed that this was part of a larger discussion that would need to take place around a potential data privacy bill in India.

This discussion, the convening agreed, would have to include a critique of the Justice Srikrishna Committee[26] recommendations on data privacy and management, and the proposed Personal Data Protection Bill, 2018[27].

"If you work in the media, this is a scary situation to be in right now," said Mr. Bhargava. Journalists' digital devices might often hold details of their work, investigations and contacts of sources – all information that they cannot afford to have slipping out into the world. Without widespread awareness of the evils of data mining, including among the particularly vulnerable rural and suburban journalists who may not have the tech savvy to protect themselves from surveillance, freedom of the press will continue to be under threat.

[24] "What is the advantage of a server located in Switzerland?"
[25] "Switzerland to become a secure haven for the world's data"
[26] Justice Srikrishna Committee Report on A Free And Fair Digital Economy
[27] The Personal Data Protection Bill, 2018

“Journalists from smaller towns, and rural areas who use social media to report on corruption are going to continue to be targeted, attacked and killed,” added Mr. Thakurta. Participants agreed that this was a particularly important area of work for SAMDEN.

RECOMMENDATIONS

1. Work in the area of creating data privacy education with focused awareness campaign. Participants suggested creating a short video series in collaboration with groups such as Down to Earth. Mr. Thakurta and Mr. Bhargava also expressed interest in this initiative.
2. Join other groups such as the Internet Freedom Foundation and to advocate for a consumer privacy legislation (the IFF has already initiated work on this). Special attention will have to be paid to points relating to specifying the period for which private companies can retain user data, and where such data will be stored.
3. As part of its handbook on best digital practices (mentioned in the preceding section), SAMDEN is to include tips on bolstering personal security, which journalists can use to shield their digital devices against illicit snooping. This handbook can be coupled with training workshops for journalists conducting with partner organisations.

MOVING FORWARD

1. **SAMDEN, as a network, should grow more rapidly, expand its activities and move rapidly in the direction of its goals. To this end**
    a. It must meet regularly as a group, either in person or through video-conferencing;
    b. It should build a solidarity group – a national network of “media defenders” -- in association with bodies such as the Editors Guild of India to increase its grassroots reach, with a special focus on rural and suburban media persons. It will document the concerns discussed at this meeting and bring them up with this network;
    c. SAMDEN will consider the feasibility of utilising UN mechanisms in addressing these concerns;
    d. It will bring more people, not just journalists but also young activists, leaders, rural groups, unions and other CSOs into the fold because the issue of freedom of expression affects them too;
    e. It will create an online email group and shared calendar which will be shared with all members.

2. **As part of its online presence, on its website, SAMDEN will**
    a. Create a platform where journalists can report attacks and threats, or accounts of being having faced breach of privacy;
    b. Connect imperilled journalists with lawyers and funding organisations who can help them in their legal battles;
    c. Publish public awareness videos in English, and eventually, in local languages in collaboration with partner groups to generate more discussions about the importance of bolstering personal digital security, the dangers of mass surveillance, and social media etiquette. Partners in these efforts are to be Paranjoy Guha Thakurta, Down To Earth, Kishore Bhargava, and moving ahead, known digital activists such as Pratik Sinha, Kunal Kamra, etc.

3. **SAMDEN will create a draft Journalist Protection Bill.**
    a. It was agreed that if the chances of getting a national legislation passed were slim, an alternative plan of action could be approach a state government with a progressive stance on freedom of expression and work on establishing a model system there, and then moving on to other states;

b. This work may be done in collaboration with Mr. Paranjoy Guha Thakurta and the Internet Freedom Foundation;
c. After drafting, the Bill will be shared with partner organisations and journalists groups for inputs and then published on the SAMDEN website to invite public comments.

4. SAMDEN will develop handbooks/reports on

a. The “chilling effect of SLAPPs” on media freedom in India, eventually expanding to other South Asian countries;
b. IT and other laws affecting journalistic freedom in South Asia;
c. Best digital practices for personal safety of journalists.

ANNEXURES

Annexure 1

Understanding the State's infringement of Privacy in light of Hohfeld's analysis

[By Sarthak Roy, Research Officer with the office of the International Director]

"Suppose that I am irritated by people who smoke in my vicinity. I meet S (smoker) in a public place, who starts to smoke in my presence. I ask him to stop, but S tells me he has a 'right' to smoke here (given the absence of any legal prohibitions). S is confusing his entitlement. He does not have a right (in the Hohfeldian sense) to smoke, but merely a liberty (a weaker right). Although I have a no-right concerning his activity of smoking, I do have a liberty myself ... to impede his smoking, say, by raising my voice or encouraging other people to make fun of S for his smoking habit, which may make him stop... Hohfeld's analysis therefore provides a clear understanding as to what the legal position of S is (i.e. what rights he has). As we can see, had it not been for Hohfeld providing us with a precise vocabulary, S would mistake his liberty for a right, and accordingly would be unable to accurately report the effect of his entitlement. He would be wrong in saying to me that I cannot stop him from smoking because he has a right to smoke in a public place, since it puts me under no duty not to interfere with his smoking."

Therefore States only have a liberty but not a right to infringe privacy of an individual.

Some important international instruments through which India can formulate a comprehensive data protection legislation, something which the Justice Sri Krishna Committee has missed taking inspiration from:

- UNGA RES71/199. The right to privacy in the digital age
- General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014, as well as Human Rights Council resolutions 28/16 of 26 March 2015 on the right to privacy in the digital age 4 and 32/13 of 1 July 2016 on the promotion, protection and enjoyment of human rights on the Internet, 5 and welcoming the appointment of the Special Rapporteur of the Human Rights Council on the right to privacy.
- article 12 of the Universal Declaration of Human Rights 1 and article 17 of the International Covenant on Civil and Political Rights;

UNGARES 71/199 Calls upon all States:

(a) To respect and protect the right to privacy, including in the context of digital communications;

(b) To take measures to put an end to violations of the right to privacy and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;

(e) To provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations;

(f) To develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data by individuals, governments, business enterprises and private organizations;

(g) To further develop or maintain, in this regard, preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women, as well as children and those vulnerable and marginalized;

(h) To promote quality education and lifelong education opportunities for all to foster, inter alia, digital literacy and the technical skills required to effectively protect their privacy;

(i) To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way;

(j) To consider appropriate measures that would enable business enterprises to adopt adequate voluntary transparency measures with regard to requests by State authorities for access to private user data and information;

(k) To develop or maintain legislation, preventive measures and remedies addressing harm from the sale or multiple resale or other corporate sharing of personal data without the individual's free, explicit and informed consent;

Indian IT laws have not defined Cyber Crimes. This definition can be averred from Tallinn Manual 1.0 and 2.0 as well as from guidelines as legislated by UNHCR and ICRC.

Annexure 2

Background note and agenda of this convening

Annexure 3

Report of the first international SAMDEN convening (2018)

Annexure 4

The Maharashtra Media Persons and Media Institutions (Prevention of Violence and Damage or Loss to Property) Bill, 2017

Annexure 5

The Chhattisgarh Special Act for Protection of Journalists and Human Rights Defenders

Annexure 6

The Mechanism to Protect Human Rights Defenders and Journalists in Mexico: Challenges and Opportunities

Annexure 7

Unshackling Expression: Criminal law and freedom of expression on the internet in India (GISWatch 2017)